iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

FRAUDDETECTNET: A CAPSULE NETWORK WITH CNN-LSTM HYBRID MODEL FOR REAL-TIME BANKING FRAUD

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

[1]IL Health & Beauty Natural Oils Co Inc, California, USA.Email:rajeswaranayyadurai@arbpo.com
[2]LTIMindtree, Florida, USA. Email:karthikeyanparthasarathy@ieee.org
[3]Virtusa Corporation, New York, USA.Email:nareshkumarreddy_panga@ieee.org
[4]Lead IT Corporation, Illinois, USA. Email:jyothibobba@ieee.org
[5]ERP Analysts, Ohio, USA. Email:ramyalakshmibolla@ieee.org
[6]Assistant Professor, Department of Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, Chennai, India.
Email: pushpakumar@veltech.edu.in

Corresponding Author Name: Pushpakumar R Corresponding Author Email: pushpakumar@veltech.edu.in

ABSTRACT
With the dynamic digital banking ecosystem, fraud detection is still an important issue. This paper introduces FraudDetectNet, a hybrid Capsule Network with CNN-LSTM model, which can detect real-time bank fraud. The model integrates CNN's spatial feature extraction power, LSTM's learning of temporal dependencies, and the hierarchical representation strength of Capsule Networks. Applying the PaySim data, the envisioned model exhibits robust performance with an accuracy of 99.38%, precision rate of 99.42%, recall rate of 99.32%, and F1-score of 99.37%. The system gains a False Positive Rate of 0.565% and a False Negative Rate of 0.675% and thus will be extremely accurate for real-time fraud detection across cloud-based bank systems.

Keywords:
Fraud Detection, Capsule Networks, CNN-LSTM Hybrid Model, Real-Time Banking Transactions, Deep Learning

1. INTRODUCTION

The rapid electronic revolution in the financial sector has revolutionized the banking systems to become advanced, more accessible, and interconnected worldwide systems. Clever networks, cloud computing, and the expanded application of e-commerce platforms have played a big role in how financial transactions are triggered and conducted [1]. Cloud computing has also come to be a key facilitator for banks, making data processing in real-time, reducing costs of operations, while making data sharing and analytics safe and over huge networks [2]. The cloud enabled financial inclusion, especially in rural and underdeveloped areas, making previously inaccessible financial services accessible [3]. Besides, mass use of the Internet of Things (IoT) in e-finance has facilitated smooth, real-time transactions, speeding up beyond conventional banking systems and becoming more dynamic and consumer-oriented [4]. With increasingly sophisticated digital banking systems, however, they become susceptible to more sophisticated types of fraud too, making fraud detection and prevention a top priority for banks worldwide.

The increase in financial transactions over the internet has resulted in a large number of fraud detection issues. The sheer volume of transactions taking place daily makes it difficult to monitor and detect fraud in real-time.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Cybercriminals are finding new ways to circumvent security, and methods such as deepfake identity fraud, phishing attacks, and AI-based exploits are being used [5]. Further, cloud-based solutions, though scalable and very efficient, pose newer threats. Cloud platforms are being increasingly targeted by hackers to target sensitive financial details and perform false transactions [6]. Moreover, the employment of centralized databases and traditional rule-based detection models opens systems to quick-changing fraudulent approaches. These models fail to cover new fraud patterns and generate too high false positives, which lead to inefficiencies as well as lose confidence in the system.

The existing fraud detection methods are predominantly rule-based and static machine learning-based, which are deficient in identifying complex and dynamic patterns of fraud. Rule-based models, although good at identifying known cases of fraud, fail to learn to maintain a pace with the changing methods of fraud and produce low rates of detection as well as false alarms [7]. Static machine learning models must be repeatedly trained to remain effective and are computationally intensive, unable to handle the growing size and complexity of financial transactions [8]. Also, scalability within these systems is typically limited by the rising volume of transactions, and they are incapable of processing large datasets in real-time. This makes them ineffective for modern digital banking platforms, where fraud detection must be fast as well as scalable.

