International Journal of Science and Engineering Applications
Volume 14-Issue 03, 51 – 57, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1011

Fraud Detection with Variational Autoencoders and Transformer Networks: A Robust Deep Learning Approach for Banking Transactions

Karthikeyan Parthasarathy[1]
LTIMindtree, Florida, USA

Naresh Kumar Reddy Panga[3]
Virtusa Corporation, New York, USA

Ramya Lakshmi Bolla[5]
ERP Analysts,Ohio, USA

Rajeswaran Ayyadurai[2]
IL Health & Beauty Natural Oils Co Inc, California, USA

Jyothi Bobba[4]
Lead IT Corporation, Illinois, USA

R Pushpakumar[6*]
Assistant Professor,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, Chennai, India

Abstract: Financial fraud is a serious threat in online banking, requiring sophisticated and responsive fraud detection systems. Rule-based systems and machine learning algorithms are at a loss in dealing with high-dimensional financial information, resulting in higher false positives and undetected fraudulent activities. To tackle these issues, this research recommends a hybrid framework for fraud detection combining Variational Autoencoders (VAE) for detecting anomalies and Transformer networks for fraud classification. VAE is trained on learning the distribution of valid transactions and identifies outliers according to the errors in reconstruction, whereas Transformer neural network employs self-attention processes to make class predictions with high accuracy. Performance is also analyzed on PaySim dataset to identify 99.48% accuracy, 99.39% precision, 99.55% recall, and minimum 0.599% false positives, clearly exceeding the efficiency of conventional machine learning classifiers. The framework under consideration increases fraud prevention mechanisms through adaptive learning functionality, scalability, and real-time transactional monitoring.

Keywords*:* Fraud Detection, Variational Autoencoder (VAE), Transformer Networks, Digital Banking, Anomaly Detection, Financial Security.

1. INTRODUCTION

The accelerated digital revolution of financial services has resulted in a boom in online transactions, thus making digital banking an essential aspect of the global economy. As cloud-based financial systems, smart networks, and sophisticated e-commerce platforms emerged, banking activities have become efficient and accessible [1]. Digital finance has closed economic divides by enhancing financial inclusion, particularly in rural and underserved communities, enabling users to access banking services effortlessly [2]. The use of cloud computing and Internet of Things (IoT) in financial transactions has facilitated real-time processing of transactions, [3] but it has also made banking systems vulnerable to advanced cyber-attacks, notably fraud.

Financial fraud, including identity theft, account takeovers, and unauthorized transactions, has been a growing issue [4]. The networked environment of modern banking, powered by AI-based financial analysis and blockchain-based secure transactions, has presented new security challenges [5]. Rule-based systems and static machine learning models, the traditional fraud detection methods, have a tendency to miss complex fraudulent attacks and yield high false positives and delayed fraud detection.

The rapid growth in online banking has significantly increased the risk of financial fraud due to various reasons behind it. The high volume of transactions done on a daily basis makes real-time identification of fraud an uphill task. Cyber attackers continue to evolve their techniques, with the use of deepfake identity fraud, top-level phishing scams, and artificial intelligence-based cyber-attacks to breach security systems [6]. Further, financial systems that are cloud-based, since they optimize transactional efficiency, come with unique security risks that cybercriminals are likely to exploit. Further, data breaches and insider attacks due to inadequate security controls are likely to result in unauthorized access of confidential financial information, enabling fraudulent transactions [7].

Conventional fraud detection methods have serious shortcomings and are therefore unable to cope with new fraud patterns. Rule-based systems depend on pre-programmed patterns that are not adaptable, resulting in high false positives and undetected fraud cases[8]. Static machine learning models also need constant retraining to keep pace with changing fraud strategies. Scalability is also a serious issue, as traditional models are not able to handle the growing number of financial transactions effectively [9]. Additionally, general anomaly detection methodologies are typically insensitive to weakly correlated fraudulent behaviors in multi-dimensional transaction records and hence have minimal impact on high-complexity banking operations [10].

