Cloud-Based Fraud Detection System for Healthcare Payments Using Sparse Autoencoders

Sunil Kumar Alavilli[1], Bhavya Kadiyala[2], Rajani Priya Nippatla[3], Subramanyam Boyapati[4], Chaitanya Vasamsetty[5], Purandhar N[6,*]
[1]Sephora, California, USA Email: sunilkumaralavilli@ieee.org
[2]Parkland Health, Texas, USA Email: bhavyakadiyala@ieee.org
[3]Kellton Technologies Inc, Texas, USA Email: rajanipriyanippatla@ieee.org
[4]American Express, Arizona, USA Email: subramanyamboyapati@ieee.org
[5]Elevance Health, Georiga, USA Email: chaitanyavasamsetty@ieee.org
[6]Assistant Professor, Department of CSE (Artificial Intelligence)
School of Computers, Madanapalle Institute of Technology and Science,
Madanapalle, College code – 69, Andhra Pradesh - 517325, India
Email: purandhar.n@gmail.com
*Corresponding Author: Purandhar N Corresponding Author Email: purandhar.n@gmail.com

Abstract— *Healthcare fraud is a serious problem that exposes the financial sustainability of healthcare systems as well as their operational integrity. Yet, increased size and complexity in terms of data have made traditional rule-based systems inadequate for detection of fraud in healthcare. This paper presents a cloud-based fraud detection system for fraudulent healthcare payment transactions. The system starts with a data collection from cloud storage where the healthcare data is securely stored, followed by preprocessing steps including handling of missing values and Z-score normalization used to standardizes the numerical features. After that, Principal Component Analysis is used in feature extraction to reduce the dataset's dimensionality while keeping the most important feature information. Finally, sparse autoencoders learn the normal transaction patterns and any deviations from them are flagged as potentially fraudulent activities by the fraud detection system. The performance of the model has been measured with an accuracy of 0.990, precision of 0.997, sensitivity of 0.982 and specificity of 0.997. Latency analysis shows that as the data size increases from 1 GB to 100 GB, latency rises from 36 ms to 557 ms. This model provides an excellent performance in terms of fraud detection for healthcare payments.*

Keywords— *Healthcare data, Cloud Storage, Fraud Detection, Sparse Autoencoders, Principal Component Analysis.*

I. INTRODUCTION

Fraudulent activities in health systems adversely affect the financial performance of the institutions, compromise the quality of care delivered to patients [1], [2], [3], [4]. As all healthcare systems are now shifting to digital platforms, the enormous amount of data generated-from insurance claims to medical records-made it possible for fraudulent transactions to spike [5] [6]. It includes applications for false claims and billing anomalies costing billions of dollars' worth of losses every year [7], [8], [9]. The need for credible mechanisms for fraud detection in healthcare has, therefore, never been more urgent: they safeguard not only financial resources but also trust and integrity in global healthcare systems [10] [11].

Fraud detection has more challenges, given that the volume and complexity of healthcare data-with medical codes, details about a patient, billing information and treatment history- form many variables [12] [13]. In most cases traditional methods for fraud detection can't match the depth and variety of fraud schemes prevailing nowadays [14], [15], [16]. Also, it is time-consuming and human error-prone to do the manual review of such big datasets, thus making it inevitable to find new, data driven, automated solutions [17] [18], [19]. The combination of added advanced technologies such as machine learning and cloud computing definitely opens up new avenues for developing very accurate, efficient and scalable solutions for enhancing fraud detection capabilities [20], [21], [22].

With the digital transformation of the healthcare sector going on, artificial intelligence and cloud technologies offer an opportunity to help resolve the persistent issues surrounding fraud detection [23] [24], [25]. Via cloud platforms that can handle enormous amounts of data and AI-powered models for analysis, these solutions considerably bolster a healthcare firm's ability to detect and prevent fraudulent activity [26], [27], [28]. Thus, making way for better financial performance, the evolution also improves the integrity of the healthcare service providers to offer a secure environment for patients and providers [29] [30].

The paper is structured as follows: it begins with a literature survey reviewing existing approaches to secure healthcare data storage. The methodology section describes the framework for data collection, Preprocessing, Feature Extraction, and Fraud detection. The results section evaluates the system's performance, followed by a conclusion summarizing key findings and future directions.

