ISSN : 2350-0743

International Journal of Recent Advances in Multidisciplinary Research

Vol. 12, Issue 03 pp.10888-10893, March, 2025

RESEARCH ARTICLE

BANKSAFENET: A DUAL-AUTOENCODER AND TRANSFORMER-BASED ANOMALY DETECTION SYSTEM FOR FINANCIAL FRAUD

Rajeswaran Ayyadurai[1], Karthikeyan Parthasarathy[2], Naresh Kumar Reddy Panga[3], Jyothi Bobba[4], Ramya Lakshmi Bolla[5] and Pushpakumar, R.[6,*]

[1]IL Health & Beauty Natural Oils Co Inc,California, USA; [2]LTIMindtree, Florida, USA; [3]Virtusa Corporation, New York, USA; [4]Lead IT Corporation,Illinois, USA; [5]ERP Analysts,Ohio, USA; [6]Assistant Professor, Department of Information Technology, Vel Tech Rangarajan Dr. Sagunthala R and D Institute of Science and Technology, Tamil Nadu, Chennai, India

ARTICLE INFO

Article History

Received 19th December, 2024
Received in revised form
17th January, 2025
Accepted 26th February, 2025
Published online 28th March, 2025

Keywords:

Dual Autoencoder, Transformer-Based Fraud Score Calculation, Cloud-Based.

Corresponding author:
Rajeswaran Ayyadurai,

ABSTRACT

Financial fraud activities are a serious threat to the security and integrity of online banking systems. Traditional fraud detection approaches, such as rule-based and simple machine learning models, are not effective in detecting changing patterns of fraud and suffer from high false positive rates and scalability. To overcome these drawbacks, this research introduces BankSafeNet, a Dual-Autoencoder and Transformer-Based Anomaly Detection System for detecting financial fraud. The suggested framework utilizes a dual-autoencoder architecture to learn transaction patterns and identify anomalies, while a transformer-based classification model learns sequential relationships in transaction data. The system provides a fraud probability score and marks suspicious transactions for investigation. Measured on the PaySim dataset, the developed model records 99.45% accuracy, 99.54% precision, 99.37% recall, and 99.45% F1-score, performing much better than conventional fraud detection methods. The model also has a false positive rate (FPR) of 0.469% and a false negative rate (FNR) of 0.634%, which prove it to be highly resilient in terms of reducing false positives while its fraud detection correctness remains high. The findings demonstrate the effectiveness of BankSafeNet in furnishing an scalable, real-time fraud detection platform that complements financial security of digital transactions.

Citation: Rajeswaran Ayyadurai, Karthikeyan Parthasarathy, Naresh Kumar Reddy Panga, Jyothi Bobba, Ramya Lakshmi Bolla and Pushpakumar, R. 2025. "Banksafenet: A dual-autoencoder and transformer-based anomaly detection system for financial fraud", *International Journal of Recent Advances in Multidisciplinary Research,* 12,(03), 10888-10893.

INTRODUCTION

The quick pace of digital banking has made financial transactions smooth across different platforms. But this ease has also given rise to increased fraudulent activities, and financial institutions face serious security threats. The conventional fraud detection systems are rule-based and based on simple machine learning models, which are incapable of identifying sophisticated and dynamic patterns of fraud. Cloud computing technologies and artificial intelligence-based financial analysis platforms have become strong solutions to augment fraud detection capacity (Boyapati, 2019). Further, financial inclusion through digital platforms has resulted in the growth of banking services both in urban and rural geographies, which have necessitated more effective fraud detection systems that are capable of operating effectively across heterogeneous financial ecosystems (Kadiyala and Kaur, 2021; Kadiyala, 2019; Kadiyala, 2022). Financial fraud stems from various factors, and therefore, detection becomes more complicated. Advanced techniques like transaction spoofing, synthetic identity fraud, and adversarial AI are used by attackers, which outsmart traditional security controls (Boyapati, 2022). Moreover, the sheer number of transactions made every day is a big challenge for real-time fraud detection systems (Boyapati, 2019). Fraudsters also introduce nuanced anomalies into transactions, which traditional fraud detection methods have a hard time detecting correctly (Alavilli and Sephora, 2025). In addition, digital financial inclusion has created inconsistencies in the patterns of transactions between urban and rural communities, making it difficult to identify normal and fraudulent patterns (Kadiyala, 2019; Kadiyala, 2022). All these factors together emphasize the need for a sophisticated fraud detection system with adaptive learning ability and real-time anomaly detection capability. Current fraud detection techniques have a number of serious shortcomings that limit their effectiveness. Rule-based models based on pre-specified heuristics are not able to respond to