For alleviating the Financial Fraud Detection Challenges, we develop a new hybrid model that marries Self-Organizing Maps (SOM) and Deep Neural Networks (DNN). The SOM system undertakes an unsupervised clustering operation for aggregating transaction behavior into coherent patterns, meaning the system could detect anomalies independently of labeled fraudulent data. Next, the clustered representations are utilized as input in the DNN classifier to provide predictions of the legitimacy or the fraudulent nature of the transactions based on high responsiveness to changing fraudulent patterns. This hybrid architecture enhances scalability and performance, making it appropriate for cloud banking systems to identify fraud in real-time. In comparison to other rule-based and static ML architectures [11], our method reduces false positives with better accuracy in fraud detection through dynamic learning. Additionally, the integration of deep learning with secure cloud-based banking systems enhances security, flexibility, and real-time fraud detection, protecting sensitive banking data from cyber-attacks [12]. By applying SOM for anomaly detection and DNN for classification, the suggested method offers a scalable, high-precision, and adaptive fraud detection system that ensures strong resilience against emerging cyber-attacks in digital banking.

2. LITERATURE SURVEY

The increasing digitization of financial transactions demands robust cryptographic techniques to ensure data privacy and discourage unlawful access. [13] suggested a decentralized cryptographic framework, integrating isogeny-based hybrid cryptography, anisotropic random walks (ARW), and decentralized cultural co-evolutionary optimization (DCCO) to adaptively control security mechanisms against cyber-attacks. Leveraging this, [14] proposed a dynamic load-balancing system based on Infinite Gaussian Mixture Models (IGMM) and PLONK-based zero-knowledge proofs for secure, scalable data dissemination in financial networks. [15] also examined a hybrid cryptosystem key generation technique through the combination of Multi-Swarm Adaptive Differential Evolution (MSADE) and Gaussian Walk Group Search Optimization (GWGSO) to enhance the strength of encryption in Super singular Elliptic Curve Isogeny Cryptography (SSEIC). These cryptological advancements emphasize the importance of optimization-based encryption procedures in protecting financial transactions and countering fraud risks within e-banking.

Clustering methods have been extensively utilized to identify suspicious transactions by identifying behavioral patterns and outliers in financial information. [16] proposed a hybrid clustering technique, combining DBSCAN and Fuzzy C-Means clustering with Artificial Bee Colony-Differential Evolution (ABC-DE) for safe data sharing in fog computing systems. The method maximized the efficiency of clustering and facilitated dynamic resource allocation to enhance the detection of transaction anomalies. Further, [17] suggested an anomaly detection framework using Reinforcement Learning (RL) and Deep Convolutional Generative Adversarial Networks (DCGANs) in an IoMT-based surgical monitoring system. Although initially used for medical image segmentation, their approach showed the strength of self-learning models to constantly learn over changing patterns—a key characteristic for fraud detection in banking transactions. By using unsupervised clustering in addition to deep learning-based anomaly detection, such methods help enhance fraud detection systems used in financial contexts.

Deep learning algorithms have increasingly been used in predictive analytics to detect fraud by utilizing adaptive learning methods to identify transactional abnormalities. [18] proposed an optimization-based deep learning model based on Particle Swarm Optimization with Time-Varying Acceleration Coefficients (PSO-TVAC) to facilitate improved healthcare data analysis in cloud computing. The authors optimized deep neural networks (DNNs) through adaptive acceleration parameter modifications, enhancing the efficiency of classification in high-dimensional data. Likewise, [19] investigated decision tree-based predictive modeling for the optimization of clinical pathways in cardiology using crowdsourced patient data to optimize classification algorithms—a method that is congruent with fraud detection in banking through the use of real-time pattern learning. In addition, [20] designed a cloud-based predictive modeling system, incorporating Stochastic Gradient Boosting (SGB), Generalized Additive Models (GAMs), Latent Dirichlet Allocation (LDA), and Regularized Greedy Forest (RGF) to overcome scalability and sparsity issues in data. These research papers affirm the contribution of ensemble learning methods and deep neural networks towards improving fraud detection systems in financial systems.