II. LITERATURE SURVEY

In the analysis undertaken by Ganesan Thirusubramanian [31], AI-machine learning detection of frauds occurring in the domain of finance is the specific topic considered in a perspective of the Internet of Things (IoT). The work discusses the use of new algorithms like anomaly and cluster-based approaches that analyze large streams of IoT data to detect fraudulent activities. In training the supervised and unsupervised learning models on historical transaction data, fraud detection accuracy was improved. Validity was enhanced through adaptive learning with methods based on retraining and automatic responses to frauds. However, their drawbacks included challenges with data quality and computational complexity, as well as dynamic changes in the setting of fraud, greatly affecting the capacity for fraud detection.

Thirusubramanian Ganesan et al. [32] propose a cutting-edge mechanism called P2DS (Proactive Dynamic Secure Backup Data Scheme), which amasses financial data in mobile cloud environments. The study aimed to address the mounting security concerns in financial institutions by integrating with Attribute-Based Encryption, Attribute-Based Semantic Access Control and the Proactive Determinative Access scheme. Any framework used must be efficient in encryption, accurate in access control, as well as fast in responding to threats. Because of these P2DS made itself a reliable way for securing sensitive financial data in dynamically changing digital environments. Some limitations found in this study are computational overhead, scalability and potential vulnerabilities due to emerging cyber threats.

The security of IoT business models in elderly healthcare has been studied by Ganesan Thirusubramanian et al. [33], who used quantitative methods to identify key nodes that allowed the system to be operational and secure. Their object was to bring an improvement in IoT security by identifying critical nodes, assessing the vulnerabilities that would allow their compromise, proposing security measures and assessing their impact on system performance. The quantitative analysis was done to find essential components of IoT followed by a full-fledged vulnerability assessment. Security measures, including intrusion detection systems, encryption techniques and access control measures along with the conducting of frequent security audits, were proposed and evaluated in terms of their effectiveness. However, implementations were severely restricted due to very high costs, scalability issues and a changing landscape of cyber threats that jeopardized the actual system security.

Yallamelli et al. [34] designed a cloudlet computing and Edge-AI-based hybrid IoT platform for intelligent healthcare data processing. The goals for this study included security of data sharing, reduced latency and enhanced decision making. Advanced AI models including Random Forest classifiers, Transformer Networks and Temporal Convolutional Networks were used in this framework. It included cloud computing, cloudlet and edge layers for distributed processing on the system. Real-time stream analytics processing was provided through Apache Flink, while blockchain was used for secure data exchange. However, the study also identified high computational costs, integration complexity and bottlenecks for large-scale processing of data as the limitations.

Devarajan et al. [35] has developed the invention of an IoMT and blockchain-based heart disease monitoring system for enhancing heart health assessment. The research considered limitations of some existing studies in including arrhythmia implications together with ECG and PCG data for better disease prediction. The classification was done using BS-THA and OA-CNN models, blockchain was integrated for secure data storage and MAC was used for authentication. The feature extraction methods included spectrum analysis, signal decomposition, scalogram conversion and DPCA-based selection for improving classification accuracy. However, the limitation involved computational complexity and integration issues, in addition to the probable latency in real-life implementations.

Devarajan et al. [36] dealt with federated learning and cloud-edge collaborative computing systems to tackle security problems in collaborative computing. The research created a framework for multi-national validation for evaluation of the performance of the system under attack and no attack scenarios. Implementation of the End-to-End Privacy-Preserving Deep Learning model was carried out on classifying attacks while protecting the data privacy. The effectiveness of the model was evaluated using estimates Time, Node Count, Routing Count and Data Delivery Ratio. However, some are high computational overhead, scalability issues and vulnerabilities due to evolving cyber threats.

Devarajan et al. [37] suggested a holistic security management system to tackle security issues pertaining to cloud computing for healthcare. The study addressed security threats through risk assessment, security implementation, continuous monitoring and compliance management. Security measures such as authentication, encryption and intrusion detection systems were put in place with blockchain and multi-factor authentication to augment data security. Case studies at the Mayo Clinic and Cleveland Clinic proved the efficacy of cloud security solutions for healthcare. Conversely, the high cost of implementation, complexity of integration and problems associated with maintaining regulatory compliance are some of the limitations.

Yallamelli et al. [38] presented the security issues the software vendors face while handling a large volume of data in cloud environments. The research employed the Analytic Hierarchy Process for systematically identifying, ranking and evaluating a category of security concerns which were about data integrity, unauthorized access and privacy of data. The results indicated that advanced encryption, AI-enabled threat detection and multi-factor authentication are the most powerful security techniques. It also provided structured recommendations to upgrade the cloud data security via real-time threat detection systems. Nonetheless, the limitations included integration complexities, computational overheads and evolving nature of cyber threats.

