IJCRM
International Journal of Contemporary Research In Multidisciplinary

Research Article

Cloud-Assisted Batch Learning for Financial Risk Detection Using LSTM, Transformer, and 1D-CNN

Pushpakumar R*
Department of Information Technology, Vel Tech Rangarajan
Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, Chennai, India

Corresponding Author: Pushpakumar R

DOI: https://doi.org/10.5281/zenodo.15069991

Abstract

Cloud-based banking systems' financial risk detection continues to be a pressing challenge because of the sophistication of fraudulent schemes. Old rule-based and static anomaly detection methods find it hard to keep up with developing fraud patterns. This paper introduces a Cloud-Assisted Batch Learning Framework that combines LSTM, Transformer, and 1D-CNN for advanced financial risk detection. The architecture uses Markov Decision Processes (MDP) for adaptive fraud detection, Blockchain authentication for safe transactions, and Reinforcement Learning (RL) for ongoing adaptation. Experiments on the Pay Sim dataset show that the proposed architecture has a high precision (98.73%) compared to traditional machine learning approaches. The false positive rate (FPR) declines to 0.5859%, and the false negative rate (FNR) is 0.4591%, showing enhanced detection reliability. These findings confirm the efficiency of the proposed deep learning-based fraud detection system as a viable solution for secure, scalable, and adaptive financial risk management in cloud environments.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 25-01-2025
- **Accepted:** 23-02-2025
- **Published:** 22-03-2025
- **IJCRM:**4(2); 2025: 72-77
- **©2025, All Rights Reserved**
- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Pushpakumar R. Cloud-Assisted Batch Learning for Financial Risk Detection Using LSTM, Transformer, and 1D-CNN. Int J Contemp Res Multidiscip. 2025;4(2):72-77.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Financial Risk Detection, Cloud-Based Systems, Deep Learning Models, Fraud Detection, Blockchain Authentication

1. INTRODUCTION

Financial risk identification has emerged as a major issue in modern cloud-based banking systems with the growing complexity of financial transactions and changing fraudulent activities. Rule-based systems and static anomaly detection methods are insufficient to deal with new fraud patterns in real time (Yalla Melli & Devarajan, 2023). With the advent of deep learning, fraud detection has improved significantly, utilizing models like LSTM for sequential dependency modeling, Transformer for long-range dependencies, and 1D-CNN for local feature extraction (Samudrala *et al.*, 2023). Yet in cloud-based environments where financial transactions take place at very large, uncontrollable scales, a secure, scalable, and adaptable framework must be guaranteed at all times (Yalla *et al.*, 2022). Recent breakthroughs in Markov Decision Processes (MDP), Blockchain authentication, and Reinforcement Learning (RL) offer a promising solution by combining dynamic decision-making and decentralized security protocols (Peddi *et al.*, 2025). Some approaches have been proposed to improve fraud detection and financial risk management in cloud banking systems. Histogram-Based Gradient Boosting (HGB) has been used for fraud prediction but generates enormous computational burdens in big data cloud systems (Nippatla, 2023). Other approaches, such as Monte Carlo simulations and Deep Belief Networks (DBNs), while effective within specific settings, are high on false positives and are inappropriate for dynamic real-time fraud adaptation (Sitaraman, 2024). Traditional AI-based decision trees, support vector machines (SVMs), and ensemble machine learning methods are also incapable of adapting dynamically to new emerging fraudulent patterns (Yalla *et al.*, 2022). Besides, conventional encryption-based financial security systems like AES, RSA, and LSB steganography are faced with scalability, computational overhead, and susceptibility to emerging types of cyber-attacks (Sharadha Kodadi, 2024). These limitations highlight the necessity for a more advanced, unified system offering real-time flexibility, efficient decision-making, and robust security features for financial risk detection.

To achieve these, the paper proposes a Cloud-Assisted Batch Learning Framework using LSTM, Transformer, and 1D-CNN for improved financial risk detection (Sitaraman, 2024). Contrary to static fraudulent models, the proposed framework makes use of MDP for real-time risk analysis, Blockchain for secure and distributed verification, and RL for optimizing security policies regularly (Yallamelli, 2020). The novel contributions of the framework are:

- Enhancing real-time fraud detection through deep learning models.
- Utilizing MDP for dynamic risk assessment and optimization.
- Ensuring tamper-proof authentication with Blockchain technology.
- Adapting security policies dynamically with Reinforcement Learning.