The literature reviewed points to the evolution from cryptographic security measures to cluster-based anomaly detection and predictive deep learning frameworks. While cryptographic approaches target securing transaction information, cluster- and pattern-detection methods boost real-time fraud detection. In contrast, deep learning frameworks use adaptive feature extraction to enhance detection of sophisticated patterns of fraud. This work builds on these developments by combining Variational Autoencoders (VAE) and Transformer Networks, taking advantage of their latent space representations and self-attention to attain high-accuracy fraud classification in online banking.

2.1 PROBLEM STATEMENT

The rise in quantity and complexity of financial transactions via online banking have raised the challenge of detecting fraud. Rule-based and static machine learning-based approaches are insufficient as fraud detection systems since they are unable to adapt to the evolving nature of fraudulent schemes, hence producing high false positives and allowing concealed fraudulent patterns to go unnoticed [21]. Cybercriminals employ

sophisticated methods such as deepfake identity theft, AI-phishing, and transactional obscuration to bypass conventional security. Furthermore, conventional anomaly detection techniques fail to detect weakly correlated fraudulent patterns in high-dimensional transaction data, limiting their effectiveness in real-time fraud detection [22]. This study, therefore, proposes a hybrid Variational Autoencoder (VAE) and Transformer fraud detection model utilizing unsupervised feature learning and attention-based classification for enhanced accuracy in fraud detection, minimization of false positives, and adjustability to novel fraud patterns within digital banking [23].

3. METHODOLOGY

The VAE + Transformer-based fraud detection model utilizes a two-stage anomaly detection and classification mechanism to detect fraudulent financial transactions. Initially, transaction information from the PaySim dataset is preprocessed, comprising missing value treatment, normalization, and categorical encoding, to achieve data consistency. The Variational Autoencoder (VAE) Encoder Layer maps transactions into a latent space representing underlying distribution patterns, and the VAE Decoder Layer reconstructs the original input. The error in reconstruction is calculated, wherein the greater values of error indicate suspicious transactions. The Transformer Encoder Block, coupled with multi-head self-attention, layer normalization, and position encoding, performs even more stringent fraud detection through the learning of contextual dependencies of transactions. The final fraud probability score is obtained using a fully connected layer activated with softmax, eventually classifying transactions as legitimate or fraudulent. The overall design, which integrates unsupervised feature learning (VAE) with context-aware classification (Transformer), provides strong real-time fraud detection. Figure 1 shows the entire architecture of the proposed model.

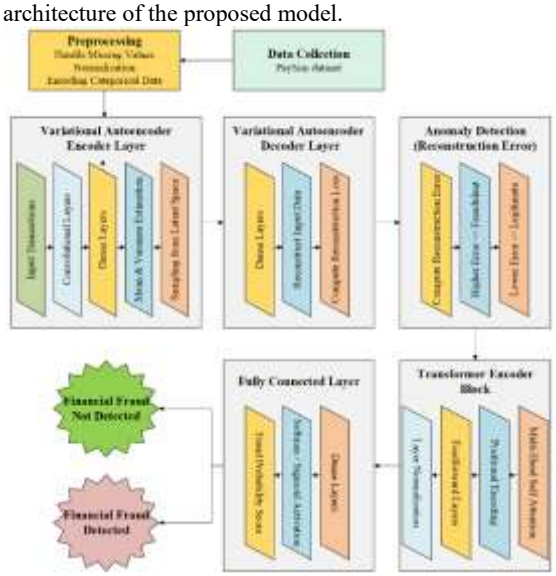

Figure 1: Architecture Diagram

3.1. Data Preprocessing

Data preprocessing is a critical process to provide high-quality input to the deep learning model. It includes missing data handling, numerical value normalization, and categorical feature encoding. These processes assist in minimizing data inconsistencies and enhancing the performance of the Variational Autoencoder (VAE) and Transformer-based fraud detection system.