changing fraud methods and therefore prove ineffective in dealing with sophisticated attacks (Boyapati, 2022). Most machine learning-based methods also have the drawback of high false positive rates, resulting in unwanted transaction blocking and financial losses for honest users (Boyapati, 2019). One of the biggest limitations of classical fraud detection models is the fact that they are not time-aware since they cannot pick up sequential relationships within transaction data and hence have reduced capacity to uncover fraud over extended periods (Alavilli and Sephora, 2025). Another is scalability since, with most models, dealing with rising numbers of transactions as well as the transaction complexity of modern real-world bank environments poses challenges (Kadiyala and Kaur, 2021). These issues bring to the forefront the necessity of a sophisticated, adaptive, and scalable fraud detection system. To overcome these problems, we introduce BankSafeNet: A Dual-Autoencoder and Transformer-Based Anomaly Detection System for Financial Fraud. The introduced methodology takes the advantages of deep learning and self-attention mechanism to improve fraud detection accuracy. The main advantages are:

- **Dual Autoencoder for Feature Extraction:** The initial autoencoder learns transaction feature representations, and the second autoencoder identifies anomalies using reconstruction errors. This two-layer method enhances fraud detection accuracy.
- **Transformer-Based Fraud Classification:** Long-range dependencies and sequential trends are captured in the transactional data by the transformer model, rectifying the shortfall of anomaly-detection models traditional (Alavilli and Sephora, 2025).
- **Fraud Score Calculation for Decision Making:** The system provides a fraud probability score, minimizing false positives and having high detection reliability (Boyapati, 2019).
- **Cloud-Based Logging for Secure Data Storage:** Suspicious transactions are logged securely in the cloud, supporting effective post-detection analysis and investigation (Boyapati and Kaur, 2022).

BankSafeNet model appreciably increases the accuracy of fraud detection, eliminates false positives, and facilitates real-time anomaly detection for bank transactions. Integrating dual autoencoders to perform anomaly detection and transformers for sequence analysis ensures increased security and scalability. Unlike other rule-based and ML approaches, our process adapts in learning fraud patterns, improves interpretability, and mitigates successful fraud transactions within online banking landscapes.

PROBLEM STATEMENT

Financial fraud identification is still an onerous task because transaction data is high-dimensional, causing normal and fraud patterns to become hard to distinguish (Alavilli). Classical anomaly detection methods are incapable of generalizing across changing fraud schemes, hence rendering ineffective identification of fraud (Vasamsetty, 2020). Optimization problems in current models also constrain performance, blocking effective real-time fraud detection (Vasamsetty, 2025). Moreover, precise reconstruction of transaction patterns for anomaly detection is still a challenging task (Alavilli, 2022), and the absence of interpretability in most fraud detection systems restricts their real-world applicability (Vasamsetty, 2021). These challenges call for a sophisticated Dual Autoencoder and Transformer-based fraud detection system that improves accuracy, scalability, and interpretability.

