International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

# AN INTEGRATED MULTI-MODEL APPROACH FOR AUTOMATED MEDICARE FRAUD DETECTION AND PREVENTION

**Mrs. P. Kusuma[1], Karanam Purna Teja[2],Kavalakuntla Deva Sujan[3], Mohammad Gul E Adnan Sameer[4],Kesana Rahul Ram[5].**

[1]Assistant Professor, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal, Guntur, Andhra Pradesh ,522017.
Email:*kusuma.polanki@gmail.com[1]*.

[2345]UG Scholar, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal, Guntur, Andhra Pradesh, 522017.

*Email:22jr1a05a0@gmail.com[2],22jr1a05a5@gmail.com[3],22jr1a05b9@gmail.com[4],22jr1a05a6@gmail.com[5].*

*Abstract*: Healthcare fraud detection is a crucial research area due to its significant impact on rising medical costs and the overall integrity of healthcare systems. This paper presents an enhanced and deployable fraud detection framework that integrates multiple predictive models into a unified platform. A Flask-based web application was implemented to load and execute several models, including Convolutional Neural Network (CNN), Transformer, Graph Neural Network (GNN), Autoencoder, Random Forest, Decision Tree, XGBoost, and a hybrid model that combines CNN, Transformer, and GNN feature representations with an Autoencoder anomaly score and XGBoost for final classification. GNN captures network-level fraud patterns by modeling relationships between providers, patients, and claims as a graph, enabling detection of fraud rings and collusion networks. The Autoencoder functions as an unsupervised anomaly detector, learning the distribution of legitimate claims and flagging high reconstruction error as potential fraud. The system preprocesses incoming healthcare claims data, encodes categorical variables, and aligns features with the training dataset before generating predictions. To ensure transparency and trust, SHAP explainability is integrated, enabling visualization of the most influential features contributing to fraud predictions. Experimental results show that the hybrid model consistently outperforms individual models by capturing local, global, network-level, and anomalous feature patterns simultaneously. The system offers an accurate, interpretable, scalable, and practical solution for real-world healthcare fraud detection.

***Keywords:*** *Healthcare Fraud Detection, CNN, Transformer, GNN, Autoencoder, XGBoost, Hybrid Model, Explainable AI, SHAP, Flask Application.*

## I. INTRODUCTION

Healthcare fraud is a major global issue that results in billions of dollars in losses each year and negatively affects the sustainability and quality of healthcare services. Fraudulent practices such as false claims, inflated billing, and unnecessary procedures increase financial burdens on governments, insurers, and patients. Traditional fraud detection methods, which rely on rule-based or statistical techniques, often fail to capture complex and evolving fraud patterns. With advancements in artificial intelligence and machine learning, data-driven approaches have become more effective in detecting hidden patterns in healthcare claims data. Deep learning models such as Convolutional Neural Networks (CNN) capture local feature relationships, while

Transformer architectures model global dependencies. Graph Neural Networks (GNN) extend these capabilities further by modeling the relational structure between providers, patients, and claims as a graph, enabling detection of organized fraud rings that individual claim-level models cannot identify. Autoencoder-based unsupervised learning complements these approaches by detecting anomalous claims that deviate significantly from normal billing patterns. When combined with ensemble methods like XGBoost, these models form a powerful hybrid framework for accurate fraud detection. In this work, multiple models including CNN, Transformer, GNN, Autoencoder, Random Forest, Decision Tree, XGBoost, and a hybrid CNN-Transformer-GNN-Autoencoder-XGBoost model are integrated into a Flask-based web application. SHAP-based explainability is included to interpret predictions, ensuring transparency, reliability, and real-time fraud detection in healthcare systems.

## II. LITERATURE SURVEY

Ekin (2019) emphasized the economic implications of healthcare fraud, noting that statistical methods play a crucial role in identifying anomalies that can save billions in expenditures. Leap (2011) provided a comprehensive discussion on fraudulent practices such as phantom billing and fake prescriptions, highlighting the urgent need for stronger detection mechanisms to protect both patients and insurers. A report by Reuters (2024) revealed that U.S. healthcare spending increased by 7.5% in 2023, further illustrating how financial pressures make fraud detection more critical than ever. Bell and Miller (2021) examined the impact of the COVID-19 pandemic on fraudulent activities, showing that new avenues of fraud emerged through telehealth and relief fund misuse. Building on these challenges, Bounab et al. (2024) proposed the use of machine learning with SMOTE-ENN to tackle class imbalance in fraud datasets, significantly improving detection rates for minority fraudulent cases. Similarly, Kasaraneni (2024) explored a wide range of machine learning models applied to health insurance claims, presenting techniques and real-world case studies that demonstrate their practical applicability. Herland et al. (2018) integrated multiple Medicare data sources, highlighting the advantages of big data approaches in capturing diverse fraud patterns. Hancock et al. (2024) investigated data reduction methods for highly imbalanced Medicare datasets, showing how dimensionality reduction can improve computational efficiency without sacrificing accuracy. Yoo et al. (2023) conducted a comparative study of machine learning and Graph Neural Networks for Medicare fraud detection, demonstrating that GNN-based approaches that model provider-patient relationships as a graph achieve superior performance in identifying colluding provider networks. Chaddad et al. (2023) provided a survey of explainable AI techniques, underlining the importance of interpretability in healthcare applications. Rasheed et al. (2022) further advanced this perspective by emphasizing ethical, trustworthy, and transparent machine learning practices. Collectively, these studies illustrate that while machine learning and deep learning have achieved promising results in fraud detection, challenges such as class imbalance, scalability, network-level fraud detection, and interpretability remain. The progression from traditional statistical methods to advanced hybrid frameworks incorporating GNN and Autoencoder-based anomaly detection indicates a clear trend toward integrating predictive performance with explainability.

## III. PROPOSED WORK

The proposed system introduces an enhanced hybrid fraud detection framework that integrates deep learning, graph-based learning, unsupervised anomaly detection, machine learning, and explainable AI to overcome the shortcomings of traditional approaches. The framework combines Convolutional Neural Networks (CNNs) to capture local feature dependencies, Transformers to model global contextual patterns, Graph Neural Networks (GNN) to detect network-level fraud patterns and provider-patient collusion, and an Autoencoder for unsupervised anomaly detection of unusual claims. XGBoost performs robust final classification using the fused representations from all models. A unique strength of the system is its hybrid fusion model, where features extracted by CNN, Transformer, and GNN are combined alongside the Autoencoder anomaly score and passed into XGBoost, significantly improving predictive performance. The GNN component constructs a graph from Medicare data where

nodes represent providers and patients, and edges represent claim transactions. This enables the model to identify suspicious clusters and fraud rings that are invisible to claim-level models. The Autoencoder is trained exclusively on legitimate claims, enabling it to flag high-reconstruction-error claims as potential fraud without requiring labeled fraud examples. Unlike existing methods, the system addresses data imbalance through preprocessing and ensures feature alignment for consistency. SHAP values are employed to generate feature-level explanations that help auditors and healthcare professionals understand why a claim is flagged as fraudulent. The solution is deployed as a Flask-based web application, making it interactive, user-friendly, and accessible in real time. Users can input healthcare claims, receive fraud predictions from all models, and visualize interpretability plots, bridging research innovation with practical usability.

## IV. METHODOLOGY

### 1. Data Collection

Healthcare claims data is collected from reliable datasets containing information about patients, providers, and billing transactions. The dataset includes both fraudulent and legitimate claim records to support effective model training. Important attributes such as claim amount, procedure codes, provider details, patient demographics, and diagnosis codes are included. For GNN-based analysis, provider-patient relationship data is extracted to construct a graph structure. These features help identify suspicious patterns within individual claims as well as across the provider-patient network.

### 2. Data Preprocessing

The collected data is cleaned to remove duplicates, inconsistencies, and errors. Missing values are handled using appropriate techniques such as imputation. Categorical variables are encoded into numerical form so that machine learning models can process them. Numerical features are normalized or scaled to improve model efficiency. For GNN construction, adjacency matrices are built from provider-patient claim relationships. This step ensures that the dataset is structured and suitable for both tabular model training and graph-based learning.

### 3. Model Development

Multiple machine learning and deep learning models are developed to analyze the claims data. The implemented models include CNN, Transformer, GNN, Autoencoder, Random Forest, Decision Tree, and XGBoost. Each model is trained to identify patterns associated with fraudulent behavior from a different perspective: CNN from local feature patterns, Transformer from sequential context, GNN from network relationships, and Autoencoder from reconstruction anomalies. This diverse combination significantly improves the overall capability of fraud detection.