3.1.1. Handling Missing Data

Missing values result in incorrect predictions and bias during fraud detection. Numerical missing values are substituted with mean imputation to preserve data distribution consistency. Categorical missing values are treated with mode imputation to ensure the most common category is used. This avoids data sparsity and improves model learning.

For missing numerical values, mean imputation is used:

$$X_{\text{new}} = \frac{1}{n}\sum_{j=1}^{n} X_j \quad (1)$$

For categorical values, mode imputation is applied:

$$X_{\text{new}} = \arg\max P(X = k) \quad (2)$$

3.1.2. Normalization (Min-Max Scaling)

To make transaction features into a comparable range, Min-Max Scaling is used. This scaling normalizes the number of transactions and the timestamps so that no feature overpowers another because of scale imbalances. Normalization also speeds up model convergence and helps avoid large numbers from skewing learning dynamics within the deep learning model.

To scale transaction amounts and timestamps:

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (3)$$

Where X is the original value, and $X_{\min}$, $X_{\max}$ are the minimum and maximum values.

3.1.3. Categorical Encoding (One-Hot Encoding)

Categorical variables, such as transaction types, must be converted into numerical representations for model training. One-hot encoding is used to transform categorical values into binary vectors, preserving unique transaction characteristics without introducing ordinal relationships. This helps in better capturing transaction behaviors within the fraud detection framework.

For categorical transaction types:

$$X_{\text{onehot}} = [x_1, x_2, \ldots, x_k] \quad (4)$$

Where k is the number of unique categories.

3.2. Variational Autoencoder (VAE) for Anomaly Detection

The Variational Autoencoder (VAE) is trained to learn the distribution of valid transactions and detect suspicious transactions based on reconstruction errors. It has an encoder that reduces input transactions into a latent representation and a decoder that reconstructs them. Suspect transactions that significantly differ from learned normal behaviors result in increased reconstruction errors. This allows unsupervised detection of fraud effectively without the need for labeled fraudulent data.

3.2.1. VAE Encoder

The encoder is used to map input transactions into a lower-dimensional latent space. The encoder learns transaction feature mean and variance and adds a small random perturbation in order to have diversity. This stochastic encoding will make the model generalize well on unseen data with retaining important transaction patterns.

The encoder compresses the transaction input X into a latent space:

$$z = \mu + \sigma \cdot \epsilon, \epsilon \sim \mathcal{N}(0,1) \quad (5)$$

Where, μ is the mean vector σ is the standard deviation vector ϵ is a random noise term.

3.2.2. VAE Decoder

The decoder reconstructs the original transaction from its underlying representation. An adequately trained decoder reconstructs valid transactions correctly, while invalid transactions lead to inaccurate reconstruction. The reconstruction error difference between the original and reconstructed transaction identifies fraud instances in the dataset.

The decoder reconstructs the input transaction X' from the latent representation:

$$X' = f_\theta(z) \quad (6)$$

3.2.3. Reconstruction Loss (Anomaly Detection)

Reconstruction loss refers to how good the decoder reconstructs the input transactions. The transaction is labeled as an anomaly if it varies greatly from the reconstructed transaction. The more elevated the reconstruction loss, the more likely a fraudulent transaction is. A low loss implies a typical transaction. This allows the model to pick up on anomalous behaviors.

VAE minimizes the reconstruction loss to measure how well the input is reconstructed:

$$\mathcal{L}_{rec} = X - X'2 \quad (7)$$

where a higher reconstruction error indicates anomalous transactions (potential fraud).

3.2.4. Kullback-Leibler (KL) Divergence Loss

KL divergence loss guarantees that the learned latent space is close to a normal distribution. This discourages overfitting and leads the model to allocate transaction representations in an efficient manner. By reducing KL divergence, the VAE guarantees that the latent space represents significant variations in transaction patterns, enhancing fraud detection robustness.

To ensure a meaningful latent space, KL-divergence loss is applied:

$$\mathcal{L}_{\text{KL}} = D_{\text{KL}}(q(z \mid X) \| p(z)) \quad (8)$$

Where, $p(z)$ is the prior normal distribution, ensuring regularization.