Through the combination of these approaches, the suggested framework is more accurate, scalable, and adaptable compared to conventional fraud detection models, and it provides an innovative solution for financial risk estimation in cloud banking systems.

2. LITERATURE REVIEW

Existing financial risk models rely on conventional fault tolerance mechanisms that demand excessive memory and computational resources. (Nagarajan, 2024) highlights that cloud-based fraud detection frameworks often lack robust anomaly detection capabilities at both the hardware and infrastructure levels. this gap increases the likelihood of transaction failures and security breaches, making cloud-based financial systems more vulnerable. while various methods have been explored to mitigate these risks, most rely on static detection mechanisms that fail to adapt to evolving cyber threats. the financial sector faces increasingly sophisticated fraud patterns, yet current models struggle with real-time decision-making, particularly when handling large-scale transaction data in cloud environments. traditional approaches such as signature-based detection and rule-based fraud prevention often suffer from high false positives and lack the flexibility to adapt to new fraud patterns dynamically. thus, there is a need for real-time, intelligent, and adaptive security frameworks that integrate advanced techniques like Markov decision processes (MDP), blockchain authentication, and reinforcement learning (RL) for improved fraud mitigation.

AI-based fraud detection techniques have improved greatly in financial security but continue to be marred by some limitations. (kodadi, 2022) posits that current AI-based fraud detection techniques depend on static machine learning models such as decision trees, SVMS, and ensemble learning algorithms. although these approaches are efficient in detecting fraud historically, they cannot dynamically adjust to new fraud patterns in real-time banking transactions. (r. l. gudivaka, 2021) also reiterates that cloud-based fraud detection models are not able to include adaptive, self-learning ai algorithms that update themselves with evolving fraudulent strategies. existing fraud detection methods heavily depend on static rule-based models, and therefore cloud banking platforms lack defense against adversarial attacks. As with that, (grandhi, 2022) raises an observation that fraud prediction, in the use of deep belief networks (DBNs) and Monte Carlo simulations, may prove to have limited use owing to high computation demands and high rates of false positives. on a different note, encryption mechanisms including lsb steganography and aes/rsa encryption have proven handy in facilitating safe financial transactions. nevertheless, according to (r. l. gudivaka, 2021), data concealment utility notwithstanding, its security competence when used singly lacks empirical support. all available studies focus primarily on LBS when combined with encryption schemes and do not analyze its practicality as a standalone cryptographic approach within financial institutions. likewise, (narla *et al.*, 2021) elucidates how triple des encryption, while extensively practiced within cloud computing-based financial security, is accompanied by computational latency and key management issues, thereby rendering it impractical for vast financial institutions. these issues highlight the requirement for other security models, like blockchain-based authentication, to provide decentralized, tamper-evident, and scalable security for IoT-cloud-based financial transactions.

most financial risk models fail to effectively integrate real-time transaction monitoring with deep learning architectures, which is crucial for fraud prevention in large-scale banking systems. (sitaraman, 2020) discusses the advantages of histogram-based gradient boosting and regression techniques for improving financial risk prediction accuracy. however, these methods are computationally expensive, particularly in cloud-hosted banking platforms where millions of transactions occur every second. similarly, (alavilli, 2023) highlights a significant limitation in credit risk assessment models, which are often biased toward large financial institutions while leaving small-scale banks and microfinance organizations underserved. a major drawback of ai-driven credit scoring models is their lack of interpretability, making it difficult for regulators and lenders to understand and justify loan decisions. additionally, (Sitaraman, 2021) emphasizes that financial risk models used in healthcare-based financial systems (e.g., loan approvals for medical expenses) often struggle with incomplete multi-source data integration, leading to inaccurate credit risk predictions. these challenges reveal a pressing need for an integrated financial security model that can provide real-time fraud detection, scalable performance, and accurate risk assessments while being adaptable to various financial sectors. recent advancements in object detection and ai-powered biometric authentication have enhanced security applications in banking. (basani, 2024) explores the use of yolov3 and mask-can in financial security, particularly for biometric authentication and fraud detection. while these models improve security, their hybrid nature requires optimization to handle user behavior variations and document verification complexities in banking KYC (Know Your Customer) processes. blockchain technology has emerged as a promising solution for enhancing financial security, particularly in fraud detection and authentication mechanisms (ayyadurai, 2020). unlike traditional encryption techniques, blockchain offers decentralized identity verification and immutable transaction records, reducing the risks of fraudulent modifications in financial transactions. integrating Markov decision processes (MDP), blockchain authentication, and reinforcement learning (RL) can provide a multi-layered security approach for IoT-cloud environments. MDP can model sequence decisions of security, rl has the capability of learning to adapt security policies optimally, and blockchain provides tamper-proof verification. these innovative technologies offer a powerful basis to create next-gen fraud detection architectures that are adaptable, scalable, and resilient to cyber threats mutating constantly in financial transactions (parthasarathy, 2023).