Problem Statement

Healthcare fraud, such as false claims and billing frauds, is very responsible for incurring huge financial losses to the system and for damaging its integrity. Earlier, different detection methods are incompetent for this scale and complexity of data in health care. The system comprises very vast transactions which manual or rule-based systems cannot process or analyze efficiently [39]. Fraudulent actions are so sophisticated that they require much advanced adaptive models, which would help detect subtle patterns within the data [40]. This paper examines detecting anomalies in healthcare payment data through Sparse Autoencoders for better accuracy and reduced false positives. The focused goal is improving fraud detection efficiency and secure healthcare payment systems.

III. Proposed Methodologies

The propose fraud detection system begins with the collection of data from the cloud storage contains healthcare-related information such as payments done and medical records safely stored. Collected data is subjected to preprocessing of handling and normalizing by Z-score so that it can standardize data before subsequently applying Principal Component Analysis (PCA) for feature extraction, whereby the dimensionality of data is reduced and its most relevant features for fraud detection are focused on. The main part of the fraud detection process takes place in Sparse Autoencoders when it learns the normal pattern of transactions and the deviation from this norm is indicated as fraud. The performance metrics like accuracy and precision will then be evaluated to ascertain the functionality of the model in this system. This process thus ensures a model which can unimpeachably detect fraud in healthcare payment. Fraud detection is clearly depicted in Figure 1.

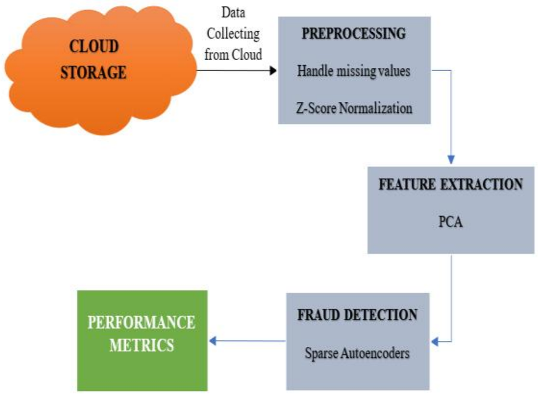

Fig 1: The Proposed Fraud Detection System in Healthcare Payments

Data Collection

Usually, the first step in fraud detection is to extract data from cloud databases, in which transactional and medical data specific to health care is deposited securely. This data can include insurance claims, demographic patient data, billing records, medical transactions and payment transactions, after which it can be pulled from a centralized cloud store incorporating various types of data collection such as electronic health records (EHR), insurance claim systems and transaction logs. Comprehensive fraud detection across the health payment landscape is then triggered by operations on data so collected. Data security, accessibility and regulatory compliance are also bolstered by cloud storage, plus the capacity to store large data needed for fraud detection.

Data Preprocessing

The most important step in data preparation for fraudulent activity detection is pre-processing, as it guarantees all data are cleansed, standardized and fit for analysis. First, missing values are handled, either through imputation or elimination of the rows/columns that contain too many missing values. Z-score normalization then standardizes the numerical features to evaluate them on a similar scale to prevent any feature from overpowering the outcome of the model. All the features are then equated as one when it comes to algorithms sensitive to feature scaling. In combination, these methods cover all the bases in preprocessing and make sure the data undergoes efficient analysis when it comes to precise fraud detection.

Feature Extraction

Feature extraction is the next step after the preprocessing, where missing values are treated and numerical features are normalized using Z-score. This step aims to minimize the dataset's dimensionality while keeping the most important information. PCA is employed, as it converts the original features into a smaller set of new features called principal components, which bear the utmost variance of the data. By doing so, PCA keeps only those components most significant to the reduction of data overload, thus facilitating machine learning algorithms. Such a procedure helps to filter out noise, mitigate overfitting and increase the accuracy of fraud detection in healthcare payments.

The first stage is to standardize the data, which is represented by equation (1), Given a dataset X with n samples and p characteristics,

$$Z = \frac{X-\mu}{\sigma} \tag{1}$$

Where, X represents the original data matrix, μ represents each feature's mean, σ indicates each feature's standard deviation and Z indicates the standardized data matrix.

Calculate the covariance matrix of the standardized data to understand how the features relate to each other and it's represented as equation (2),

$$C = \frac{1}{n-1} Z^T Z \tag{2}$$

In this case, C is the covariance matrix, while Z^T is the standardized data matrix transposed.

Find the eigenvalues and eigenvectors of the covariance matrix.

$$Cv = \lambda v \tag{3}$$

Where v is the corresponding eigenvector and λ is an eigenvalue. The magnitude of that variance is represented by eigenvalues, whereas the directions of highest variance are represented by eigenvectors.

Form the Principal Components: The largest eigenvalues correspond to the top k eigenvectors. The primary components that encapsulate the most significant aspects of the data are these eigenvectors and it's represented as equation (4),

$$X_{pca} = Z \cdot V_k \tag{4}$$

The matrix of the top k eigenvectors is denoted by V_k, the transformed dataset in terms of the principal components is denoted by X_{pca}.

To begin, standardize the data so that every feature can be compared. After that, compute the covariance matrix to determine how the features relate to one another. To identify the major components, find the covariance matrix's eigenvalues and eigen vectors. Lastly, to minimize dimensionality and preserve the most crucial aspects for analysis, project the data onto these primary components.

Fraud Detection

Anomaly detection methods are utilized in fraud detection with Sparse Autoencoders for detecting fraudulent transactions in health care payment data. The autoencoder model is trained on legitimate (non-fraudulent) transactions, giving it the power to reconstruct normal patterns scintillatingly. When a transaction is received by the model, it matches the transaction against the previously learned normal patterns and infers the reconstruction error. Big reconstruction error implies deviation from normal behavior and hence the transaction deserves to be scrutinized for the contamination of potential fraud. The model can thus flag observations of outliers and abnormal patterns, which are telltale indicators of possible fraudulent behavior while automatically concentrating on the most relevant features and thus curbing the false positives and false negatives. This leads to a highly accurate and reliable fraud detection system that focuses on identifying subtle patterns of fraud in healthcare payments.

An autoencoder is trained to reconstruct the input data x_i by encoding it into a lower-dimensional representation z_i and then decoding it back to $\hat{x}_i$ (the reconstruction) and it's expressed as equation (5),

$$\hat{x}_i = g(W_2 f(W_1 x_i + b_1) + b_2) \tag{5}$$

Where, W_1 and W_2 are weight matrices for the encoder and decoder, f and g are activation functions (like ReLU or sigmoid). The model learns to represent normal (non-fraudulent) transactions and reconstruct them with minimal error. Fraudulent transactions, being different from normal ones, will have a higher reconstruction error.

The model is trained by minimizing the reconstruction error, measured as the squared difference between the original input and the reconstruction is represented as equation (6),

$$\mathcal{L} = \|x_i - \hat{x}_i\|^2 \tag{6}$$

A higher reconstruction error indicates that the transaction doesn't match the learned patterns and is flagged as anomalous.

To encourage sparsity and focus on the most important features, a regularization term is added to the loss function, penalizing large activations in the hidden layer is expressed as equation (7),

$$\mathcal{L}_{\text{total}} = \mathcal{L} + \lambda \sum_j \|z_j\|_1 \tag{7}$$

Where, $\|z_j\|_1$ is the L1 norm for sparsity, λ is the regularization parameter. Ensures the model focuses only on the most relevant features by enforcing sparsity, helping to improve the accuracy of fraud detection.

After training, each transaction is passed through the model and if the reconstruction error exceeds a predefined threshold, it is flagged as potentially fraudulent and its expressed as equation (8),

$$\text{Fraud Score} = \|x_i - \hat{x}_i\|^2 \tag{8}$$

If Fraud Score $> \epsilon$, the transaction is classified as fraudulent. After training, any new transaction with a reconstruction error greater than a certain threshold is flagged as potentially fraudulent, as it doesn't conform to the learned patterns of legitimate transactions.

IV. Results

The results section presents the performance calculation of the fraud detection model based on various metrics and visualizations. The analysis includes cloud performance metrics, the confusion matrix and key model performance metrics. These outcomes demonstrate the model's effectiveness in accurately detecting fraudulent transactions and its efficiency in a cloud-based environment.

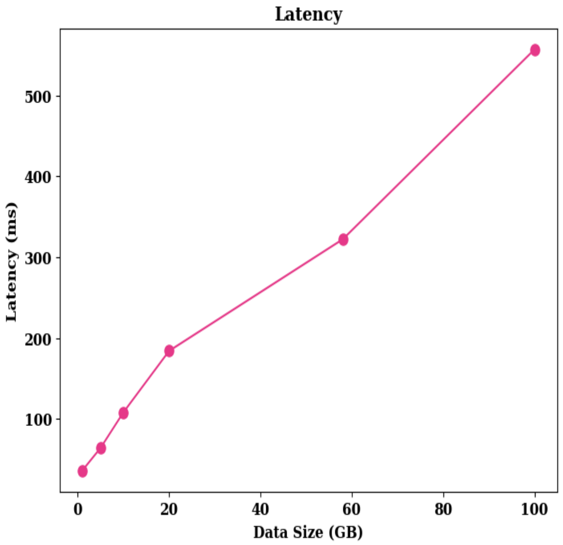

Fig 2: Latency

Figure 2 represents the relational properties between data size (GB) and latency (in milliseconds) regarding the fraud detection system. The figure shows that as data size increases, latency increases. For small data sizes (from 0 to 20 GB), latency is relatively low, at about 100 ms. However, once data size reaches 100 GB, latency spikes to above 500 ms as seen on the graph. This phenomenon suggests that the time taken to process information by the system is based on the amount of data and would require more tuning for superior performance in managing heavier loads of data. Hence, this graph complements the need for data storage against speed processing for ultimate optimization in performance for cloud-based fraud detection systems.

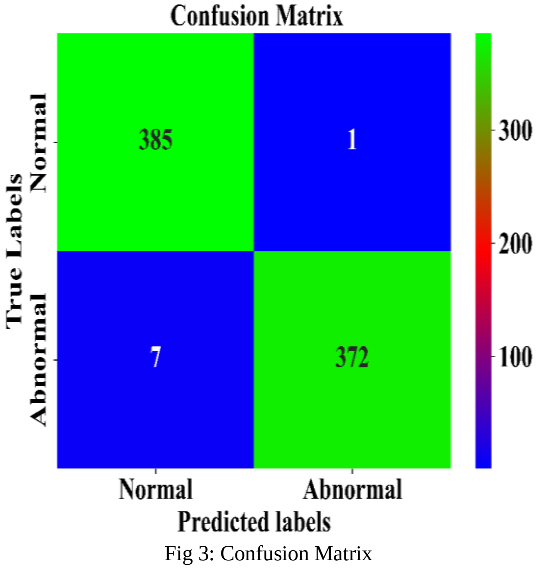

Fig 3: Confusion Matrix

The confusion matrix shown in Figure 3 gives an illustration of the fraud detection model for classifying healthcare payment transactions into normal or abnormal transactions. The model identifies 385 normal transactions as normal and 372 abnormal transactions as being genuinely so, represented by the green cells. Out of these, 1 normal transaction misclassified itself as abnormal and 7 abnormal transactions misclassified themselves as normal. Thus, these are false-positive and false-negative categorised misclassifications. Overall, the results reflect that the model is able to differentiate normal from abnormal transactions with a high degree of accuracy in prediction.

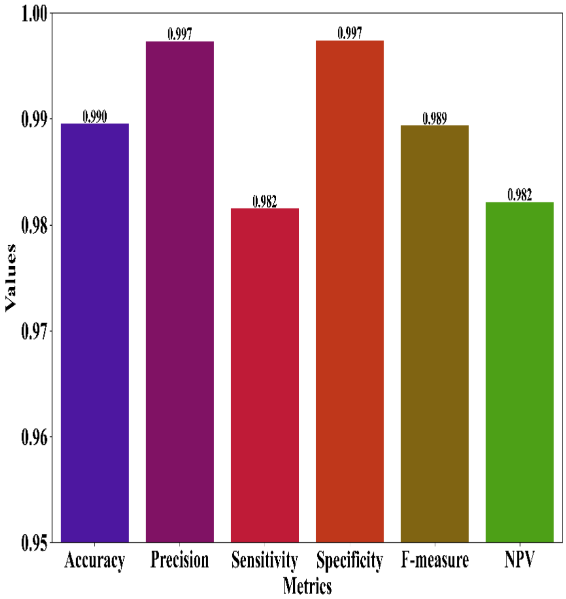

Fig 4: Performance Metrics

All the performance parameters of the fraud detection model are given in Figure 4. The model has an accuracy of 0.990, that is, 99% transactions are found to be correctly classified. Both Precision and Specificity are at 0.997, thus, the model can identify fraudulent transactions with minimum false positive cases. The Sensitivity value is 0.982, which stands for the model's ability to classify as abnormal (fraudulent) accordingly. F-measure, which combines the two parameters of the measures at hand, was found to be equal to 0.989, making the model highly robust in detecting fraudulent transactions. Finally, the Negative Predictive Value (NPV) stands at 0.982, which indicates the percentage of non-fraudulent transactions correctly classified by the model and is proof of the model's overall good performance in fraud detection.