3.2.5. Total VAE Loss

The VAE's total loss function is a combination of reconstruction loss and KL divergence. This balance is such that the model reconstructs normal transactions well while keeping the latent space well-organized. The weighted sum of these losses enables the model to distinguish between fraudulent and legitimate transactions effectively.

$$\mathcal{L}_{\text{VAE}} = \mathcal{L}_{\text{rec}} + \beta \mathcal{L}_{\text{KL}} \quad (9)$$

Where, β controls the regularization strength.

3.3. Transformer Network for Fraud Classification

The Transformer model improves fraud detection through the analysis of long-distance dependencies in sequential transaction data. The Transformer does not use recurrent models, as it utilizes self-attention mechanisms to dynamically weight the significance of varying transaction features. This enables the model to recognize intricate transactional relationships and provide more accurate fraud classification. Integrating the Transformer with the VAE, it ensures flagged anomalies are labeled with greater precision and reliability.

3.3.1. Multi-Head Self-Attention Mechanism

Multi-head self-attention allows the model to attend to multiple aspects of transactions at once. It places attention weights on descriptive features that point to key fraud indicators. With the learning of intricate relationships between transactions, the mechanism boosts the accuracy of classification and makes the detection of fraudulent activities more efficient.

The Transformer captures relationships between sequential transactions:

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (10)$$

Where, Q, K, V are query, key, and value matrices derived from transaction embeddings, d_k is the dimensionality of the key vectors.

3.3.2. Multi-Head Attention (MHA)

Multi-head attention also enhances the Transformer's capability to identify fraud by considering multiple representations of transactions. Each attention head examines various fraud features and provides a comprehensive insight into transaction behavior, making the model flexible to learn new fraud tactics in a dynamic manner.

To allow multiple perspectives in analyzing transactions:

$$\text{MHA}(Q, K, V) = \text{Concat}(\text{head}_1, \ldots, \text{head}_h)W_O \quad (11)$$

where each attention head is:

$$\text{head}_i = \text{Attention}\left(QW_i^Q, KW_i^K, VW_i^V\right) \quad (12)$$

3.3.3. Fully Connected Layer & Fraud Probability Prediction

The features are extracted with attention mechanisms afterwards, and a final classification is conducted via a fully connected layer. Sigmoid activation function is used to calculate fraud probability. Higher probability transactions are marked as fraudulent, while lower probability suggests a valid transaction. This makes the decision highly accurate.

After Transformer processing, the final classification layer computes:

$$y = \sigma(W_o h_T + b_o) \quad (13)$$

Where, $\sigma(x) = \frac{1}{1+e^{-x}}$ ensures output between 0 and 1 (fraud probability). h_T is the final hidden state representation.

3.4. Fraud Decision Based on Thresholding

A fraud risk score is determined for every transaction that assists the system in determining if a transaction is fraudulent. A transaction is flagged as fraud when the fraud probability is higher than a set threshold. The use of a threshold-based classification supports flexibility to varying levels of fraud risk in bank transactions.

A fraud risk score is computed for each transaction:

$$\text{Risk Score} = \frac{1}{T}\sum_{i=1}^{T} y_i \quad (14)$$

Where T is the number of transactions analyzed.

If the fraud probability exceeds a threshold (τ), the transaction is flagged as fraud:

International Journal of Science and Engineering Applications
Volume 14-Issue 03, 51 – 57, 2025, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1403.1011

$$\text{Fraud} = \begin{cases} 1, & \text{if Risk Score} \geq \tau \\ 0, & \text{otherwise} \end{cases} \quad (15)$$

3.5. Loss Function & Optimization

The model is trained with an adaptive loss function and optimization approach to provide efficient fraud detection while addressing the issue of class imbalance.

Fraudulent transactions are few in number as opposed to valid transactions, so the use of weighted cross-entropy loss is necessary. This loss function gives greater weight to fraudulent transactions so that the model will not be skewed toward non-fraud cases. This will promote balanced learning and better fraud detection.