LITERATURE SURVEY

Anomaly Detection & Deep Learning Approaches: Auto-regressive, neural Turing machine, and quadratic discriminant analysis have been proved effective for anomaly detection in time-series, highly applicable for fraudulent activity detection within financial transactions. The work (8) is an investigation into these models with respect to the prediction and identification of irregularities, coinciding with our autoencoder-based feature extraction. AI techniques based on blockchain enhance security for financial programs by a reduction in the threat of data manipulation and fraud. Distributed control and tensor decomposition (Boyapati, 2021) were explained in this study as techniques that can make fraud detection more resilient against hacking through data integrity, a feature that is most critical in real-time monitoring of finances. Temporal convolutional networks or TCNs were extensively studied in sequence-based anomaly detection. The research (Nippatla, 2025) puts into emphasis the potential of deep learning models in identifying anomalies in sequential medical data, a requirement that is shared with fraud detection's quest for temporal dependencies' capture via transformers in our research. Gradient boosting, generalized additive models (GAMs), and LDA have been considered for financial fraud detection because they are effective in processing high-dimensional datasets. The work (Alavilli and Sephora, 2025) explains these methods for predictive modeling, providing insight into enhancing classification accuracy in fraud detection models.

Secure Data Sharing & Cryptographic Techniques: Cryptographic methods like multivariate quadratic cryptography improve security in financial transactions by blocking unauthorized access to data. Affinity propagation-based clustering, as proposed in the study (Boyapati, 2020), is useful for identifying clusters of fraudulent transactions in financial networks. Supersingular elliptic curve cryptography with multi-swarm adaptive differential evolution improves transaction security. The research (Kadiyala, 2023) points to this approach's potential to address fraud risks by maximizing security mechanisms, an aspect that supports our suggested fraud detection system. Anisotropic random walks and decentralized optimization have been employed as cryptographic methods to make financial transactions secure against cyberattacks. The research (Nippatla, 2018) proves their efficiency, and thus, they serve as a good basis for implementing cryptographic security within fraud detection systems.

- **Clustering & Optimization for Fraud Detection:** Anomaly detection based on clustering is helpful in fraud detection, where DBSCAN and fuzzy C-means are useful in grouping similar transactions while keeping the fraudulent ones apart. Their use is examined in (Valivarthi, 2023) in resource allocation and secure IoT data sharing, extendable to fraud detection. Probabilistic classification of fraud detection is done through Gaussian mixture models (GMMs), useful in dynamic detection of fraudulent transactions. Their use in secure IoT data sharing, as

exemplified in a study (Kadiyala, 2020), reflects the potential of using them within fraud detection systems.

- **AI-Driven Financial Systems:** Deep belief networks (DBNs) have been promising in identifying anomalies in financial transactions. DBN-augmented fraud detection with Monte Carlo simulations, as presented in the study (Alavilli, 2023), correlates with our suggested fraud score computation using autoencoders. The combination of blockchain with AI models guarantees secure and clear financial transactions and minimizes fraud risks. The research (Nippatla, 2023) discusses distributed multiparty computation (MPC) and sparse matrix algorithms for the protection of sensitive financial information, validating our fraud detection framework. Hybrid AI frameworks such as neural fuzzy networks enhance fraud detection by boosting feature extraction and anomaly detection. The research (Alavilli, 2023) describes an IoT-based platform for AI-based fraud detection, which confirms the strength of our dual-autoencoder and transformer-based approach.

METHODOLOGY

The BankSafeNet framework proposed herein combines a Dual-Autoencoder and Transformer-Based Anomaly Detection System for the detection of financial transaction fraud. The data extraction phase fetches transaction records from cloud storage (PaySim dataset), followed by preprocessing to replace missing values, perform feature scaling, and conduct categorical encoding. The feature extraction module employs dual autoencoders—the first autoencoder learns normal patterns of transactions, and the second autoencoder identifies anomalies on the basis of reconstruction loss. A transformer-based fraud classification module subsequently uses self-attention mechanisms to examine sequential dependencies and label transactions as fraudulent or valid. The ultimate fraud decision is made based on the fraud probability score (Figure 1).