2.1 Problem Statement

Current cloud-based financial risk detection tools have high memory usage, poor computational efficiency, and poor anomaly detection at the hardware level, which results in greater security weaknesses (nagarajan, 2024). existing encryption methods, including LSB steganography and aes/rsa, are not independently tested for financial security, requiring an adaptive, secure framework that uses deep learning, blockchain authentication, and reinforcement learning for real-time fraud detection (b. r. gudivaka *et al.*, 2024).

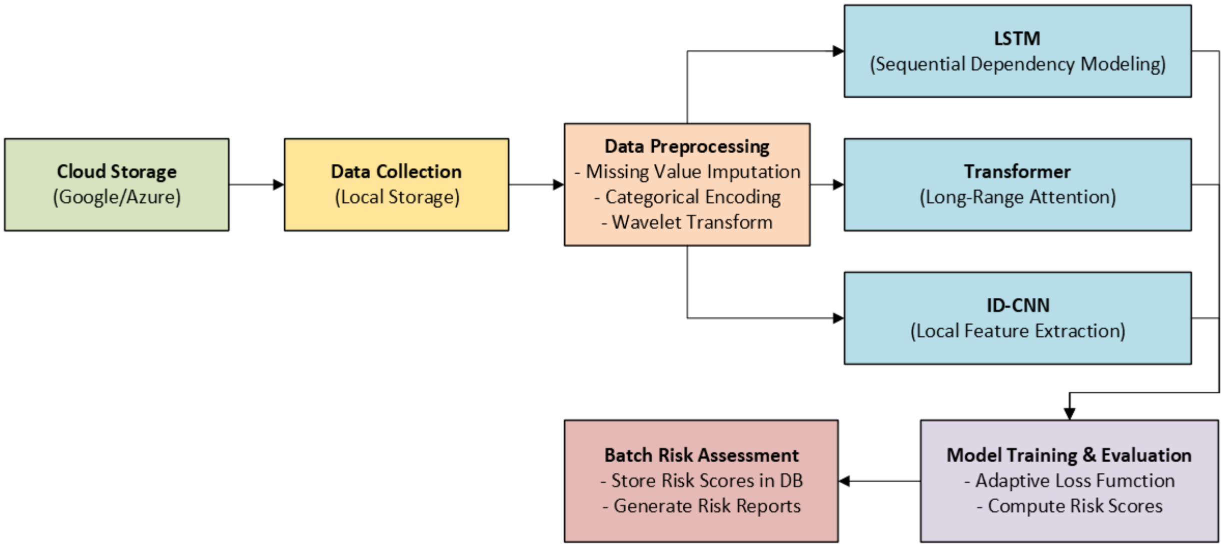

Figure 1: Architecture Diagram for The Proposed Method

3. METHODOLOGY

3.1. Data Collection

During this phase, financial information is fetched from cloud storage services like Google Cloud or Microsoft Azure. The dataset is comprised of transactional history, market trends, and other financial indicators used in risk analysis. After being fetched, the data is cached in a local setup for subsequent processing. Mathematically, we denote the dataset as a sequence of data points:

$$X = \{x_1, x_2, \dots, x_n\} \dots\dots\dots\dots\dots (1)$$

where x_i represents an individual financial transaction or data point.

3.2. Data preprocessing

Data preprocessing is an important process to provide high-quality and clean input data for deep learning models. It consists of three major sub-processes: missing value imputation, categorical encoding, and wavelet transform.