To handle imbalanced fraud detection, Weighted Cross-Entropy Loss is used:

$$\mathcal{L} = -w_{\text{pos}} y \log(y) - w_{\text{neg}}(1 - y)\log(1 - y) \quad (16)$$

Where, $w_{\text{pos}}, w_{\text{neg}}$ are weights for fraud and non-fraud classes.

3.6. Optimization: Adam

The Adam optimizer is utilized to efficiently update model parameters. It incorporates momentum and adaptive learning rates to speed up convergence while avoiding overfitting. The adaptive nature of Adam guarantees stable learning across various types of transactions, enhancing fraud detection performance with time.

The model is trained using the Adam optimizer, updating parameters as:

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t \quad (17)$$

$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2 \quad (18)$$

$$\theta_t = \theta_{t-1} - \frac{\alpha}{\sqrt{v_t} + \epsilon} m_t \quad (19)$$

Where, m_t, v_t are momentum terms, θ_t are the model parameters updated at step t.

4. RESULT AND DISCUSSION

4.1. Dataset Description

The PaySim dataset [24] models mobile money transactions for 30 days, drawn from financial logs of a mobile service in a country in Africa. It has 744 hourly steps and has transaction type (CASH-IN, CASH-OUT, DEBIT, PAYMENT, TRANSFER), amount, and customer identifiers (nameOrig, nameDest). Fraudulent transactions are labeled as isFraud, and high-value unauthorized transfers are indicated with isFlaggedFraud. Some columns such as balances are not used for fraud detection, since fraudulent transactions are reversed.

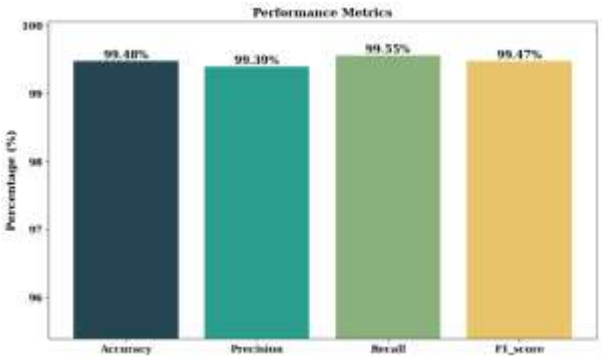

Figure 2: Performance Metrices

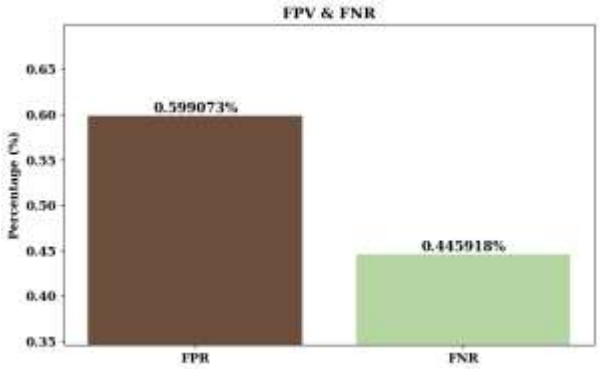

Figure 3: Performance of FPR and FNR

The DCAE model proposed here is 99.48% accurate, guaranteeing high classification efficiency. With 99.39% precision, it reduces false positives to a minimum, while a 99.55% recall guarantees most fraud cases are caught. The 99.47% F1-score attests to the strong precision-recall balance, demonstrating the robustness of the model. Figure 2 shows the Performance Metrices.

Low FPR (0.599%) prevents incorrect fraud signals from leading to blocking of transactions and a low FNR (0.446%) minimizes missed cases of fraud. Such low errors establish the robustness of the model to identify fraudulent activities correctly. Figure 3 shows the FPR and FNR.

5. CONCLUSION

The VAE + Transformer-based fraud detection model proposed works well in boosting fraud identification in electronic banking using unsupervised anomaly detection and self-attention-based classification. With 99.48% accuracy and lower false positive rates, the model proves to be better fraud detection compared to the conventional technique. Owing to a small amount of computational overhead but with high scalability, flexibility, and real-time monitoring potential, it is an effective solution to current financial safety. Subsequent work will concentrate on continued optimization of model effectiveness and its translation into real-world banking settings.