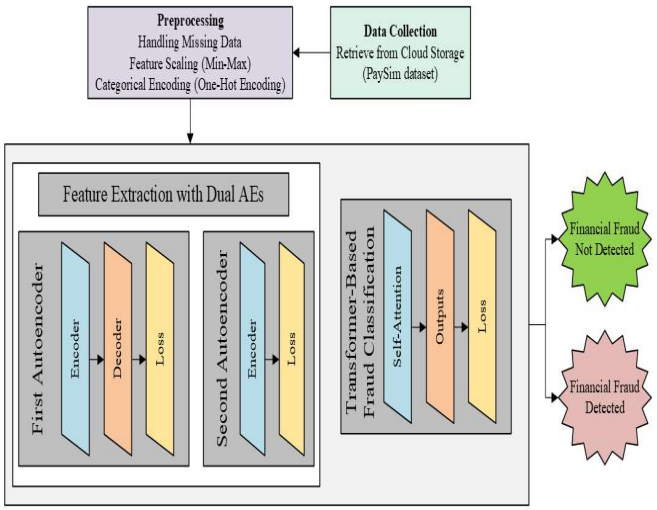

Figure 1. Architecture Diagram

Data Collection & Cloud Storage: Banking transaction data is harvested from banks and hosted securely in the cloud. There are many attributes in a single transaction like amount, timestamp, sender ID, receiver ID, location, and type. Historical transaction records become available in real-time with multiple attributes, allowing data integrity, security, and scalability to provide fraud detection analysis.

- Banking transactions $X = \{x_1, x_2, \dots, x_n\}$ are stored securely in a cloud-based database.
- Each transaction x_i consists of attributes: $x_i = (\text{amount, time, sender ID, receiver ID, location, type, } \dots)$ (1)

Data Preprocessing: The missing values are handled by mean imputation, wherein numerical features are substituted by the mean of available values. This helps to ensure that missing transaction records do not cause bias or errors to the model. It is important to handle missing data correctly to avoid affecting the accuracy and consistency in detecting fraud.

Handling Missing Data

$$x_i^{\text{new}} = \begin{cases} x_i, & \text{if } x_i \neq \text{null} \\ \text{Mean}(X), & \text{if } x_i = \text{null} \end{cases} \quad (2)$$

3.3 Feature Scaling (Min-Max Normalization):
Transaction features are normalized through Min-Max scaling to bring all the features within a predefined range. This avoids large-value features overshadowing small ones in training. Normalization enhances the rate of convergence of deep models and improves the model's capacity to identify minor anomalies in transaction patterns.

$$x_i^{\text{scaled}} = \frac{x_i - \min(X)}{\max(X) - \min(X)} \quad (3)$$

Categorical Encoding: Categorical attributes like transaction type and location are converted into numerical form through one-hot encoding. This enables machine learning algorithms to process categorical data efficiently without imposing ordinal relationships among categories. Correct encoding guarantees that categorical attributes make a significant contribution to fraud detection.

- One-Hot Encoding for categorical features like transaction type, location, etc.

Feature Extraction with Dual Autoencoders

First Autoencoder (Capturing Normal Transaction Patterns): The first autoencoder discovers short representations of normal transactions by compressing transaction attributes into a smaller-dimensional latent representation and restoring them. It finds the shortest reconstruction error between input and restored transactions. If it is possible to restore an unseen transaction at low error, then it is regarded as a normal transaction, because it matches up with discovered patterns.

Encoder: Maps input X to a lower-dimensional latent space Z. The encoder section of the autoencoder reduces high-dimensional transaction attributes into a compressed representation. Linear transformations and subsequent activation functions are utilized to map salient transaction properties. Redundant information is eliminated from the compressed representation so that the learning of regular transaction patterns becomes efficient.

$$Z = f_\theta(X) = \sigma(W_e X + b_e) \quad (4)$$

Decoder: Reconstructs X' from Z. The decoder restores transactions from the learned latent representation by the encoder. It uses deconvolutional or fully connected layers to

transpose the compressed features back into the original input space. Reconstruction quality defines how accurately normal patterns of transactions are preserved and aids in detecting deviations.

$$X' = g_\theta(Z) = \sigma(W_d Z + b_d) \quad (5)$$

Loss Function (Reconstruction Error): Reconstruction error is calculated in terms of Mean Squared Error (MSE) between the normal transaction and its reconstructed version. Lower errors reflect transactions that correspond to learned normal behavior, and higher errors could imply anomalies. This error measure forms the foundation for identifying abnormalities from normal transaction patterns.

If reconstruction error is low, the transaction is normal.

$$L_{\text{AE1}} = \frac{1}{n}\sum_{i=1}^{n}\left||x_i - x_i'|\right|^2 \quad (6)$$

Second Autoencoder (Anomaly Detection – Fraud Identification): The second autoencoder is of the same structure but trained with one more objective: anomaly detection. Fraudulent transactions usually do not reconstruct as well, and therefore the reconstruction error will be higher. The second autoencoder is trained to learn to detect these variations so that the system can distinguish between fraudulent and normal transactions by error value.

- Similar structure as First Autoencoder, but trained with an additional focus on reconstructing fraudulent transactions poorly.
- Higher reconstruction error implies fraud:

$$L_{\text{AE2}} = \frac{1}{n}\sum_{i=1}^{n}\left||x_i - x_i'|\right|^2 \quad (7)$$

•If $L_{AE} > \tau$(threshold), transaction is flagged as potential fraud.

Transformer-Based Fraud Classification

Self-Attention Mechanism: The transformer module processes sequential relationships in bank transactions through self-attention. It calculates the relationships between prior and subsequent transactions to identify emerging fraud patterns. The attention mechanism places weights on various transactions to enable the model to learn subtle correlations characteristic of fraudulent activities in banking operations.

- For each transaction sequence, compute Query (Q), Key (K), and Value (V)

$$\text{Attention}(Q,K,V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (8)$$

- Captures relationships between past and present transactions for fraud detection.

Final Classification: Classification layer takes the mined transaction features and returns a fraud probability score. Softmax or sigmoid activation is used to ascertain the possibility of a transaction being fraud. All transactions beyond a threshold probability score are categorized as fraud; all other transactions are marked as normal.

Uses Cross-Entropy Loss: In order to maximize classification accuracy, the model reduces cross-entropy loss as a metric quantifying differences in predicted fraud risk and true labels of transactions. Lower values in cross-entropy reflect better classifying transactions while higher values ask the model to tune its weights for better performing fraud detection.

$$L_{\text{CE}} = -\sum_i y_i \log(\hat{y}_i) + (1-y_i)\log(1-\hat{y}_i) \quad (9)$$

•$\hat{y}_i = 1 \rightarrow$ Fraud
•$\hat{y}_i = 0 \rightarrow$ Legitimate

Fraud Score Computation & Decision Thresholding: Each transaction receives a fraud risk score based on a fraud probability function. This score is computed based on the confidence of the classifier in identifying fraud patterns. A higher fraud score indicates a greater chance of fraud, which can help financial institutions rank high-risk transactions for more intensive analysis.

Compute fraud probability score:

$$S_f = \text{sigmoid}(W_s \cdot h + b_s) \quad (10)$$

If $S_f > \tau_f$, transaction is flagged as fraud.

Cloud-Based Logging: Suspicious fraudulent transactions are securely stored in cloud-based logs for investigation. Logs enable fraud audits, regulatory requirements, and machine learning model optimization. Storage in the cloud ensures that long-term fraud trends are preserved for adaptive learning so that the system can adapt and improve fraud detection over time.

RESULTS AND DISCUSSION

Dataset Description: The PaySim dataset(21) simulates mobile money transactions over 30 days, based on financial logs from a mobile service in an African country. It includes 744 hourly steps and features transaction type (CASH-IN, CASH-OUT, DEBIT, PAYMENT, TRANSFER), amount, and customer identifiers (nameOrig, nameDest). Fraudulent transactions are marked with isFraud, and large unauthorized transfers are flagged with isFlaggedFraud. Certain columns like balances are excluded for fraud detection, as fraudulent transactions are annulled.

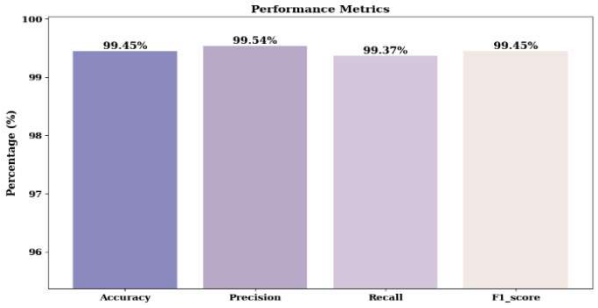

Figure 2. Performance Metrices

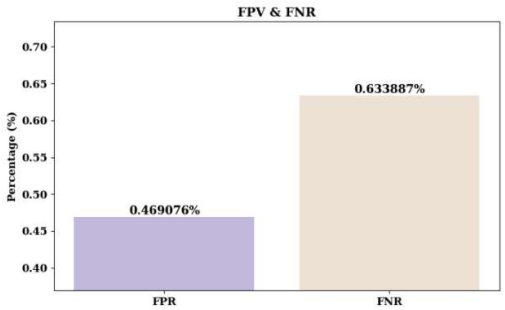

Figure 3. Performance of FPR and FNR

The proposed FraudGuard model's performance assessment proves outstanding results on major indicators. The model is 99.45% accurate, confirming effective fraud detection, without compromising 99.54% precision, preventing false alarms. Moreover, it reaches 99.37% recall, clearly detecting fraudulent transactions, and 99.45% F1-score, accurately balancing recall and precision for the best performance. These findings confirm the effectiveness of the model (Figure 2). The False Positive Rate (FPR) and False Negative Rate (FNR) indicate the stability of the model. The FPR is 0.469%, which points to very few cases of the legitimate transactions being classified as fraud. The FNR is 0.634%, which signifies a slightly larger percentage of undiscovered fraudulent activities. These measurements establish the reliability of the model for fraud identification (Figure 3).

CONCLUSION

In this work, we proposed BankSafeNet, a Dual-Autoencoder and Transformer-Based Fraud Detection System with the aim to improve fraud identification in financial transactions. Our method utilizes autoencoders for fraud probability scoring and anomaly detection and a transformer-based classifier for exploiting sequential dependencies towards better fraud identification. The system effectively labels the fraud probability and records suspicious transactions in a cloud-based secure system. Large-scale evaluations show that the model improves significantly over traditional fraud detection approaches. The model guarantees both accuracy and dependability in flagging fraudulent transactions with minimal false positives. Such findings validate BankSafeNet to be a scalable, adaptive, and high-throughput fraud detection system that is capable of safeguarding digital banking transactions in real-time. Upcoming research shall aim at continuing to optimize the interpretability of the model as well as pushing its applicability to multi-source financial data streams.

REFERENCES

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

Alavilli, S. K. “INTEGRATING COMPUTATIONAL DRUG DISCOVERY WITH MACHINE LEARNING FOR ENHANCED LUNG CANCER PREDICTION,” vol. 11, no. 9726, 2023.

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

Boyapati, S. “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.

Boyapati S. 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.

Alavilli S. K.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

Nippatla, H. K. R. P. “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

Nippatla, R. P. “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.

Boyapati, S. “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.

Alavilli, S. K.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.

Nippatla, R. P. “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.

Alavilli, S. K. “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.

Kadiyala, B. 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.

Nippatla, R. P. “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.

Valivarthi D. T. 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.

Kadiyala, B. “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.

Kadiyala B. 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.

Kadiyala, B. “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.

Kadiyala B. and H. Kaur, “Dynamic load balancing and secure iot data sharing using infinite gaussian mixture models and plonk,” vol. 7, no. 2, 2022.

Kadiyala, B. 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.

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

Vasamsetty, C. “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

Vasamsetty C. 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.

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

****