International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 607-614 www.ijaem.net ISSN: 2395-5252

Dynamic Fraud Detection in Cloud-Based Banking Systems with Graph Convolutional Networks and Temporal Attention

Dharma Teja Valivarthi [1], Swapna Narla [2], Sai Sathish Kethu [3], Durai Rajesh Natarajan [4], Sreekar Peddi [5], G. Arulkumaran [6, *]

[1]*Tek Leaders, Texas, USA,*
[2]*Tek Yantra Inc, California, USA*
[3]*NeuraFlash, Georgia, USA*
[4]*Estrada Consulting Inc, California, USA*
[5]*Tek Leaders, Texas, USA*
[6]*Associate Professor, School of C&IT, REVA University, Bangalore, India*

Date of Submission: 10-03-2025 Date of Acceptance: 20-03-2025

ABSTRACT: The model suggested for detection of financial fraud detection a Modified Graph Convolutional Network with Temporal Features Network (MGCN-TFNet) for spatial as well as temporal data analysis. The model initiates with acquiring the dataset and normalizing it, followed by applying Graph Convolutional Networks to learn about transactional structural patterns and embeddings of features. Temporal attention layers emphasize corresponding time-based features and identify transactions according to relevance for various windows of time. An integration layer of temporal-structural embeddings enhances fraud detection. A fine-tune and final classification fully connected layer by a SoftMax classifier detect valid and invalid transactions. The performance of the model is tested based on a confusion matrix, with an accuracy of 0.991, precision of 0.992, sensitivity of 0.990, specificity of 0.992, and 0.991 in F-measure. The Negative Predictive Value (NPV) is 0.939, which is indicative of superior performance in identifying true fraudulent transactions. This methodology is very effective in integrating structure learning and temporal pattern discovery for detecting financial fraud.

Keywords: Graph Convolutional Networks (GCN), Temporal Features Network, Fraud Detection,Banking Systems, Digital Banking.

I. INTRODUCTION

The financial sector experienced a fundamental change through cloud computing and digital banking solutions that allowed banks to provide scalable efficient easy services to their customers. New banking solutions provide additional spaces for fraud to occur. The shift of banks to cloud services requires new fraud detection methods because modern financial data maintains large scale and complex structures[1]. Modern criminal techniques aimed at security points are evolving which makes it harder for cloud-based banking systems to detect fraudulent activities.Advanced data processing systems are necessary for detecting fraud within enormous databases containing complex unstructured patterns. Complex financial transactions keep rising so institutions must use advanced machine learning algorithms with deep learning capacity to identify potential frauds early during high-precision stages[2].

The traditional fraud detection systems encounter implementation challenges when combining rules and statistics with anomaly detection models. The experience significant problems that restrict scalability and necessitate complex feature creation practices and flexibility degrees. The current analytical methods experience operational inefficiencies because rising transaction

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 607-614 www.ijaem.net ISSN: 2395-5252

volumes and data points produce more false alarms and undetected illegal transactions. The identification of complex patterns in enormous multi-dimensional datasets requires manual work on traditional datasets to extract interrelationship patterns traditional methods cannot detect. The old systems struggle to detect new fraud patterns since these patterns are constantly undergoing changes[3]. Increasing machine learning and deep learning popularity brings solutions to combat those problems. This problem can perhaps be solved when Graph Conventional Networks (GCNs) combine with Temporal Attention processes. The ability of GCNs to discover intricate data relationships enables good performance but Temporal Attention maintains specialized abilities in temporal pattern detection which results in a precise adaptable fraud detection system[4].

The need of GCN in Large-scale financial data in cloud-based banking requires complex entity relationships between accounts, users, transactions, devices and locations. The complex data network can be successfully modelled through Graph Convolutional Networks (GCNs) because of their ability to handle interconnected data[5]. The spatial relationships between entities in graphs become detectable through the special capabilities of GCNs. The nodes in fraud detection represent accounts or transactions while edges show the relationships between these elements including transactions between matching accounts and suspicious device or location patterns[6]. Modelling complex interconnections becomes essential for finding advanced fraud patterns because these patterns develop from analysing time-based relationships between multiple entities. The feature propagation mechanism of GCNs traverses the graph structure to discover relationships between nodes while collecting information from adjacent nodes thus revealing fraudulent activities that link between different accounts or users. GCNs provide an optimal solution for detecting fraud in cloud-based banking systems because of their capabilities[7].

The patterns of fraudulent activities show non-stationary behaviour because they evolve through time with sudden transaction amount spikes and unusual timing patterns. The integration of temporal attention mechanisms allows the model to detect these patterns of change that occur across time[8]. Through temporal attention the model identifies important information within transaction sequences so it can identify unsafe communication patterns during distinct time periods[9]. The model determines attention values to particular segments of time-series data which allows it to prioritize transactions demonstrating irregularities regarding their frequency and amount and timing. The attention mechanism proves crucial for fraud detection since it allows the model to analyse sequences with elevated fraud risks[10]. Sudden big withdrawals along with several transactions made from different locations within a short period will trigger concern. Through temporal attention the model identifies which events hold the most significance and their position in transaction sequences[11].

Security threats against cloud-based financial systems continue to evolve because hackers employ advanced strategies and financial data shows both extensive amounts and variable patterns[12]. The Graph Convolutional Networks and Temporal Attention system develops into a dynamic structure which detects financial data patterns together with structural linkages[12].Institutional clients alongside their customers can achieve Realtime fraud defence through hybrid system approaches that offer better performance alongside expansion possibilities and adaptability[14].The role of the proposed techniques in the model of dynamic fraud detection in cloud banking systems includes:

- GCNs assist in learning structural features in the transaction data by extracting spatial correlations between various entities like users, accounts, transactions, and devices. This enables the system to capture the relationships and interactions between such entities and significantly enhances fraud pattern detection through the network structure.
- Through the allocation of the attention weights to the windows of time, the approach insists on the model giving a specific weight to impactful transactions while attempting to discover fraud.
- All various data sources are encoded and normalized so they turn homogeneous and in an appropriate form to input into the network.
- The data are organized in the form of a dynamic graph, where users, accounts, transactions, and devices are all nodes.
- Binary cross-entropy loss is employed for the balancing of the model during training time, one of the usual loss functions used in binary classification.

This paper is organized as follows: Section 2 reviews fraud detection techniques and their limitations. Section 3 details the proposed MGCN-TFNet. Section 4 presents the performance

evaluation of MGCN-TFNet using the Financial Fraud detection dataset. Section 5 concludes with a summary and future research directions.

II. LITERATURE SURVEY

The paper describes a cloud-based finance analysis system that utilizes advanced algorithms such as Cat-Boost, ELECTRA, t-SNE, and Genetic Algorithms to handle category data, text, and feature reduction. It maintains 95% accuracy, 92% precision, and 95% scalability, demonstrating its usefulness in financial analysis[15].Banking and e-commerce are leveraging intelligent networks, blockchain, and cloud computing to enhance scalability, efficiency, and security on huge datasets. By virtue of combining Cloudbasedresource administration andIo Tbased analytics with blockchainfor secure transact ions, the use of resources boosted by 30%, scalability enhanced by 25%, security boosted by 35%, and speed of transactions rose by 20%[16].The suggested secure cloud-based financial analysis system enhances risk forecasting and financial modelling by utilizing Monte Carlo simulations, Deep Belief Networks, and Bulk Synchronous Parallel. It offers scalability, security, and high-performance data processing with reduced computational time and data security via encryption. It attempts to enhance memory, accuracy, and precision over conventional procedures[17].The study investigates the impact of cloud-based digital finance on income equality in urban and rural economies, finding that combined digital finance choices significantly improve financial inclusivity, enhancing rural access to transactions and savings[18].The research examines the effect of internet-inclusive finance on the economic development of rural Africa, specifically on e-commerce. It is indicated that this approach greatly increases income, entrepreneurship, and business development in rural areas, thus narrowing the urban-rural gap and enhancing global progress [19]. The study investigates the effect of cloud computing and internet financing on urban-rural income inequality. The study uses panel data analysis to investigate the relationship between levels of income and the adoption of digital banking. According to the study, enhanced access to cloud computing and internet finance reduces income inequality as well as improving financial inclusion as well as economic opportunities for rural populations [20].

III. METHODOLOGY

The proposed framework for financial fraud detection begins with dataset collection, where the financial fraud detection dataset is collected. Normalization of data and imputation of missing values is performed so that it is in a proper format to be fed into a model. The data is then fed into the input layer of the Modified GCN with Temporal Features Network (MGCN-TFNet). Graph Convolutional Network block is where spatial correlation-based patterns of structural data are learned for entities like users, accounts, and transactions. Structural feature embeddings are next used to represent descriptions of intricate transaction patterns. Temporal attention layers that are targeting salient time-based features and labelling salient transactions with respect to weights over various intervals of time are then used by the system. These temporal attributes are being used in conjunction with the structural embeddings of the temporal-structural embeddings integration layer to combine both spatial and temporal information for even better fraud detection. The data is then sent through a fully connected layer again for additional fine-tuning, and the final output is predicted by a SoftMax classifier that classifies transactions as Financial Fraud Detection or Financial Fraud Not Detection. This method successfully combines structural learning and temporal pattern discovery to identify illegal activity in financial transactions.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 607-614 www.ijaem.net ISSN: 2395-5252

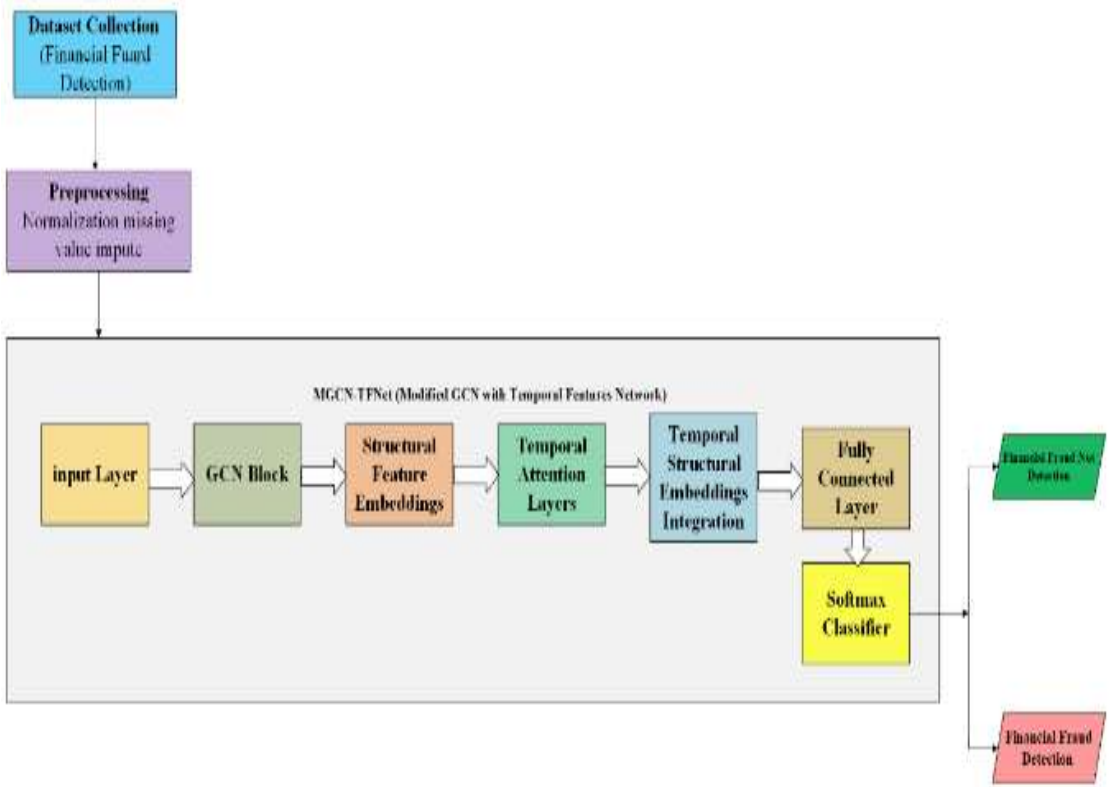

Figure 1 Architecture Diagram

3.1 Data Preprocessing

The data must undergo pre-processing before Graph Convolutional Networks (GCNs) and Temporal Attention can be applied for fraud detection purposes. The data processing workflow consists of two main operations which are normalization and missing value treatment. Data normalization ensures all features have standardized scales while missing value imputation fills empty data points to resolve gaps in the information. The data preparation along with model performance enhancement requires these essential steps.

3.2 Normalization

The normalization technique transforms numerical attributes into a standardized scale. The technique serves to stop attributes with extensive value ranges from dominating the learning process. Min-Max Scaling stands as one of the most common normalization techniques because it transforms data values into the [0,1] or [-1,1] range. The formula for Min-Max normalization appears as follows:

$$x_{norm} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

The normalization process requires original feature value x together with minimum and maximum feature values min(x) and max(x) to produce normalized value x_{norm} .

The normalization scales all data equally so features of varying ranges do not affect the modelling process. Min-Max normalization applies to features with transaction amount and time scales that differ greatly by adjusting their ranges to maintain proportionality between large and small values.

3.3 Missing Value Imputation

The analysis of real-world datasets contains numerous missing data points which machine learning models require appropriate management since they do not operate with null or NaN values. The replacement of missing values through useful estimates constitutes the imputation process. The multiple imputation techniques include mean/median imputation and KNN imputation which provide distinct methods to calculate and substitute missing data values.

a) Mean/Median Imputation

The replacement of missing numerical values by their feature means or median works as a simple method for imputation. The method helps prevent bias from entering the feature because of missing values. Mean imputation follows this mathematical formula:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 607-614 www.ijaem.net ISSN: 2395-5252

$$x_{imputed} = \frac{\sum_{i=1}^{n} x_i}{n} \quad (2)$$

Where, x_i are the observed values of the feature, nis the number of non-missing values, $x_{imputed}$ is the imputed value for the missing entry.The median proves more appropriate than the mean for biased data because outliers have less influence on the median. The use of median analysis helps to protect the integrity of data.

3.4 MGCN-TFNet (Modified GCN with Temporal Features Network)

MGCN-TFNet is a cloud banking system fraudulent behavior detection model that employs Modified Graph Convolutional Networks and Temporal Features. It employs graph learning for discovering rich relationships between entities such as users, accounts, transactions, and devices. The Modified GCN enhances the capacity of the model to handle complex interrelated data sets. The Temporal Features module applies Temporal Attention in the tracking of transactions over time with emphasis on relevant time periods that can point towards fraudulent transactions. The hybrid framework improves the precision, adaptability, and extensibility of the model in developing a stable real-time fraud detection system in advanced banking setups.

3.5 Graph Convolutional Networks (GCN)

GCNs serve as a powerful method of data extraction in banking use cases to handle complex interconnected data sets which encompass transactions along with accounts users and devices. Fraud detection is enhanced by GCNs due to the fact that they identify entity relations through nodes and edges that symbolize these entities. The feature propagation mechanism in GCNs has two operations that preserve node features and maintain connection topology. The model applies this mechanism to discover connections among data points that would be non-visible when the data appears in isolated groups. The bank system realizes optimal fraud pattern detection ability through its GCN-based implementation for feature learning. The GCN system learns the most important data features automatically without being affected by fluctuating patterns in data.

$$N^{(l+1)} = \sigma\left(WN^{(l)}P^{(l)}\right) \quad (3)$$

Where;

$N^{(l)}$ is the feature matrix at layer l,W is the normalized adjacency matrix of the graphs, $P^{(l)}$ is the weight matrix of layer l, σ is an activation function.

3.6 Structural Feature Embeddings

Graph structure remains understandable through these embeddings because they transform entity relationships into lower dimensional vectors which improves machine learning model ability to comprehend the data. Structural feature embeddings enable the model to identify potential fraud activities by processing the connections between different accounts or transactions. The identification of linked financial accounts or devices with parallel suspicious activities happens through the analysis of graph-based structural representations. The system benefits from encoding intricate business associations into feature embeddings which help uncover hidden fraud indicators that older data evaluation techniques fail to identify thus achieving better performance in banking fraud prevention.

3.7 Temporal Attention Layer

The Temporal Attention Layer serves as a fundamental element to detect temporal patterns in sequential data which finds its most prominent use in fraud detection in banking systems that reveal changing transaction behavior. The model focuses on particular time-series data sections through this layer by applying different attention scores to various time intervals. The model uses this layer to identify the most important transactions by analyzing their time-based characteristics and monetary values and transaction frequencies because these elements indicate possible fraud. The Temporal Attention Layer detects suspicious activities through its ability to learn about sudden large withdrawals that occur from various locations within short timeframes. The model achieves better fraud detection capability through adjustable attention weights across timespans that helps detect new activity patterns and anomalies which emerge over time thus advancing the system results for fraud systems operating in environments with temporal complexity.

$$\alpha_t = \frac{\exp(\text{LeakyReLu}(H[h_{t-1}, x_t]))}{\sum_t \exp(\text{LeakyReLu}(H[h_{t-1}, x_t]))} \quad (4)$$

Where;

h_{t-1} is the previous hidden state from the RNN, x_t represents the transaction feature at the time step t, H is a learnable weight matrix.

3.8 Temporal-Structural Embeddings

The Temporal-Structural Embeddings Integration is applied to analyze intricate patterns of sequential and relational data with the use of the combination of strength-based temporal and structural feature embeddings. The integration framework is very effective in identifying bank

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 607-614 www.ijaem.net ISSN: 2395-5252

fraud since it deals with temporal patterns and relations between devices and users, accounts and transactions. Temporal embeddings are employed by embedding techniques to recognize patterns of changes in behavior through time but structural embeddings reveal interaction patterns between entities. The two processes enable the two embedding methodologies to build high-level understandings that integrate structures of transaction sequences and entity interaction structures. The collaborative approach identifies more sophisticated patterns of fraud better by detecting anomalous time-related behavior with sudden behavior changes and dysfunctional relational relationships such as the use of a shared device or connected accounts. The model identifies more sophisticated patterns of fraud that combine temporal and structural anomalies with Temporal-Structural Embeddings Integration.

3.9 Fully Connected Neural Network (FCNN)

Both relational (GCN) and Temporal Attention fraud patterns are extracted before a fully connected neural network (FCNN) with SoftMax classifier determines transaction fraud. The calculation of the final classification probability requires:The learned weights and biases are denoted as Wand b.

$$P(y = \text{fraud} \mid X) = \frac{\exp(WX + b)}{\sum_c \exp(W_c X + b_c)} \quad (5)$$

IV. RESULT AND DISCUSSION:

This section presents the online bank fraud detection performance of new MGCN-TFNet (Modified Graph Convolution Network with Temporal Features Network) model. This model is tried on the Pay Sim dataset and compared based on key performance measurements such as precision, recall, accuracy, and F1-score. The conclusion validates that the MGCN-TFNet model performs better than such legacy models with more precise detection, reduced false alarms, and high scalability. The findings validate the model performance in real-time fraud detection to demonstrate its capability to handle crafty patterns of fraud and its ability to handle crafty fraudulent behavior appropriately.

4.1 Datasets Description:

A financial fraud detection dataset [21] is a collection of fraud detection transaction data and features. It contains transaction data, user and account data, fraud labels, behavioral features, temporal and context features, aggregated user behavior features, and abnormal behavior signs. They assist in evaluating abnormal behavior deviations and suspicious activity. Some of the financial fraud detection datasets include Credit Card Fraud Detection Dataset, IEEE-CIS Fraud Detection Dataset, and Kaggle's Credit Card Fraud Detection Dataset. These datasets are applied in detecting fraudulent transactions and offer useful information to companies for avoidance and minimization of financial risk.

4.2 Confusion matrix:

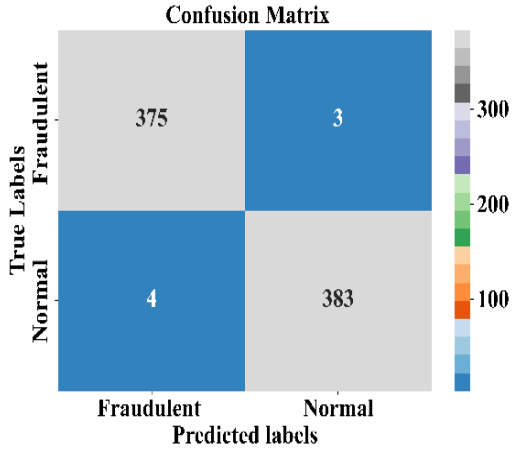

Figure 2 Confusion matrix

Confusion matrix is a method to measure the performance of a fraud detection model's classification. It is between true fraud and regular transaction labels and predicted labels. The matrix reveals that 375 fraud transactions are recognized as fraud and 383 normal transactions are well predicted as normal. Three normal transactions are labeled as fraud and four fraud transactions as normal by the model. The scale of color represents the frequency of each category with higher values in darker shades. The matrix gives a snapshot of model performance in predicting valid transactions and fraudulent ones and those requiring an improvement.

4.3 Performances Metrics

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 03 Mar. 2025, pp: 607-614 www.ijaem.net ISSN: 2395-5252

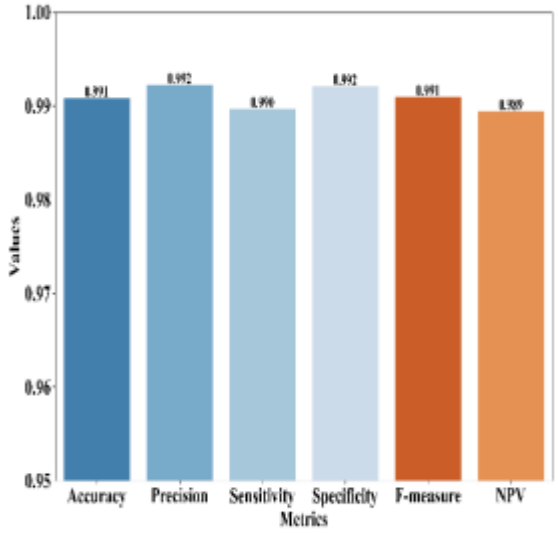

Figure 3 Performances Metrics

The graph 3 shows a classification model that is used for fraud detection performing several performance measures. The model is precise to 0.991, meaning that it correctly identifies 99.1% of the transactions. Its precision is 0.992, meaning that 99.2% of the transactions labeled as fraudulent by the model are actually fraudulent. Sensitivity is 0.990, indicating that 99.0% of actual fraud transactions were correctly detected. The model achieves a precision of 0.992, having correctly identified 99.2% of the normal transactions. Finally, the value of NPV (Negative Predictive Value) is 0.939, indicating that the model is accurately classifying 93.9% of the predicted ones as normal out of all predicted ones. In general, the graph indicates how the model is performing really well on most aspects with high recall and precision and high capability to classify fraud transactions accurately.

V. CONCLUSION

In conclusion, the suggested framework to detect financial fraud efficiently combines temporal pattern discovery with structural learning for effectively detecting fraudulent transactions. The framework incorporates a sequence of powerful techniques like Graph Convolutional Networks (GCNs), temporal attention layers, and integration of temporal-structural embeddings to ultimately improve fraud detection through spatial and temporal pattern learning in transaction information. The confusion matrix indicates that the model is working effectively, correctly classifying both the fraudulent and legitimate transactions with a bit of misclassifications. The performance measures indicate that the model possesses an immensely high accuracy (0.991), precision (0.992), sensitivity (0.990), specificity (0.992), F-measure (0.991), and NPV (0.939), demonstrating its effectiveness at detecting fraud and having high performance using various metrics. Overall, the model presented is demonstrated to be effective in detecting fraudulent activity, thus proving to be a valid instrument in detecting financial fraud.

REFERENCES

[1] B. Kadiyala, S. K. Alavilli, R. P. Nippatla, S. Boyapati, and C. Vasamsetty, “Integrating Multivariate Quadratic Cryptography with Affinity Propagation for Secure Document Clustering in IoT Data Sharing,” International Journal of Information Technology and Computer Engineering, vol. 11, no. 3, pp. 163–178, Oct. 2023.

[2] J. Zhao and W. Li, “The Impact of Digital Finance on the Urban–Rural Income Gap in China: The Mediating Role of Employment Structural Transformation,” Sustainability, vol. 16, no. 19, Art. no. 19, Jan. 2024, doi: 10.3390/su16198365.

[3] S. K. Alavilli, B. Kadiyala, R. P. Nippatla, and S. Boyapati, “A Predictive Modeling Framework for Complex Healthcare Data Analysis in The Cloud Using Stochastic Gradient Boosting, Gams, Lda, And Regularized Greedy Forest,” International Journal of Information Technology and Computer Engineering, vol. 12, no. 6, 2023.

[4] S. K. Alavilli, “Innovative Diagnosis Via Hybrid Learning and Neural Fuzzy Models On A Cloud-Based IoT Platform,” Journal of Science & Technology (JST), vol. 7, no. 12, Art. no. 12, Dec. 2022.

[5] C. Vasamsetty, “IJORET | Volume 7 - Issue 1,” IJORET.com. Accessed: Mar. 11, 2025. [Online]. Available: http://ijoret.com/Volume7-issue1.html

[6] B. Kadiyala and H. Kaur, “Dynamic Load Balancing and Secure IoT Data Sharing Using Infinite Gaussian Mixture Models and Plonk,” International Journal of Information Technology and Computer Engineering, vol. 7, no. 2, 2023.

[7] R. P. Nippatla, “AI and ML-Driven Blockchain-Based Secure Employee Data Management: Applications of Distributed Control and Tensor Decomposition in HRM,” International Journal of Engineering

Research and Science & Technology, vol. 15, no. 2, pp. 1–16, Jun. 2019.

[8] S. B. H. Gollavilli, K. Gattupalli, H. Nagarajan, P. Alagarsundaram, and S. R. Sitaraman, "Innovative Cloud Computing Strategies for Automotive Supply Chain Data Security and Business Intelligence," International Journal of Information Technology and Computer Engineering, vol. 11, no. 4, pp. 259–282, Oct. 2023.

[9] D. T. Valivarthi and T. Leaders, "Fog Computing-Based Optimized and Secured IoT Data Sharing Using CMA-ES and Firefly Algorithm with DAG Protocols and Federated Byzantine Agreement," International Journal of Engineering, vol. 13, no. 1, 2023.

[10] C. Vasamsetty, "Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends," International Journal of Information Technology and Computer Engineering, vol. 8, no. 2, 2020.

[11] C. Vasamsetty and H. Kaur, "Optimizing Healthcare Data Analysis: A Cloud Computing Approach Using Particle Swarm Optimization with Time-Varying Acceleration Coefficients (PSO-TVAC)," Journal of Science & Technology (JST), vol. 6, no. 5, Art. no. 5, Sep. 2021.

[12] B. Kadiyala, S. K. Alavilli, R. P. Nippatla, S. Boyapati, C. Vasamsetty, and H. Kaur, "An IoMT-Based Surgical Monitoring System for Automated Image Synthesis and Segmentation Using Reinforcement Learning and DCGANs," in 2024 International Conference on Emerging Research in Computational Science (ICERCS), Dec. 2024, pp. 1–6, doi: 10.1109/ICERCS63125.2024.10895115.

[13] S. K. Alavilli, "Integrating Computational Drug Discovery with Machine Learning for Enhanced Lung Cancer Prediction," International Journal of Information Technology and Computer Engineering, vol. 11, no. 9726, 2023.

A. Nithya, M. Yashwanth, K. P. D. Anand, and M. NaveenKumar, "A Real-Time Video Streaming Platform for Device to Mobile Networking," International Journal of Information Technology and Computer Engineering, vol. 5, no. 2, 2020.

[14] R. P. Nippatla, "A Robust Cloud-Based Financial Analysis System Using Efficient Categorical Embeddings with CatBoost, ELECTRA, t-SNE, and Genetic Algorithms," International Journal of Engineering, vol. 13, no. 3, 2023.

[15] S. K. Alavilli, "Smart Networks and Cloud Technologies: Shaping The Next Generation Of E-Commerce And Finance," International Journal of Information Technology and Computer Engineering, vol. 6, no. 3, 2018.

[16] R. P. Nippatla, "A Secure Cloud-Based Financial Analysis System for Enhancing Monte Carlo Simulations and Deep Belief Network Models Using Bulk Synchronous Parallel Processing," International Journal of Information Technology and Computer Engineering, vol. 6, no. 3, pp. 89–100, Jul. 2018.

[17] S. Boyapati, "Assessing Digital Finance as a Cloud Path for Income Equality: Evidence from Urban and Rural Economies," International Journal of Information Technology and Computer Engineering, vol. 8, no. 3, 2020.

[18] S. Boyapati, "Bridging the Urban-Rural Divide: A Data-Driven Analysis of Internet Inclusive Finance in the E-Commerce Era," International Journal of Engineering, vol. 11, no. 1, 2023.

[19] S. Boyapati and H. Kaur, "Mapping the Urban-Rural Income Gap: A Panel Data Analysis of Cloud Computing and Internet Inclusive Finance in the E-Commerce Era," International Journal of Information Technology and Computer Engineering, vol. 7, no. 4, 2022.

[20] smmmmmmmmm, "Financial Fraud Detection." Accessed: Mar. 11, 2025. [Online]. Available: https://www.kaggle.com/datasets/smmmmmmmmmmm/financial-fraud-detection