REFERENCES

[1] S. K. Alavilli, "Smart Networks And Cloud Technologies: Shaping The Next Generation Of E-Commerce And Finance," vol. 12, no. 4.

[2] 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, 2021.

[3] S. Boyapati, "Assessing Digital Finance as a Cloud Path for Income Equality: Evidence from Urban and Rural Economies," vol. 8, no. 3, 2020.

[4] 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.

[5] S. Boyapati, "The Impact of Digital Financial Inclusion using Cloud IOT on Income Equality: A Data-Driven Approach to Urban and Rural Economics," vol. 7, no. 9726, 2019.

[6] 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.

[7] 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," vol. 7, no. 4, 2022.

[8] R. P. Nippatla, "A Robust Cloud-based Financial Analysis System using Efficient Categorical Embeddings with Cat Boost, ELECTRA, t-SNE, and Genetic Algorithms," *International Journal of Engineering*, vol. 13, no. 3, 2023.

[9] 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.

[10] H. K. R. P. Nippatla, "A Secure Cloud-Based Financial Time Series Analysis System Using Advanced Auto-Regressive and Discriminant Models: Deep AR, NTMs, and QDA." Accessed: Mar. 06, 2025. [Online]. Available: https://ijmrr.com/admin/uploads/IJMRR%20(V-12,%20i-4%20)%20%5b1-15%5d_c.pdf

[11] S. K. Alavilli and Sephora, "Predicting Heart Failure with Explainable Deep Learning Using Advanced Temporal Convolutional Networks," ijcsejournal.org. Accessed: Mar. 06, 2025. [Online]. Available: http://www.ijcsejournal.org/IJCSE-V5I2P9.pdf

[12] 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.

[13] B. Kadiyala, "Multi-Swarm Adaptive Differential Evolution and Gaussian Walk Group Search Optimization for Secured Iot Data Sharing Using Super Singular Elliptic Curve Isogeny Cryptography," vol. 8, no. 3, 2020.

[14] B. Kadiyala and H. Kaur, "Secured IoT Data Sharing through Decentralized Cultural Co- Evolutionary Optimization and Anisotropic Random Walks with Isogeny- Based Hybrid Cryptography," *Journal of Science & Technology (JST)*, vol. 6, no. 6, Art. no. 6, Dec. 2021.

[15] B. Kadiyala and H. Kaur, "DYNAMIC LOAD BALANCING AND SECURE IOT DATA SHARING USING INFINITE GAUSSIAN MIXTURE MODELS AND PLONK," vol. 7, no. 2, 2022.

[16] B. Kadiyala, "INTEGRATING DBSCAN AND FUZZY C-MEANS WITH HYBRID ABC-DE FOR EFFICIENT RESOURCE ALLOCATION AND SECURED IOT DATA SHARING IN FOG COMPUTING," *International Journal of HRM and Organizational Behavior*, vol. 7, no. 4, pp. 1–13, Oct. 2019.

[17] 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.

[18] 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.

[19] C. Vasamsetty, "Patient-Centric Approaches in Cardiology: Leveraging Crowdsourcing and Decision Trees for Optimized Clinical Pathways," IJORET.com. Accessed: Mar. 06, 2025. [Online]. Available: http://ijoret.com/IJORET-V7I1P1.pdf

[20] 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," vol. 12, no. 6, 2023.

[21] S. K. Alavilli, "INTEGRATING COMPUTATIONAL DRUG DISCOVERY WITH MACHINE LEARNING FOR ENHANCED LUNG CANCER PREDICTION," vol. 11, no. 9726, 2023.

[22] C. Vasamsetty, "Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends," vol. 8, no. 2, 2020.

[23] 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.

[24] S. H. Eedala, "Financial Fraud Detection Dataset." Accessed: Feb. 28, 2025. [Online]. Available: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset