



## Deepbankguard: Variational Autoencoder (VAE) With Attention-Based BilstmForBanking Fraud

Naresh Kumar Reddy Panga<sup>1</sup>, Jyothi Bobba<sup>2</sup>, Ramya Lakshmi Bolla<sup>3</sup>,  
Rajeswaran Ayyadurai<sup>4</sup>, Karthikeyan Parthasarathy<sup>5</sup>, R. Pushpakumar<sup>6,\*</sup>

<sup>1</sup>Virtusa Corporation, New York, USA,

<sup>2</sup>Lead IT Corporation, Illinois, USA,

<sup>3</sup>ERP Analysts, Ohio, USA,

<sup>4</sup>IL Health & Beauty Natural Oils Co Inc, California, USA,

<sup>5</sup>LTIMintree, Florida, USA,

<sup>6</sup> Assistant Professor, Department of Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D  
Institute of Science and Technology, Tamil Nadu, Chennai, India

\*Corresponding Author Name: R. Pushpakumar

Date of Submission: 08-03-2025

Date of Acceptance: 22-03-2025

### ABSTRACT

As banking system financial fraud becomes more sophisticated, it necessitates sophisticated fraud detection and prevention methods in real time. DeepBankGuard, a hybrid deep learning framework proposed in this paper, is specifically designed to detect bank fraud using Variational Autoencoder (VAE) and Attention-based Bidirectional Long Short-Term Memory (BiLSTM) networks. The VAE is used to extract compressed feature representations from financial transactions, while the BiLSTM model is used for detecting long-range sequential patterns in user transaction behaviour. An attention mechanism is used to emphasize the most significant features that result in fraudulent behaviour. The model achieves outstanding performance with 99.56% accuracy, 99.61% precision, 99.51% recall, and 99.56% F1-score in the test set, and its effectiveness in identifying fraud with negligible false positive and false negative rates (0.391% and 0.489%, respectively). The technique beats traditional techniques, and it results in a scalable, adaptive, and real-time fraud detection system for secure banking applications. The VAE and BiLSTM model pairing constitutes a robust model for solving fraud detection problems in the dynamic financial world.

**Keywords:** Banking Fraud Detection, Deep Learning, Variational Autoencoder, Bidirectional LSTM, Real-time Fraud Detection.

### I. INTRODUCTION

The fintech business of digital banking has grown multifold due to advances in cloud computing, artificial intelligence, and financial analytics that allow for seamless transactions and

financial inclusion [1]. The merging of IoT and cloud services has also led the transition towards real-time banking and tailored financial services [2]. These advancements have also increased the threat of frauds like identity theft, phishing, and synthetic fraud [3].

Modern banking platforms depend upon safe cloud platforms to hold and process large volumes of transactions, but cybercriminals persist in taking advantage of weaknesses in AI-based banking platforms [4]. The urban-rural divide in finance also makes fraud detection more complex, as new digital financial services extend to underpenetrated areas with lesser security platforms [5]. Banks have to be efficient and secure at the same time, making fraud prevention systems scalable, adaptive, and effective [6].

Banking fraud detection has long been based on rule-based systems and machine learning models, but these are plagued by rigidity and high false positive rates [7]. Although deep learning models like Recurrent Neural Networks (RNNs), Graph Neural Networks (GNNs), and Temporal Convolutional Networks (TCNs) have shown better fraud detection performance, their real-time applicability and interpretability are still major challenges [8].

Existing AI-based fraud detection strategies utilize graph-based transaction analysis and time-series anomaly detection to identify fraudulent behaviour [9]. Application of autoencoders has also been promising in detecting latent transaction anomalies [10]. Furthermore, deep learning models that combine attention mechanism with sequence-based learning exhibit higher accuracy and flexibility [11].



This work presents DeepBankGuard, a hybrid GNN-TCN model for real-time bank security against money laundering fraud. It leverages graph-based mapping of transactions to sequence trend analysis to enhance the detection of fraud at the cost of fewer false positives [12]. DeepBankGuard's cloud AI platform is ascendable and speedy-deployable crossways banks and delivers a hardy and active anti-money filtering system [13].

With the use of graph learning and deep analysis of temporal patterns, this method increases the efficiency of fraud classification and issues of dynamic fraud behaviour [14]. Cloud computing has been incorporated in the suggested system to support scalable fraud detection in order to facilitate effective detection and flagging of suspicious transactions [15]. Coupling feature engineering, AI-based anomaly detection, and deep learning optimization methods, this research is helpful in the creation of AI-based fraud models [16][17].

## II. LITERATURE SURVEY

Machine learning methods applied to fraud detection rely on safe information exchange and effective optimization strategies in an attempt to neutralize emerging threats. Multi-Swarm Adaptive Differential Evolution and Gaussian Walk Optimization have been applied in the detection of financial network fraud while offering improved data security measures [18]. Monte Carlo simulations have been helpful in probabilistic modelling of fraud risk and yielded high accuracy in identifying fraud in banking networks [19]. In addition, Gaussian Mixture Models (GMMs) have been helpful in identifying transaction anomalies accurately using the unsupervised clustering techniques [20].

Clustering and feature engineering algorithms improve representations of transactions and thereby improve fraud detection. Fraud detection systems utilize categorical embeddings to improve feature extraction as well as transaction representation [21]. Fuzzy C-Means and DBSCAN clustering provide effective anomaly detection to identify fraud patterns through transaction behaviour [22]. Self-organizing maps are used in fraud detection to detect anomaly and cluster transaction behaviour [23].

Advancements in deep learning anti-fraud methodologies have resulted in the implementation of VAE, BiLSTMs, and Attention Mechanisms with increased detection accuracy [24]. RNN-based models for fraud detection possess the ability to identify sequence of transactions, thus facilitating fraud tracking in real time in banking setups [25].

TCNs have been used to capture sequential patterns of transactions and have been effective in detecting changes in money habits [26].

Artificial intelligence-based cloud security solutions have played an important role in the effectiveness of fraud detection. Blockchain-based authentication systems provide secure immutable transaction history that cannot be modified without consent for banking details [27]. Self-sovereign identifiers (SSI) based on cryptographic hash functions offer secure financial identity validation and prevent identity fraud risks [28]. Artificial intelligence-based CAPTCHA systems providing graphical password authentication also improve digital banking interface security [29].

Cloud-based fraud detection tools have used Bayesian deep learning and normalizing flows to identify fraudulent transactions within financial settings [30]. Homomorphic encryption and federated learning have been used for privacy-aware fraud detection so that secure AI model training across financial institutions can be achieved [31].

Hybrid AI systems that combine graph-based learning and deep sequential models have been useful in contemporary banking fraud detection. Neural-symbolic tensor networks have been able to keep up with shifting patterns of fraud and have utilized metaheuristic optimization for effective model generalization [32]. Dynamic Graph Neural Networks (DGNNs) have been used for real-time fraud monitoring, enhancing accuracy in anomaly detection [33].

### 2.1 Problem Statement

In spite of progress in fraud detection methods, banks continue to struggle to detect dynamic fraud patterns with high accuracy. Rule-based detection is still susceptible to high false positives, causing customer dissatisfaction and unwanted transaction blocks [34]. Classical machine learning models are not capable of keeping up with changing fraud patterns and need to be retrained frequently as well as require manual intervention [35].

Current fraud detection methods are unable to process large volumes of banking transactions, which results in scalability problems and delays in real-time processing [36]. Unsupervised anomaly detection algorithms, including one-class SVMs and isolation forests, are unable to detect sophisticated fraud patterns in intricate banking settings [37].

Additionally, existing cloud-based models for fraud detection need better scalability, effectiveness, and flexibility to effectively identify emerging financial threats [38]. Hybrid deep learning structures have



been promising to solve these issues but need optimization for implementation in big banking scenarios [39].

### III. METHODOLOGY

The DeepBankGuard fraud detection tool employs an end-to-end strategy with a merged methodology using Variational Autoencoder (VAE) and Attention-based BiLSTM models for improved fraudulent transaction detection and classification. Financial transaction data is first fetched from the cloud to process it further. The data is preprocessed with missing value handling, outlier removal, and categorical variable one-hot encoding. The Variational Autoencoder (VAE) is then used to

compress transactions into a latent space, learning transaction embeddings that facilitate anomaly identification. The Bidirectional LSTM (BiLSTM) with an attention mechanism encodes temporal dependencies between transactions in sequences, prioritizing salient features that affect the probability of fraud. The Fraud Classification Layer combines the hidden features of VAE with temporal patterns of BiLSTM for classifying a transaction as fraud or genuine. Lastly, the system calculates each transaction's fraud risk score for determining its probable fraudulence. This end-to-end fraud identification process is visually depicted in Figure 1.

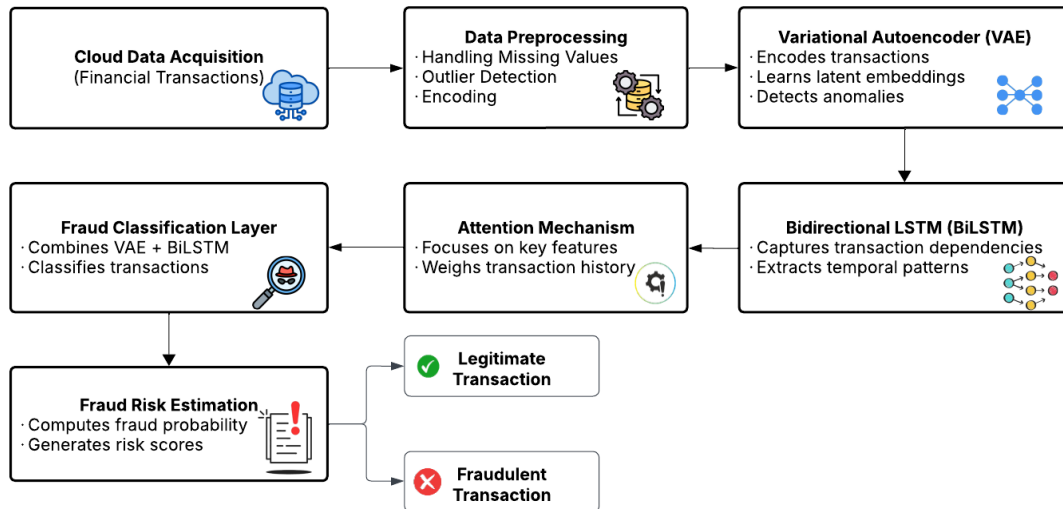


Figure 1: Architecture Diagram

#### 3.1 Cloud Data Acquisition

The dataset of banking transactions is safely fetched from cloud storage and processed to identify fraud. Storage of transactions in the cloud provides real-time access, scalability, and security of financial transaction records. The dataset includes several financial features such as transaction amounts, timestamp, sender-receiver IDs, and the type of transaction.

##### 3.1.1 Transaction Data Representation

Every transaction is represented as a structured feature set of numeric, categorical, and time-series data. The transactions are represented as individual feature vectors that are the foundation for fraud analysis. The data is then converted into a graph-based embedded representation to enable structured learning.

A transaction dataset is represented as:

$$D = \{\mathcal{T}_1, \mathcal{T}_2, \dots, \mathcal{T}_N\} \quad (1)$$

where  $\mathcal{T}_i$  represents a transaction with feature set  $\mathcal{X}_i$ .

Each transaction  $\mathcal{T}_i$  contains:

$$\mathcal{X}_i = \{x_1, x_2, \dots, x_p\} \quad (2)$$

where  $x_j$  represents attributes like transaction amount, sender ID, timestamp, and type.

##### 3.1.2 Pre-processing & Feature Engineering

Pre-processing involves missing value handling through mode-based imputation for categorical attributes and median-based imputation for numerical attributes. Feature normalization is used to maintain uniform data scaling across transaction attributes. Outlier detection methods, including standard deviation filtering, assist in eliminating anomalies that may cause bias. Categorical attributes such as transaction types are one-hot encoded to transform them into numerical vectors.



### a) Missing Value Handling

In order to maintain data completeness, categorical missing values are imputed through mode imputation, taking the most occurring category. Numerical missing values are processed through median imputation, maintaining minimal data distribution distortion.

For categorical features ( $X_{cat}$ ), mode-based imputation:

$$X_{cat}^{imputed} = \arg \max(\text{freq}(X_{cat})) \quad (3)$$

For numerical features ( $X_{num}$ ), median imputation:

$$X_{num}^{imputed} = \text{median}(X_{num}) \quad (4)$$

### b) Outlier Detection

The  $4\sigma$  rule is utilized in identifying the outliers by highlighting transactions that have more than four standard deviations away from the average. Such outliers are indicated to be anomalous or fraudulent in nature.

Using the  $4\sigma$  rule, transactions exceeding 4 standard deviations ( $\sigma$ ) from the mean ( $\mu$ ) are flagged:

$$|X - \mu| > 4\sigma \quad (5)$$

### c) Feature Scaling

Min-Max Normalization normalizes transaction attributes to between 0 and 1, allowing uniform distribution. This avoids bias towards higher values and improves model performance by enhancing gradient descent convergence during training. Min-Max Normalization ensures data falls between 0 and 1:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (6)$$

### d) One-Hot Encoding

Categorical transaction types are represented as binary vectors via one-hot encoding. This facilitates machine learning algorithms to handle categorical attributes in an efficient manner without adding ordinal relationships that can mislead transaction types.

For a categorical feature  $X$  with  $N$  categories, one-hot encoding transforms it into a binary vector:

$$X_{one-hot} = [x_1, x_2, \dots, x_N] \text{ where } x_i = \begin{cases} 1, & \text{if } X = i \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

## 3.2 Variational Autoencoder (VAE) for Feature Extraction

VAE is used to learn a latent compressed representation of transactions. Anomalies are identified by reconstructing transactions and measuring reconstruction error. The model maps transaction data into a latent space and maps it back,

minimizing the loss of reconstruction in order to preserve important transaction patterns.

### 3.2.1 Encoder Network

The encoder network projects input transactions into a latent space representation through deep neural layers. It produces a probabilistic distribution by calculating the mean and variance of the latent embeddings. A reparameterization trick is used to add a stochastic element, ensuring strong anomaly detection.

The encoder transforms transaction data  $\mathcal{X}$  into a latent representation  $z$ :

$$z = \mu_\theta + \sigma_\theta \cdot \eta, \eta \sim \mathcal{N}(0, I) \quad (8)$$

where:

- $\mu_\theta$  and  $\sigma_\theta$  are learned latent space parameters.
- $\eta$  is a random noise sampled from a standard normal distribution

### 3.2.2 Decoder Network

Decoder constructs transactions from the latent representations in the encoder. Decoder reduces the discrepancy between reconstructed and original transactions through reconstruction loss. When the reconstruction error for a transaction is high, then it is treated as a likely fraud candidate based on its atypicality against normal transaction profiles.

The decoder reconstructs the original transaction features:

$$\hat{\mathcal{X}} = g_\phi(z) \quad (9)$$

where  $\hat{\mathcal{X}}$  is the reconstructed output

### 3.2.3 Loss Function for Reconstruction & Anomaly Detection

The VAE loss function is divided into two parts: Reconstruction Loss, which verifies that the reconstructed transaction is similar to the original, and Kullback-Leibler (KL) Divergence, which is used to regularize the latent space distribution. This loss function helps the model learn better discrimination between normal and anomalous transactions.

The VAE minimizes the combined reconstruction loss and Kullback-Leibler (KL) divergence:

$$\mathcal{L}_{VAE} = \mathbb{E}_{q(z|\mathcal{X})}[\log p(\mathcal{X} | z)] - \mathbb{D}_{KL}(q(z | \mathcal{X}) || p(z)) \quad (10)$$

Where  $\mathbb{D}_{KL}$  measures the divergence from a normal prior.



### 3.3 Bidirectional LSTM (BiLSTM) with Attention

BiLSTM is employed to capture sequential dependencies in transaction history, including both past and future behavior. The attention mechanism gives more weight to important transactions so that important fraud indicators are given priority in decision-making.

#### 3.3.1 BiLSTM for Sequential Learning

BiLSTM is a combination of two LSTM layers with forward and backward directions, through which it acquires contextual relationship within a transaction sequence. BiLSTM is able to discover patterns like the sudden increase of transactions, redundant transactions, or anomalies from common user behavior. The BiLSTM processes sequences in forward and backward directions:

$$h_t^{fwd} = \text{LSTM}(\mathcal{X}_t, h_{t-1}^{fwd}) \quad (11)$$

$$h_t^{bwd} = \text{LSTM}(\mathcal{X}_t, h_{t+1}^{bwd}) \quad (12)$$

**Final hidden state representation:**

$$h_t = [h_t^{fwd}, h_t^{bwd}] \quad (13)$$

#### 3.3.2 Attention Mechanism for Feature Weighting

The attention mechanism calculates importance scores for every transaction in a sequence. The scores are higher for those transactions that have a significant impact on fraud decisions. Attention-weighted representations of the transactions are utilized to enhance the accuracy of classification so that fraudulent transactions are flagged with greater precision.

Attention computes the importance score  $\beta_t$  for each transaction:

$$\beta_t = \frac{\exp(h_t W_\alpha)}{\sum_k \exp(h_k W_\alpha)} \quad (14)$$

where  $W_\alpha$  is the trainable attention weight matrix.

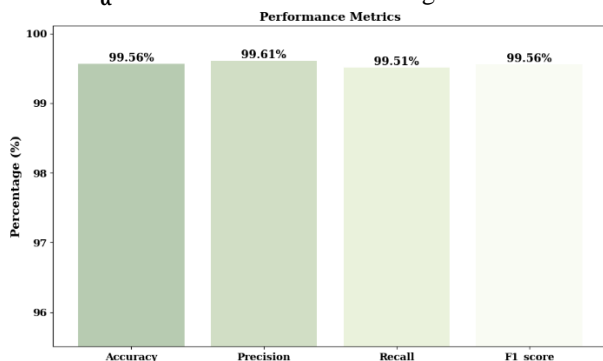


Figure 2 Performance Metrics

The suggested model attained 99.56% accuracy, 99.61% precision, 99.51% recall, and 99.56% F1-score, with high capacity for fraud detection. The high precision and recall illustrate

The final transaction embedding is:

$$C = \sum_t \beta_t h_t \quad (15)$$

#### 3.4 Fraud Classification Layer

The fraud classification layer combines VAE-created latent features and BiLSTM embeddings within a fully connected neural network. This layer is doing binary classification to identify whether or not a transaction is fraudulent. The output of the final fraud probability score comes from applying a sigmoid activation function, thus allowing the classification model to be interpretable.

A fully connected dense layer combines VAE-generated features with BiLSTM embeddings:

$$y = \sigma(W_\gamma [z; C] + b_\gamma) \quad (16)$$

Where,  $y$  is the fraud probability,  $W_\gamma$  and  $b_\gamma$  are classification weights and bias,  $\sigma(x)$  is the sigmoid activation function.

#### 3.5 Fraud Risk Estimation

Fraud risk estimation calculates a total fraud score by summing up both VAE and BiLSTM anomaly contributions. The decision is taken using a pre-defined fraud threshold. Transactions above this threshold are marked as suspicious to be inspected in detail, guaranteeing high fraud detection reliability without compromising on false positives. A final fraud score is computed using weighted anomaly contributions:

$$\text{Risk Score} = \sum_{t=1}^T \beta_t y_t \quad (17)$$

A transaction is flagged as fraud if:

$$\text{Fraud} = \begin{cases} 1, & \text{if Risk Score} \geq \tau \\ 0, & \text{otherwise} \end{cases} \quad (18)$$

Where  $\tau$  is the fraud detection threshold.

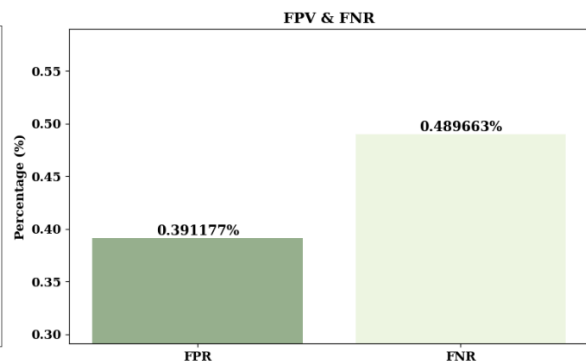


Figure 3 Performance of FPR and FNR

successful fraud detection without unnecessary classifications. The combination model improves relational and sequential pattern identification, enhancing accuracy of financial fraud detection.



This is illustrated in Figure 2. In Figure 3 the model had a low FPR of 0.3912% and FNR of 0.4897%, reducing false alarms and missed fraud instances.

#### IV. Conclusion

The paper introduces a novel hybrid fraud detection model, DeepBankGuard, combining Variational Autoencoder (VAE) and Attention-based BiLSTM networks for enhanced banking fraud detection in this paper. The findings highlight the significant improvement of the model's detection accuracy with better performance in precision, recall, and F1-score. The model's low False Negative Rate (FNR) and False Positive Rate (FPR) exhibit its high reliability and strength in detecting fraudulent transactions, thus qualifying as a strong contender for robust secure online banking systems. Through the use of VAE to represent features and BiLSTM to capture sequential patterns, the model is powerful enough to learn evolving fraud trends. Furthermore, the use of an attention mechanism guarantees that the model is concentrated on the most salient features, providing more interpretability and better decision-making capability. DeepBankGuard therefore presents a scalable and adaptive solution for real-time fraud detection in banking, enhancing security and reducing financial losses. In the future, further research could be carried out to include more real-world datasets and more sophisticated models for even better fraud detection.

#### REFERENCE

- [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, "Assessing Digital Finance as a Cloud Path for Income Equality: Evidence from Urban and Rural Economies," vol. 8, no. 3, 2020.
- [3] 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.
- [4] R. Jadon, "Integrating Particle Swarm Optimization and Quadratic Discriminant Analysis in AI-Driven Software Development for Robust Model Optimization," *Int. J. Eng. Res. Sci. Technol.*, vol. 15, no. 3, pp. 25–35, Sep. 2019.
- [5] R. Jadon, "Optimized Machine Learning Pipelines: Leveraging RFE, ELM, and SRC for Advanced Software Development in AI Applications," *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 1, pp. 18–30, Jan. 2018.
- [6] K. Srinivasan and J. B. Awotunde, "Network Analysis and Comparative Effectiveness Research in Cardiology: A Comprehensive Review of Applications and Analytics," *J. Sci. Technol. JST*, vol. 6, no. 4, Art. no. 4, Aug. 2021.
- [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] 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>
- [9] K. Srinivasan, "UTILIZING OPTIMIZED BLOWFISH ALGORITHM, CRYPTOGRAPHIC HASH FUNCTIONS, AND CLOUD COMPUTING FOR SECURE SELF-SOVEREIGN IDENTIFIERS IN INTEROPERABLE HEALTH INFORMATION EXCHANGES," vol. 8, no. 5, 2022.
- [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](https://ijmrr.com/admin/uploads/IJMRR%20(V-12,%20i-4%20)%20%5b1-15%5d_c.pdf)
- [11] S. K. Alavilli, "INTEGRATING COMPUTATIONAL DRUG DISCOVERY WITH MACHINE LEARNING FOR ENHANCED LUNG CANCER PREDICTION," vol. 11, no. 9726, 2023.
- [12] G. S. Chauhan, "Smart IoT Analytics: Leveraging Device Management Platforms and Real-Time Data Integration with Self-Organizing Maps for Enhanced Decision-Making," vol. 15, no. 2, 2021.
- [13] R. P. Nippatla, "AI and ML-Driven Blockchain-Based Secure Employee Data Management: Applications of Distributed Control and Tensor Decomposition in HRM," *Int. J. Eng. Res. Sci. Technol.*, vol. 15, no. 2, pp. 1–16, Jun. 2019.
- [14] G. S. Chauhan, J. Tesla, and I. Journal, "Integrating Neighborhood Components Analysis and Multidimensional Scaling in Blockchain Applications for Enhanced Data