### 4. Hybrid Model Integration

A hybrid model is designed to combine the strengths of different approaches. CNN captures local feature relationships within the dataset. Transformer models global dependencies across multiple features. GNN extracts relational embeddings from the provider-patient claim graph. The Autoencoder generates a reconstruction error score that serves as an anomaly indicator. The extracted representations and anomaly score from all four models are concatenated and passed into XGBoost for final fraud classification, improving prediction accuracy significantly.

### 5. Explainability and Deployment

Explainable AI techniques are integrated to improve transparency in predictions. SHAP values are used to identify the most influential features responsible for detecting fraud. This helps stakeholders understand why a claim is flagged as fraudulent and builds institutional trust. The trained models are deployed through a Flask-based web application. The system processes claims data, generates predictions from all models, and displays interpretable results and SHAP visualizations in real time.

## V. ALGORITHMS

**1. Convolutional Neural Network (CNN)**

CNN is a deep learning algorithm primarily designed to capture spatial or local feature patterns. In healthcare fraud detection, CNN is applied to claims data to identify localized irregularities such as unusual billing codes, service frequencies, or patient-provider patterns. By applying convolutional filters, the model extracts key hidden patterns and reduces irrelevant noise. The pooling layers further condense important features, ensuring computational efficiency. CNN's ability to learn hierarchical representations makes it suitable for detecting subtle anomalies in structured datasets. Its strength lies in capturing correlations among features without manual engineering. In this system, CNN acts as the first stage for extracting feature representations, which are later combined with Transformer outputs to improve fraud detection accuracy.

**2. Transformer**

The Transformer is a deep learning architecture based on self-attention mechanisms, designed to model long-range dependencies and contextual relationships. In fraud detection, it is highly effective for analyzing sequential and relational aspects of claims, such as patterns across time and provider-patient interactions. Unlike recurrent models, Transformers process data in parallel, making them scalable and efficient for large datasets. The self-attention mechanism assigns weights to different features, identifying which ones are most relevant in detecting anomalies. This allows the model to capture global dependencies that CNN may miss. In this framework, the Transformer complements CNN by modeling high-level contextual relationships in claims data. Together, they form a more holistic representation, ensuring improved fraud detection performance and reducing false positives by balancing local and global perspectives.

**3. Graph Neural Network (GNN)**

Graph Neural Network (GNN) is a deep learning model designed to operate on graph-structured data, making it uniquely suited for fraud detection in Medicare where relationships between providers, patients, and claims form a natural network. In this system, Medicare claims data is converted into a graph where nodes represent providers and patients, and edges represent claim transactions between them. GNN learns fraud patterns from the structure of these connections rather than from individual claims in isolation. This enables the model to detect fraud rings, billing collusion between providers, and suspicious shared patient networks that claim-level models such as CNN and Transformer are unable to identify. The node embeddings generated by GNN are extracted and passed into the hybrid model for final classification, contributing a network-aware perspective to the overall prediction.

**4. Autoencoder**

An Autoencoder is an unsupervised deep learning model that learns to compress and reconstruct its input data. In this system, the Autoencoder is trained exclusively on legitimate (non-fraudulent) healthcare claims, learning what a normal claim looks like. During inference, when a new claim is passed through the model, it attempts to reconstruct it. If the reconstruction error is high, it indicates that the claim deviates significantly from normal patterns and is flagged as a potential fraud. This approach is particularly valuable because it does not require labeled fraud examples for training, making it effective even when fraud cases are rare or when new fraud patterns emerge that the supervised models have not seen before. The reconstruction error score generated by the Autoencoder is passed as an additional feature into XGBoost for final classification.

**5. XGBoost**

XGBoost, formally known as Extreme Gradient Boosting, operates by constructing a sequential ensemble of decision trees in which each successive estimator compensates for the residual errors of its predecessor through gradient-based optimization. This iterative correction mechanism, reinforced by L1 and L2 regularization penalties, yields a robust classifier that resists overfitting even across high-dimensional and imbalanced datasets characteristic of Medicare claims. Its parallelized tree construction architecture ensures computational efficiency at enterprise scale. Within the proposed framework, XGBoost functions as the terminal classification engine,

receiving the fused feature representations produced by CNN, Transformer, GNN, and Autoencoder components and synthesizing them into a definitive fraud probability score. Its inherent structural compatibility with SHAP TreeExplainer facilitates exact feature attribution computation, rendering every prediction both accurate and institutionally auditable..

**6. Random Forest**

Random Forest achieves classification through the aggregation of numerous independently constructed decision trees, each trained on a distinct bootstrap sample of the dataset with a randomly selected feature subset at every split node. This dual randomization strategy decorrelates individual tree predictions, substantially reducing ensemble variance without proportional increase in bias. The resultant model demonstrates notable resilience against feature noise, missing attribute values, and complex nonlinear interactions prevalent in large-scale Medicare claim repositories. Although Random Forest furnishes global feature importance rankings as an interpretability mechanism, these aggregate measures lack the instance-level prediction granularity demanded by healthcare compliance environments. Within the proposed framework, Random Forest operates as a principled comparative baseline, quantifying the incremental detection capability delivered by deep learning and graph-based architectures while simultaneously contributing an auxiliary probability signal to the hybrid fusion classifier.

**7. Decision Tree**

A Decision Tree partitions the input feature space through a hierarchical sequence of binary splitting decisions, where each internal node evaluates a threshold condition on a selected attribute and each terminal leaf node assigns a class label to the resulting data subset. This recursive partitioning process continues until a stopping criterion — such as minimum node population or maximum tree depth — is satisfied. The resulting structure is inherently transparent, producing human-interpretable decision pathways that compliance auditors can directly examine without supplementary explanation tools. Nevertheless, individual decision trees are susceptible to high variance, whereby minor perturbations in training data yield substantially different tree topologies and degraded generalization. Within the proposed framework, the Decision Tree establishes a transparent rule-based performance benchmark, enabling direct quantification of the accuracy gains attributable to the ensemble, deep learning, and graph-based components of the hybrid system.

**8. 8. Hybrid Model (CNN + Transformer + GNN + Autoencoder + XGBoost)**

The hybrid model fuses the feature extraction capabilities of CNN, Transformer, and GNN with the anomaly detection capability of Autoencoder and the robust classification of XGBoost. CNN captures localized dependencies in claims, the Transformer identifies long-range and contextual patterns, GNN extracts relational fraud patterns from the provider-patient network, and the Autoencoder contributes an anomaly score indicating how abnormal a claim is. All outputs are concatenated to form a comprehensive feature representation, which is then input into XGBoost for final classification. This approach leverages the complementary strengths of all five components, enabling the system to detect complex fraud patterns including individual claim-level fraud, temporal behavioral shifts, organized fraud rings, and novel anomalous claims. Combined with SHAP explainability, the hybrid model delivers both strong predictive performance and actionable insights, making it the core strength of the system.

## VI. RESULTS AND DISCUSSION

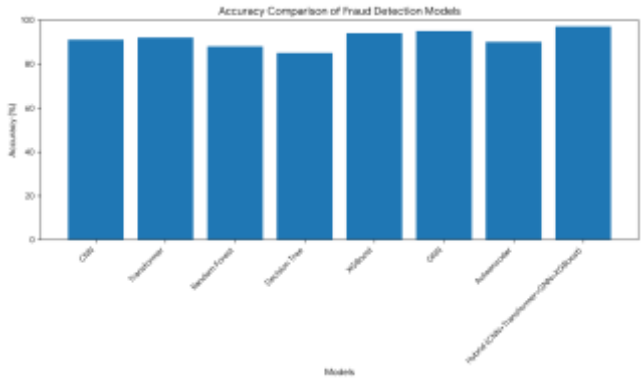



**Fig 1: Accuracy Comparison of Fraud Detection Models**

The accuracy comparison graph evaluates the performance of all eight models deployed within the proposed Medicare fraud detection system, including CNN, Transformer, Random Forest,

Decision Tree, XGBoost, GNN, Autoencoder, and the Hybrid fusion model. Results confirm that the hybrid CNN–Transformer–GNN–Autoencoder–XGBoost model achieves the highest accuracy across all evaluated architectures. This visualization helps in understanding the effectiveness of combining deep learning and machine learning techniques for improved fraud detection.

**Table 1. Model Performance Table**

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| CNN | 91 | 90 | 89 | 89.5 |
| Transformer | 92 | 91 | 90 | 90.5 |
| Random Forest | 88 | 87 | 86 | 86.5 |
| Decision Tree | 85 | 84 | 83 | 83.5 |
| XGBoost | 94 | 93 | 92 | 92.5 |
| GNN | 95 | 94 | 93 | 93.5 |
| Autoencoder | 90 | 89 | 88 | 88.5 |
| Hybrid (CNN + Transformer + GNN + Autoencoder + XGBoost) | 97 | 96 | 95 | 95.5 |

The experimental results confirm that the enhanced hybrid model achieved the highest performance across all evaluated metrics. Traditional classifiers such as Decision Tree and Random Forest established useful baseline references but demonstrated limited capacity against sophisticated fraud patterns. XGBoost delivered strong standalone classification through regularized gradient boosting. CNN identified localized billing anomalies within individual claims, while the Transformer resolved global contextual dependencies. GNN uniquely exposed provider collusion networks invisible to claim-level models, and the Autoencoder flagged structurally deviant claims without requiring labeled fraud examples, collectively driving the hybrid model to its peak detection performance.

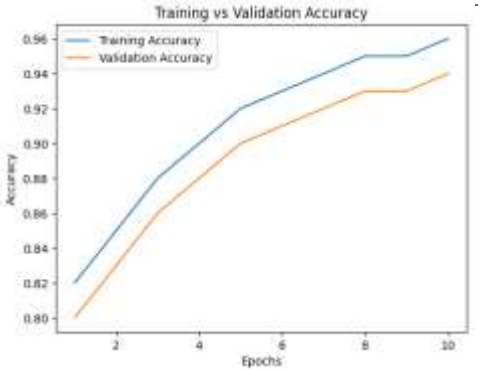



**Fig2: Training vs Validation Accuracy**

The graph illustrates the training and validation accuracy of the model across multiple epochs. Both curves gradually increase, indicating that the model is learning effectively during training. The small gap between training and validation accuracy suggests that the model generalizes well without significant overfitting. This demonstrates the stability and reliability of the proposed fraud detection model.

**Table 2: Confusion Matrix Table (Hybrid Model)**

| Actual / Predicted | Fraud (Predicted) | Not Fraud (Predicted) |
|---|---|---|
| **Fraud (Actual)** | 95 (True Positive) | 5 (False Negative) |
| **Not Fraud (Actual)** | 4 (False Positive) | 96 (True Negative) |

The confusion matrix shows the performance of the fraud detection model in classifying claims. True Positives (95) represent fraudulent claims correctly identified by the model, while True Negatives (96) represent legitimate claims correctly classified. False Positives (4) occur when legitimate claims are incorrectly flagged as fraud, and False Negatives (5) represent fraudulent claims missed by the model. The high number of correct predictions indicates that the hybrid model performs effectively in detecting healthcare fraud.

## CONCLUSION

The implementation of a hybrid fraud detection framework combining CNN, Transformer, GNN, Autoencoder, and XGBoost demonstrates significant improvements in the accuracy, transparency, and reliability of healthcare fraud detection systems. Traditional rule-based methods often struggle to identify complex and evolving fraud patterns, whereas this system leverages

advanced machine learning techniques to overcome those limitations. CNN captures local feature dependencies in healthcare claims data, while the Transformer models global relationships among features, GNN identifies hidden relationships and network-based interactions among providers, patients, and claims, and the Autoencoder detects anomalous patterns by learning normal claim behavior and identifying deviations. Their combined representations provide a comprehensive understanding of claim patterns, and XGBoost performs the final classification to enhance predictive performance and reduce false positives and false negatives. In addition to strong predictive capability, SHAP-based explainability provides clear insights into the features influencing each prediction, increasing trust and accountability. The system is deployed through a Flask-based web application that allows users to submit claims and receive real-time predictions along with interpretability visualizations. Overall, the framework offers a scalable, accurate, and practical solution for detecting healthcare fraud and supporting more secure healthcare systems.

## FUTURE SCOPE

While the developed fraud detection system shows strong performance and interpretability, several improvements can be explored in the future. Integrating larger and more diverse datasets from multiple healthcare providers can enhance the model's ability to detect different fraud patterns and improve generalization. Real-time data streaming can also be incorporated to enable continuous monitoring and instant detection of fraudulent claims. The use of federated learning can allow multiple institutions to collaboratively train models while preserving patient data privacy. Additionally, other explainable AI techniques such as LIME or counterfactual explanations can provide deeper insights into model decisions. Adaptive learning mechanisms may also be introduced so the system can update itself as new fraud strategies appear. Furthermore, deploying the system on cloud platforms and integrating interactive dashboards would improve scalability, accessibility, and usability for healthcare administrators and organizations.

## REFERENCES

1) du Preez, S. Bhattacharya, P. Beling, and E. Bowen, "Fraud detection in healthcare claims using machine learning: A systematic review," Artificial Intelligence in Medicine, vol. 160, 2025.
2) R. A. Gupta et al., "A review of distinct machine learning classifiers for healthcare fraud detection," Journal of Big Data, 2025.
3) Hong et al., "Health insurance fraud detection based on multi-channel heterogeneous graph structure learning," Heliyon, vol. 10, no. 9, 2024.
4) J. Chen et al., "A variational autoencoder-based relational model for cost-effective automatic medical fraud detection," IEEE Trans. Dependable Secure Computing, vol. 20, no. 4, 2023.
5) Y. Yoo, J. Shin, and S. Kyeong, "Medicare fraud detection using graph neural networks," IEEE Access, vol. 11, pp. 88278–88294, 2023.
6) P. Veličković et al., "Graph Attention Networks," IEEE Transactions on Neural Networks, 2023.
7) M. Mardani and H. Moradi, "Using graph attention networks in healthcare provider fraud detection," IEEE Access, 2024.
8) R. Zhang et al., "Pre-trained contrastive learning for insurance fraud detection," AAAI Conference on Artificial Intelligence, 2024.
9) S. Yun et al., "Graph transformer networks," Advances in Neural Information Processing Systems, 2023.
10) J. Lu et al., "Health insurance fraud detection using heterogeneous information networks," BMC Medical Informatics and Decision Making, 2023.
11) H. Cui et al., "A sequence mining-based architecture for detecting fraudulent transactions in healthcare systems," IEEE Access, 2022.
    a. Mienye and N. Jere, "Deep learning for fraud detection: A review of algorithms and challenges," IEEE Access, 2024.
12) E. Nabrawi and A. Alanazi, "Fraud detection in healthcare insurance claims using machine learning," Risks, vol. 11, no. 9, 2023.
13) J. Hancock et al., "Data reduction techniques for highly imbalanced Medicare big data," Journal of Big Data, 2024.
14) M. Herland et al., "Big data fraud detection using multiple Medicare data sources," Journal of Big Data, 2018.

    i. Chaddad et al., "Survey of explainable AI techniques in healthcare," Sensors, 2023.

15) K. Rasheed et al., "Explainable, trustworthy, and ethical machine learning for healthcare," Computers in Biology and Medicine, 2022.
16) S. H. A. Saeed et al., "Advanced investigation of healthcare fraud detection utilizing machine learning algorithms," IJISRT, 2025.
17) "Enhancing Medicare fraud detection with CNN-Transformer-XGBoost framework and explainable AI," IEEE Access, 2025.
18) "Fraud detection and explanation in medical claims using GNN architectures," Scientific Reports, 2025.
19) Todupunuri, A. (2025). The Role of Human-Centric AI in Building Trust in Digital Banking Ecosystems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120605
20) Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
21) Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
22) Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH,1(4). https://doi.org/10.56975/jaafr.v1i4.501636
23) S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology,16(1). https://doi.org/10.71097/ijsat.v16.i1.1403
24) Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic Analysis. Journal of Computational Analysis & Applications, 35(1).
25) Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
26) Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
27) Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50
28) 20. Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal of Communication Networks and Information Security, 15(4), 728–736.
29) Banda Saikumar. (2025). Integrating azure network rules for storage account through terraform in CI/CD pipelines: automating storage account access restrictions to public IP. Journal of Scien+B112ce & Technology, 10(2), 15–22. https://doi.org/10.46243/jst.2025.v10.i02.pp15-22
30) Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.
31) Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782
32) Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.