To address such issues, we propose a Capsule Network (CapsNet), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) hybrid fraud detection model. Capsule Network enables the model to retain hierarchical relationships in transactional data more effectively, while CNNs learn spatial features and LSTMs learn temporal dependencies. This hybrid architecture enables the detection of advanced, new fraud patterns by learning to adapt to new fraud tactics without the need for constant retraining. In addition, with the application of deep learning techniques, our model provides better accuracy, scalability, and real-time detection of fraudulent transactions. The use of Capsule Networks reduces false positives significantly and improves detection accuracy compared to traditional systems and therefore is a reliable solution for cloud-based financial transactions security [9]. With this approach, we can offer a highly scalable, effective, and flexible fraud detection system that can secure digital banking systems from the rapidly changing threat landscape.

2. LITERATURE SURVEY

Applied to fraud detection systems, optimization is key to improving security and efficiency in these models. [10] details various optimization methods employed in secure Internet of Things (IoT) data sharing and, in the process, have a direct impact on the security features of fraud detection systems. Secure sharing of data between distributed systems while maintaining privacy is required in efficient fraud detection, particularly with cloud-based implementations. [11] offers Monte Carlo simulations, a powerful statistical tool used in financial networks. Fraud detection algorithms via such simulations have the ability to simulate various hypothetical fraud scenarios, providing robust vulnerabilities identification in transactional data prior to fraud occurring. Additionally, [12] presents applying Gaussian mixture models (GMMs) in secure data exchange in IoT ecosystems, a mechanism transferable to fraud detection systems. GMMs improve anomaly detection through the learning of the probability distribution of the transaction data and hence enhancing the ability of the system to detect unusual transaction patterns that can be employed for detecting fraudulent behavior. Furthermore, [13] highlights the requirement of dynamic load balancing of IoT platforms to ensure fraud detection models remain scalable and optimal. By distributing the computational load among various nodes, the system can process enormous amounts of data without compromising performance or accuracy of fraud detection.

Clustering and feature extraction are critical modules in any effective anti-fraud system. [14] is placed on categorical embeddings that underlie strong cloud-based financial analytics and facilitate processing and classification of complicated financial information. These embeddings change transactional information into one better suited to deep learning algorithms so that these are better suited to identify fraud trends. [15] discusses hybrid clustering methodologies, including DBSCAN and Fuzzy C-Means, which are quite useful for pattern

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

analysis of transactions in fraud detection systems. Such clustering algorithms enable the model to cluster transactions with respect to similarities in behavior and detect outliers or anomalous transactions that may pose a threat as fraud. By employing these algorithms, fraud detection systems can deal with big data efficiently while filtering out only important patterns.

Fraud detection mechanisms in monetary environments, specifically those that capitalize on IoT information, are moving very fast. [16] presents a quantitative analysis of urban-rural contrast and the plight of maintaining money inclusion in peripheral communities. It is made difficult by the issue of fraud discovery in areas that have less mature monetary systems and demands specialized strategies of fraud discovery that can successfully work in the given environments. [17] provides insightful contributions to predictive modeling paradigms in healthcare, an area where deep learning has been effectively utilized to identify abnormalities in patient information. The same deep learning algorithms can be tailored to financial fraud detection systems, enhancing their effectiveness and accuracy in detecting fraudulent patterns. [18] presents decentralized cultural co-evolutionary optimization, a strategy for optimizing data sharing of IoT in distributed systems. This method is very applicable to fraud detection in financial networks, where transactions occur at multiple nodes. By minimizing how the data is shared and analyzed, the fraud detection system is more efficient, scalable, and able to identify fraud within large, distributed networks.

2.1 Problem Statement

Digital banking fraud detection is hindered by changing fraud techniques and the complexities of high-value transaction data. Conventional systems, based usually on rule-based systems or shallow machine learning, are not responsive to new patterns of fraud. [19] points out that hybrid learning and neural fuzzy models have the capability to be incorporated in predictive models, such as fraud detection. [20] introduces reinforcement learning and DCGANs to be used for anomaly detection in financial data. [21] focuses on pattern recognition in clinical decision systems, which applies to detection of fraud in banking. [22] introduces decision trees as a basic algorithm for complex fraud detection. [23] also optimizes model training via PSO-TVAC to improve fraud detection accuracy.

3. METHODOLOGY:

The methodology begins with fetching transaction data from the cloud, and then preprocessing is done in the form of feature selection, normalization, and padding of sequences. Next, CNN-based feature learning is performed to learn spatial patterns from the transactions. Afterwards, LSTM is employed to capture the sequential user behavior over time. Capsule Network layer classifies transactions by preserving spatial hierarchies, and then fraud probability is predicted. The final output classifies transactions into valid or suspicious. (Figure 1).

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

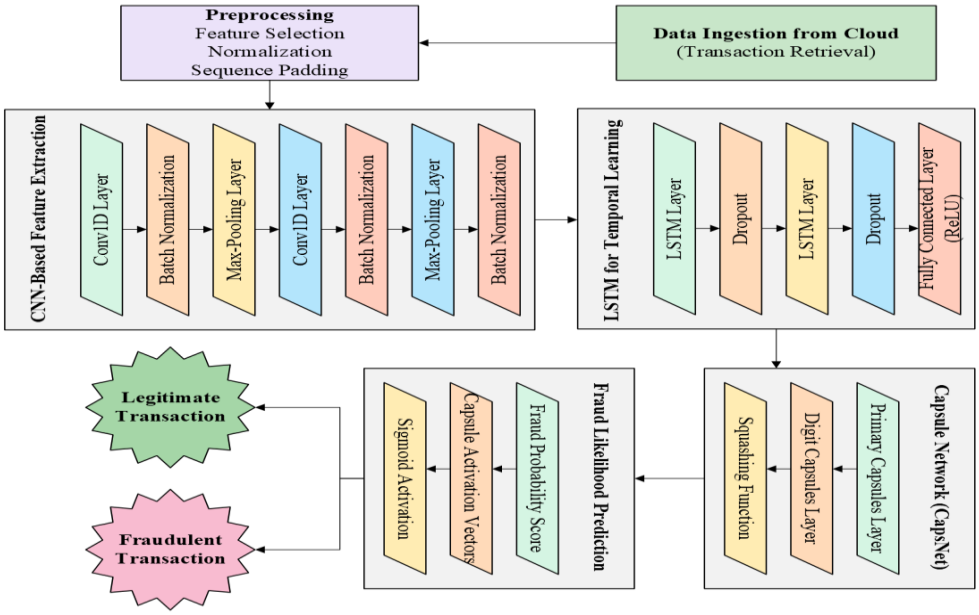

Figure 1: Architecture Diagram

3.1. Data Ingestion from Cloud

Banking transactions are fetched from the cloud database for processing in the fraud detection system. The data includes transaction information like amounts, timestamps, and user identifiers, which are required for feature extraction and fraud classification.

Banking transactions are retrieved from the cloud database for real-time fraud detection.

$$\mathcal{D} = \{X_k, Y_k\} \text{ where } X_k \in \mathbb{R}^m, Y_k \in \{0,1\} \quad (1)$$

- X_k represents the feature vector of the k -th transaction.
- Y_k is the label ($0 =$ legitimate, $1 =$ fraud).
- The dataset D is stored in the cloud and preprocessed before entering the model.

3.2 Data Preprocessing

The final step is cleansing and converting data to model input. It is encompassed within feature selection, normalization, and padding of the sequence to enable each transaction to possess similar format and values. Feature selection simply removes irrelevant features, whereas normalization makes the features homogeneous to the same range.