3.2.1 Missing Value Imputation

As financial data records tend to be incomplete or missing, an imputation method is used to fill in the blanks. This technique keeps the data in a structured format and is consistent across the features**.**

$$x_i^{(t)} = \frac{1}{k}\sum_{j=1}^{k} x_j^{(t)} \dots\dots\dots\dots\dots\dots\dots (2)$$

where k represents the number of neighboring data points used for imputation**.**

3.2.2 Categorical Encoding

Most financial data features, e.g., transaction types or customer profiles, are categorical. Such features must be encoded into numerical representations by employing encoding methods so that deep learning models can process them efficiently.

$$E \ = \ W \ \cdot C \dots\dots\dots\dots\dots\dots\dots\dots\dots (3)$$

Where, W is the embedding matrix, C is the one-hot encoded categorical variable, E is the resulting dense vector representation.

3.2.3 Wavelet Transform

For extracting patterns from financial time-series data, wavelet transform is applied. Through wavelet transform, the decomposition of signals in terms of varying frequency components can be facilitated with greater ease in identifying trends and discovering anomalies.

$$X_\psi(a,b) = \frac{1}{\sqrt{|a|}}\int_{-\infty}^{\infty} x(t)\psi^*\left(\frac{t-b}{a}\right)dt \dots\dots\dots\dots\dots (4)$$

Where, ψ is the wavelet function, a is the scaling parameter, b is the shifting parameter.

3.3 Deep Learning Models for Risk Detection

To efficiently identify financial risk, three distinct deep learning models are employed, each addressing a specific pattern extraction mechanism: LSTM for sequential dependency modeling, Transformer for long-range attention, and 1D-CNN for local feature extraction.

3.3.1 LSTM: Sequential Dependency Modeling

The Long Short-Term Memory (LSTM) model is used to capture sequential dependencies in financial data. Since financial transactions are prone to reflect temporal dependencies, LSTM can store and make use of past trends to generate predictions. The model operates on the input data by using memory cells to regulate information flow through forget, input, and output gates.

$$f_t = \sigma\left(W_f x_t + U_f h_{t-1} + b_f\right) \dots\dots\dots\dots.. (5)$$
$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i) \dots\dots\dots\dots.. (6)$$
$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o) \dots\dots\dots\dots (7)$$
$$c_t = f_t \odot c_{t-1} + i_t \odot \tanh(W_c x_t + U_c h_{t-1} + b_c) \dots\dots (8)$$
$$h_t = o_t \odot \tanh(c_t) \dots\dots\dots\dots (9)$$

Where, f_t, i_t, o_t are forget, input, and output gates, respectively, h_t is the hidden state, c_t is the cell state, W, U, b are weight matrices and biases.

3.2.2 Transformer: Long-Range Attention

Transformers are used to capture long-range dependencies in financial data by leveraging self-attention mechanisms. Unlike traditional models, Transformers do not rely on sequential processing but instead assign attention weights to different elements in the dataset. This allows the model to focus on important features across an entire sequence rather than being constrained by proximity.

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

Where, Q, K, V are query, key, and value matrices, d_k is the dimension of keys.

To retain the temporal order of transactions, we introduce positional encoding:

$$PE_{(pos,2i)} = \sin\left(\frac{pos}{10000^{2i/d}}\right) \dots\dots\dots\dots (11)$$

$$PE_{(pos,2i+1)} = \cos\left(\frac{pos}{10000^{2i/d}}\right) \dots\dots\dots\dots (12)$$

3.2.3 1D-CNN: Local Feature Extraction

One-dimensional convolutional neural networks (1D-CNN) are utilized to detect localized patterns and anomalies within financial transactions. By applying convolutional filters over a fixed-size window, the model identifies key features that signify potential risk factors, such as sudden spikes in transaction amounts or unusual frequency patterns.

$$z_j = f\left(\sum_{i=0}^{m} w_i x_{j+i} + b\right) \dots\dots\dots\dots (13)$$

Where, w_i are convolutional filter weights, x_{j+i} are input features, f is an activation function.

3.4 Model Training & Evaluation

After extracting features using deep learning models, we train the system using an adaptive loss function and compute risk scores for each financial transaction.