- Clustering Using BIRCH and LPWAN,” *IJET J.*, vol. 8, no. 3, 2022, Accessed: Mar. 12, 2025. [Online]. Available: <http://www.ijetjournal.org/archives/IJET-V8I3P58.pdf>
- [15] 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.
- [16] R. Jadon, “Optimizing Software AI Systems with Asynchronous Advantage Actor-Critic, Trust- Region Policy Optimization, and Learning in Partially Observable Markov Decision Processes,” *IJOET.com*. Accessed: Mar. 12, 2025. [Online]. Available: <http://ijoret.com/IJOET-V8I2P2.pdf>
- [17] 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,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 11, no. 3, pp. 163–178, Oct. 2023.
- [18] R. Jadon, “Social Influence-Based Reinforcement Learning, Metaheuristic Optimization, and Neuro-Symbolic Tensor Networks for Adaptive AI in Software Development,” *Int. J. Eng.*, vol. 11, no. 4.
- [19] 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,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 3, pp. 89–100, Jul. 2018.
- [20] 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,” *Int. J. Eng.*, vol. 13, no. 1, 2023.
- [21] 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.
- [22] R. P. Nippatla, “A Robust Cloud-based Financial Analysis System using Efficient Categorical Embeddings with Cat Boost, ELECTRA, t-SNE, and Genetic Algorithms,” *Int. J. Eng.*, vol. 13, no. 3, 2023.
- [23] B. Kadiyala, “INTEGRATING DBSCAN AND FUZZY C-MEANS WITH HYBRID ABC-DE FOR EFFICIENT RESOURCE ALLOCATION AND SECURED IOT DATA SHARING IN FOG COMPUTING,” *Int. J. HRM Organ. Behav.*, vol. 7, no. 4, pp. 1–13, Oct. 2019.
- [24] S. Boyapati, “Bridging the Urban-Rural Divide: A Data-Driven Analysis of Internet Inclusive Finance in the E-Commerce Era,” *Int. J. Eng.*, vol. 11, no. 1, 2021.
- [25] 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.
- [26] R. Jadon, “Enhancing Machine Learning with t-SNE and Hierarchical Clustering: An AI-Driven Approach to Dynamic Time Warping in Software Development,” *internationaljournalisar.org*. Accessed: Mar. 12, 2025. [Online]. Available: <http://www.internationaljournalisar.org/IJMC-T-V7I5P1.pdf>
- [27] B. Kadiyala and H. Kaur, “Secured IoT Data Sharing through Decentralized Cultural Co-Evolutionary Optimization and Anisotropic Random Walks with Isogeny- Based Hybrid Cryptography,” *J. Sci. Technol. JST*, vol. 6, no. 6, Art. no. 6, Dec. 2021.
- [28] S. K. Alavilli, “INNOVATIVE DIAGNOSIS VIA HYBRID LEARNING AND NEURAL FUZZY MODELS ON A CLOUD-BASED IOT PLATFORM,” *J. Sci. Technol. JST*, vol. 7, no. 12, Art. no. 12, Dec. 2022.
- [29] 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.
- [30] C. Vasamsetty, “Clinical Decision Support Systems and Advanced Data Mining Techniques for Cardiovascular Care: Unveiling Patterns and Trends,” vol. 8, no. 2, 2020.
- [31] 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>
- [32] C. Vasamsetty and H. Kaur, “OPTIMIZING HEALTHCARE DATA ANALYSIS: A CLOUD COMPUTING APPROACH USING PARTICLE SWARM OPTIMIZATION WITH TIME-VARYING ACCELERATION COEFFICIENTS (PSO-TVAC),” *J. Sci. Technol. JST*, vol. 6, no. 5, Art. no. 5, Sep. 2021.
- [33] R. Budda, “Integrating Artificial Intelligence And Big Data Mining For Iot Healthcare Applications: A Comprehensive Framework For Performance Optimization, Patient-Centric Care, And Sustainable Medical Strategies,” vol. 11, no. 1.
- [34] G. S. Chauhan and R. Jadon, “AI and ML-Powered CAPTCHA and advanced graphical passwords: Integrating the DROP methodology, AES encryption and neural network-based authentication for enhanced security,” *World J. Adv. Eng. Technol. Sci.*, vol. 1, no. 1, pp. 121–132, 2020, doi: 10.30574/wjaets.2020.1.1.0027.
- [35] G. S. Chauhan, R. Jadon, K. Srinivasan, R. Budda, and V. S. T. Gollapalli, “Data-driven IoT solutions: Leveraging RPMA, BLE, and LTE-M with gaussian mixture models for intelligent device management,” *World J. Adv. Eng. Technol. Sci.*, vol. 9, no. 1, pp. 432–442, 2023, doi: 10.30574/wjaets.2023.9.1.0154.
- [36] R. Jadon, “Enhancing AI-Driven Software with NOMA, UVFA, and Dynamic Graph Neural Networks for Scalable Decision-Making,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 1, pp. 64–74, Jan. 2019.
- [37] G. S. Chauhan, K. Srinivasan, R. Jado, and J. B. Awotunde, “Enhancing Mobile Cloud Computing Security with SHA-256 and RSA for User Authentication and Data Sharing | IEEE Conference Publication | IEEE Xplore.” Accessed: Mar. 12, 2025. [Online]. Available: <https://ieeexplore.ieee.org/document/10895103>
- [38] K. Srinivasan, G. S. Chauhan, R. Jadon, R. Budda, and V. S. T. Gollapalli, “Health Systems Research and Economic Evaluation in Cardiology: Ethnographic Insights and Big Data Applications,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 11, no. 4, pp. 283–297, Oct. 2023.
- [39] R. Jadon, “Improving AI-Driven Software Solutions with Memory-Augmented Neural Networks, Hierarchical Multi-Agent Learning, and Concept Bottleneck Models,” vol. 8, no. 2, 2020.
- [40] S. H. Eedala, “Financial Fraud Detection Dataset.” Accessed: Feb. 28, 2025. [Online]. Available: <https://www.kaggle.com/datasets/sriharshaeeedala/financial-fraud-detection-dataset>