3.2.1 Feature Selection

Feature selection is the act of selecting the most pertinent transaction features. This process enhances the efficiency of the model by eliminating extraneous data and targeting the most informative features that help in successful fraud detection.

Only relevant features (F') are selected:

$$X'_k = X_k \cdot W'_F \quad (2)$$

Where, W'_F is a feature selection matrix that retains only important attributes.

3.2.2 Normalization (Min-Max Scaling)

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Normalization brings features of a transaction onto the same scale. This avoids letting the model have a bias towards features with higher magnitudes and makes all features contribute equally to the fraud detection.
To standardize transaction features:

$$X'_{norm} = \frac{x' - x'_{\min}}{x'_{\max} - x'_{\min}} \quad (3)$$

Where, $X'_{\min}, X'_{\max}$ represent the minimum and maximum values in the feature set.

3.2.3 Sequence Padding

Sequence padding guarantees transactions of different lengths are converted to inputs of equal size. This process is vital for models such as LSTM, which need constant sequence lengths in order to learn time-dependent patterns and identify fraud patterns.
For handling variable-length sequences, padding ensures all transactions have equal timestep lengths T.

$$X'_{\text{padded}} = [X'_1 \quad X'_2 \quad \dots \quad X'_T] \quad (4)$$

3.3. CNN-Based Feature Extraction

The Convolutional Neural Network (CNN) discovers spatial patterns of transaction features. It is capable of recognizing inherent relationships of transaction data through convolutional layers that are adept at identifying local dependencies, necessary to detect fraud within transaction metadata.
CNN extracts spatial relationships in transaction data using 1D Convolutional Layers.

3.3.1 Convolutional Layer

The convolutional layer carries out the central function of feature extraction through the convolution of transaction data with filters. Patterns are identified and feature maps that summarize significant features of the transactions are produced, thus facilitating enhanced fraud detection.
Feature maps (Fl′) are generated by applying filters (W_l') with stride s.

$$F_l' = \sigma(W_l' * X' + b_l') \quad (5)$$

Where, * is the convolution operation, W_l' and b_l' are the filter weights and biases, σ is the ReLU activation function.

3.3.2 Max-Pooling Layer

Max-pooling diminishes the spatial size of the feature maps, preserving only the salient information. This downsampling process lessens computation and highlights the most prominent patterns in transactional data that help identify fraudulent activities.
Downsamples the feature maps to retain key features.

$$P_l' = \max(F_l') \quad (6)$$

Where, P_l' is the pooled feature vector.

3.4 LSTM for Temporal Dependency Learning

Long Short-Term Memory (LSTM) networks learn sequence transactions' temporal dependencies. It is a vital step to realize user spending behavior and find anomalies over time to enable the model to detect sequenced fraud.
LSTM captures sequential transaction patterns over time.

3.4.1 LSTM Cell Computation

LSTM cells learn transaction sequences using gates to regulate the flow of data. Forget, input, and output gates assist in determining what information to keep or forget, and the memory cell retains the learnt patterns of transaction behavior over time.
Each LSTM unit updates its hidden state based on the input.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

$$f_t' = \sigma\left(W_f' \cdot [h_{t-1}', x_t'] + b_f'\right)$$
$$i_t' = \sigma(W_i' \cdot [h_{t-1}', x_t'] + b_i')$$
$$\tilde{C}_t' = \tanh\left(W_C' \cdot [h_{t-1}', x_t'] + b_C'\right) \quad (8)$$
$$C_t' = f_t' \odot C_{t-1}' + i_t' \odot \tilde{C}_t'$$
$$o_t' = \sigma(W_o' \cdot [h_{t-1}', x_t'] + b_o')$$
$$h_t' = o_t' \odot \tanh\left(C_t'\right) \quad (9)$$

Where, f_t', i_t', o_t' are the forget, input, and output gates, C_t' is the memory cell state, h_t' is the hidden state.

3.5. Capsule Network for Classification

CapsNet is utilized for the end-classification of transactions. It models spatial hierarchies and spatial relationships between features, allowing more effective fraud detection by capturing subtle patterns and maintaining significant features that standard CNNs may not pick up.

3.5.1 Primary Capsules Layer

The main capsules layer transforms the extracted features from CNN and LSTM layers into capsules, which are abstractions of higher levels of the data. The capsules contain both the existence and spatial information of the patterns of fraud.

Converts extracted features into capsule vectors.

$$u_i' = W_{\text{caps}}' \cdot X' \quad (9)$$

Where, u_i' is the input capsule representation, W_{caps}' represents learned capsule weights.

3.5.2 Squashing Function

The squashing function makes sure that the norm of every capsule vector falls within the range of 0 and 1. This normalizes the capsule outputs, avoiding the large activations and making sure only the most significant features are fed to the next layer.

Ensures each capsule vector has a magnitude between 0 and 1.

$$v_j' = \frac{\left\|s_j'\right\|^2}{1+\left\|s_j'\right\|^2} \frac{s_j'}{\left\|s_j'\right\|} \quad (10)$$

Where, S_j' is the sum of weighted inputs.

3.5.3 Dynamic Routing

Dynamic routing is an iterative process whereby capsules interact and tune their weights. This causes the appropriate capsules to contribute towards the output, enhancing the capability of the model to classify transactions accurately by retaining complicated spatial relations within the data.

Capsules interact through an iterative routing process.

$$c_{ij}' = \frac{\exp\left(b_{ij}'\right)}{\sum_k \exp\left(b_{ik}'\right)} \quad (11)$$

Where, b_{ij}' represents the agreement between capsule i and j.

3.6. Hybrid Equation: CNN-LSTM-Capsule Integration

The outputs of CNN and LSTM are fused and fed to the Capsule Network for the classification of fraud. The spatial features are detected by the CNN, temporal dependency is detected by the LSTM, and the Capsule Network enforces that rich relationships between features of transactions are learned for detecting fraud accurately.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

The combined output of CNN and LSTM is processed by the Capsule Network for fraud classification. The hybrid equation for fraud likelihood prediction is:

$$F_t' = \text{CNN}(X') \text{ and } h_t' = \text{LSTM}(F_t') \quad (12)$$

Where, F_t' is the output of the CNN feature extraction, h_t' is the temporal sequence information extracted by LSTM.

The Capsule Network then refines the combined features ht' for fraud detection.

$$P(Y = 1 \mid X') = \sigma\left(W_{\text{fraud}}' \cdot v_j' + b'\right) \quad (13)$$

Where, $\hat{y}_t$ is the final fraud likelihood score.

3.7. Fraud Likelihood Prediction

Fraud probability is forecasted by examining the capsule activation vectors. The ultimate probability of a transaction being fraudulent is calculated using the output of the Capsule Network, which is applied to a sigmoid function to yield a probability value between 0 and 1.

Fraud probability is computed from capsule activation vectors.

$$P(Y = 1 \mid X') = \sigma\left(W_{\text{fraud}}' \cdot v_j' + b'\right) \quad (14)$$

Where, W_{fraud}' is the weight matrix for fraud classification, v_j' is the output capsule, σ is the Sigmoid activation function.

3.8. Final Decision & Cloud Storage

When the model identifies fraud, the transaction is marked and stored in the cloud for auditing purposes. This permits financial institutions to correct the issues and have a safe record of marked transactions to analyze later.

Flagged fraudulent transactions are stored in the cloud for auditing.

$$\text{Flag} = \begin{cases} 1, & \text{if } P(Y = 1 \mid X') \geq \tau \\ 0, & \text{otherwise} \end{cases} \quad (15)$$

Where, τ is the fraud detection threshold.

- Transactions with fraud probability above τ are flagged.

4. RESULTS AND DISCUSSION

4.1 Dataset Description

The PaySim dataset [24] 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.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

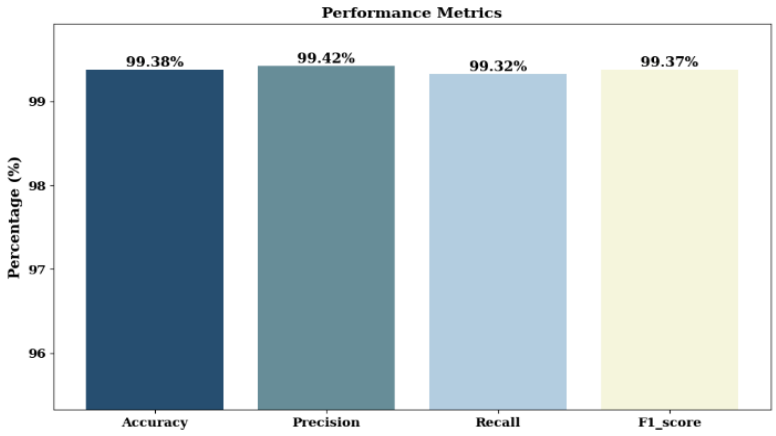

Figure 2 Performance Metrices

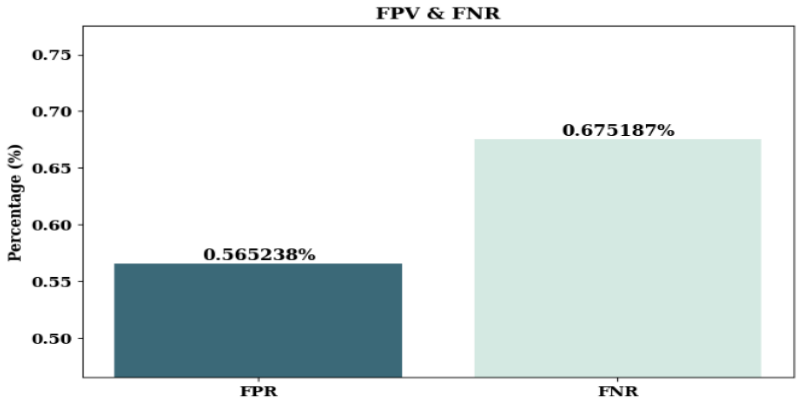

Figure 3 Performance of FPR and FNR

The performance of the proposed FraudGuard model shows outstanding results on critical measures. Without compromising on 99.38% accuracy and false alarms, the accuracy of the model at 99.42% precision effective fraud detection. The model also gets 99.32% recall, which is clearly shown to detect fraudulent transactions, and 99.37% F1-score, which accurately achieves a balance between recall and precision for best performance. The outcomes establish the effectiveness of the model (Figure 2).

The stability of the model is reflected in the False Positive Rate (FPR) and False Negative Rate (FNR). There are quite low cases of legal transactions being detected as fraud, as revealed by the FPR of 0.565%. The FNR is 0.675%, representing a slightly higher ratio of unidentified fraudulent activity. The above measurements reveal the reliability of the model to identify fraud (Figure 3).

5. CONCLUSION

This paper presents FraudDetectNet, a novel fraud detection model that employs a hybrid framework of Capsule Networks, CNNs, and LSTMs to overcome the shortcomings of conventional fraud detection systems. The spatial and temporal pattern capture capability of the model improves its performance in detecting dynamic fraudulent patterns while reducing false positives. Experimental results show the better performance of FraudDetectNet, with high recall and accuracy rates, offering a strong solution for real-time fraud detection in online banking scenarios. Future research may involve further optimization, including the use of online learning techniques to improve the model's adaptability to new and emerging fraud trends.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

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] 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.

[5] 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

[6] 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

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

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] 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

[23] 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.

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