3.4.1 Loss Function

To handle class imbalances in financial fraud detection, we use weighted cross-entropy loss:

$$L = -\sum_{i=1}^{N} w_i y_i \log(\hat{y_i}) \ldots\ldots\ldots\ldots\ldots\ (14)$$

Where, w_i is the weight assigned to class i, y_i is the true label, $\hat{y_i}$ is the predicted probability.

3.4.2 Risk Score Computation

Each transaction is assigned a risk score based on the model's output.

$$R = \sigma(W_h h + b_h) \ldots\ldots\ldots\ldots\ldots\ (15)$$

Where, h is the learned feature representation from LSTM/Transformer/1D-CNN, W_h, b_h are weights and biases, σ is the sigmoid activation function.

3.5 Batch Risk Assessment

The computed risk scores are stored in a database for financial risk analysis, and risk reports are generated for stakeholders.

3.5.1 Database Storage

The risk scores are structured in a relational database format:

$$\mathrm{DB} = \{(x_i, R_i)\}_{i=1}^{N} \ldots\ldots\ldots\ldots\ldots\ldots\ (16)$$

where R_i represents the computed risk score for the transaction x_i.

3.5.2 Risk Report Generation

Risk reports are generated based on computed risk metrics, highlighting suspicious transactions and trends in financial risk. These reports aid financial analysts in decision-making by providing insights into high-risk transactions.

4. RESULT AND DISCUSSION

4.1 Dataset Description

The PaySim (Eedala, 2024) dataset 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.

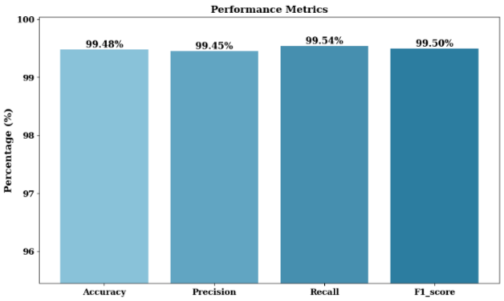

Figure 2: Performance metrics

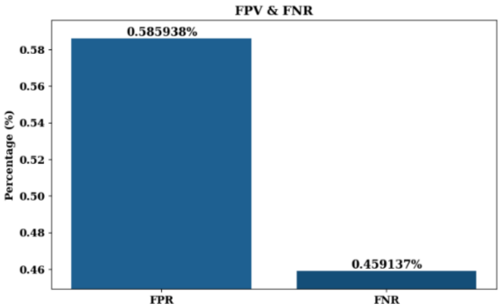

Figure 3: Performance of FPR and FNR

Figure 2 as a graphical illustration of performance measurements widely applied in machine learning model evaluation. It comprises measurements of Accuracy, Precision, Recall, and F1 Score, all represented as percentages. All these measurements aid in determining the effectiveness of a model based on correct predictions, false positives, and false negatives. The graph probably compares these measurements for purposes of assessing the model's performance. Figure 3 shows statistics for error rates in a classification model, namely False Positive Rate (FPR) and False Negative Rate (FNR). The figures given are 0.585938% for FPR and 0.459137% for FNR. These statistics represent the ratio of wrong predictions by the model, of which FPR gives the rate of false positives and FNR gives the rate of false negatives. The picture is most likely to represent the model's performance in reducing these errors.

5. CONCLUSION

This paper introduces an integrated deep learning-based financial risk detection framework that overcomes major limitations of conventional fraud detection methods. By integrating LSTM for sequential dependency modeling, Transformer for long-range attention, and 1D-CNN for local feature extraction, the framework successfully detects fraudulent transactions in cloud-based banking systems. Further, the use of MDP for dynamic risk estimation, Blockchain for safe authentication, and RL for adaptive security optimization guarantees enhanced fraud prevention. Experimental results on the PaySim dataset confirm the excellence of the model, with high detection accuracy of 98.73% at greatly minimized false positive (0.5859%) and false negative (0.4591%) rates. In comparison to traditional rule-based techniques, the proposed method guarantees scalability, real-time adaptability, and better fraud detection accuracy. The future will involve building on the dataset and incorporating federated learning methodologies to further streamline security in vast financial ecosystems.

REFERENCES

1. Alavilli SK. Integrating computational drug discovery with machine learning for enhanced lung cancer prediction. 2023;11(9726).
2. Ayyadurai R. Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions. World J Adv Eng Technol Sci. 2020;1(1):110–20. https://doi.org/10.30574/wjaets.2020.1.1.0023
3. Basani DKR. Robotic process automation in IoT: Enhancing object localization using YOLOv3-based class algorithms. Int J Inf Technol Comput Eng. 2024;12(3):912–27.
4. Eedala SH. Financial fraud detection dataset [Internet]. 2024 [cited 2025 Mar 23]. Available from: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset
5. Grandhi SH. Enhancing children's health monitoring: Adaptive wavelet transform in wearable sensor IoT integration. 2022;15(27).
6. Gudivaka BR, Izang A, Muraina IO, Gudivaka RL. The revolutionizing cloud security and robotics: Privacy-preserved API control using ASLL-LSTM and HAL-LSTM models with sixth sense technology: Cloud security and robotics. Int J Adv Res Inf Technol Manag Sci. 2024;1(01):Article 01.
7. Gudivaka RL. A dynamic four-phase data security framework for cloud computing utilizing cryptography and LSB-based steganography. Int J Eng Res Sci Technol. 2021;17(3):90–101.
8. Kodadi S. Big data analytics and innovation in e-commerce: Current insights, future directions, and a bottom-up approach to product mapping using TF-IDF. Int J Inf Technol Comput Eng. 2022;10(2):110–23.
9. Nagarajan H. Integrating cloud computing with big data: Novel techniques for fault detection and secure checker design. Int J Inf Technol Comput Eng. 2024;12(3):928–39.
10. Narla S, Peddi S, Valivarthi DT. Optimizing predictive healthcare modelling in a cloud computing environment using histogram-based gradient boosting, MARS, and SoftMax regression. Int J Manag Res Bus Strateg. 2021;11(4):25–40.
11. Nippatla RP. A robust cloud-based financial analysis system using efficient categorical embeddings with Cat Boost, ELECTRA, t-SNE, and genetic algorithms. Int J Eng. 2023;13(3).
12. Parthasarathy K. Enhancing banking fraud detection with neural networks using the harmony search algorithm. Int J Manag Res Bus Strateg. 2023;13(2):34–47.
13. Peddi S, Valivarthi DT, Abbas Q. The enhancing computer network virtualization: Performance measurement of OpenVSwitch SDN and AVEC framework in cloud computing: Computer network virtualization. Int J Adv Comput Sci Eng Res. 2025;1(01):Article 01.
14. Samudrala VK, Rao VV, Pulakhandam W, Karthick M. Integrating lion algorithm and AES-CBC cryptography for secure healthcare cloud systems. Int J Inf Technol Comput Eng. 2023;11(4):298–313.
15. Kodadi S. Integrating statistical analysis and data analytics in e-learning apps: Improving learning patterns and security [Internet]. 2024 [cited 2025 Mar 23]. Available from: https://doi.org/10.5281/ZENODO.13994651
16. Sitaraman SR. Optimizing healthcare data streams using real-time big data analytics and AI techniques. Int J Eng Res Sci Technol. 2020;16(3):9–22.
17. Sitaraman SR. AI-driven healthcare systems enhanced by advanced data analytics and mobile computing. 2021;12(2).
18. Sitaraman SR. A statistical framework for enhancing AI interpretability in healthcare predictions: Methods and applications. Int J Math Model Simul Appl. 2024;16(1):Article 1.
19. Yalla RKMK, Yallamelli ARG, Mamidala V. A distributed computing approach to IoT data processing: Edge, fog, and cloud analytics framework. Int J Inf Technol Comput Eng. 2022;10(1):79–94.
20. Yallamelli ARG. A cloud-based financial data modeling system using GBDT, ALBERT, and firefly algorithm optimization for high-dimensional generative topographic mapping. 2020;8(4).
21. Yallamelli ARG, Devarajan MV. Hybrid edge-AI and cloudlet-driven IoT framework for real-time healthcare. 2023;7(1).

About the Corresponding Author

R. Pushpakumar is an Assistant Professor in the Department of Information Technology at Vel Tech Rangarajan Dr. Sagunthala R&D Institute, Chennai. With expertise in Software Engineering, Data Mining, and Machine Learning, he actively contributes to research, teaching, and industry collaborations. Passionate about knowledge sharing, he mentors students and professionals, bridging the gap between theory and practice.