V. Conclusion and Future Enhancements

This paper proposed a cloud-based fraud detection system for healthcare payments implemented using Sparse Autoencoders for fraud detection. This system was conceived to address the challenges posed by an ever-increasing volume and complexity of information in healthcare. With cloud utilization as storage to ensure scalability and efficient resource utilization. The fraud detection consisted of data preprocessing, Z-score normalization application for normalization and feature extraction with PCA for dimensionality reduction. Sparse Autoencoders learned patterns for normal transactions and flagged deviations as possible fraud. The model was highly successful, achieving an accuracy of 0.990, precision of 0.997 and sensitivity of 0.982 with respect to the true classification of transactions as either legitimate or fraudulent. Latency analysis shows that as the data size increases from 1 GB to 100 GB, latency rises from 36 ms to 557 ms. The system may be highly promising for fraud detection. Future works will focus on making the system adaptable to new fraud patterns, improving resource utilization on larger datasets and exploring hybrid models to improve further the accuracy and efficiency of fraud detection.

References

[1] T. Ganesan, "Integrating Artificial Intelligence And Cloud Computing For The Development Of A Smart Education Management Platform: Design, Implementation, And Performance Analysis," *Int. J. Eng.*, vol. 11, no. 2.

[2] P. Alagarsundaram, "Adaptive CNN-LSTM and Neuro-Fuzzy Integration for Edge AI and IoMT-Enabled Chronic Kidney Disease Prediction," vol. 18, no. 3, 2024.

[3] P. Alagarsundaram and N. Carolina, "Physiological Signals: A Blockchain-Based Data Sharing Model For Enhanced Big Data Medical Research Integrating Rfid And Blockchain Technologies," vol. 09, no. 9726, 2024.

[4] 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.

[5] A. R. G. Yallamelli, V. Mamidala, M. V. Devarajan, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "Dynamic mathematical hybridized modeling algorithm for e-commerce for order patching issue in the warehouse," *Serv. Oriented Comput. Appl.*, Nov. 2024, doi: 10.1007/s11761-024-00431-w.

[6] A. R. G. Yallamelli, "Wipro Ltd, Hyderabad, Telangana, India," vol. 7, no. 9726, 2019.

[7] M. V. Devarajan, A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem," *Serv. Oriented Comput. Appl.*, Nov. 2024, doi: 10.1007/s11761-024-00438-3.

[8] 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, 2021.

[9] S. H. Grandhi, B. R. Gudivaka, R. L. Gudivaka, R. K. Gudivaka, D. K. R. Basani, and M. M. Kamruzzaman, "Detection and Diagnosis of ECH Signal Wearable System for Sportsperson using Improved Monkey-based Search Support Vector Machine," *Int. J. High Speed Electron. Syst.*, p. 2540149, Jan. 2025, doi: 10.1142/S0129156425401494.

[10] T. Ganesan, R. R. Al-Fatlawy, S. Srinath, S. Aluvala, and R. L. Kumar, "Dynamic Resource Allocation-Enabled Distributed Learning as a Service for Vehicular Networks," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594602.

[11] S. Nelson, A. Raj Gaius Yallamelli, A. Alkhayyat, N. Naga Saranya, and S. M, "Hybrid Autoregressive Integrated Moving Average and Bi-directional Gated Recurrent Unit for Time Series Forecasting," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, Jul. 2024, pp. 1–4. doi: 10.1109/ICDSNS62112.2024.10690898.

[12] M. V. Devarajan and C. Solutions, "An Improved Bp Neural Network Algorithm For Forecasting Workload In Intelligent Cloud Computing," vol. 10, no. 9726, 2022.

[13] T. Ganesan, M. Almusawi, K. Sudhakar, B. R. Sathishkumar, and K. S. Kumar, "Resource Allocation and Task Scheduling in Cloud Computing Using Improved Bat and Modified Social Group Optimization," in *2024 Second International Conference on Networks,*

Multimedia and Information Technology (NMITCON), Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699250.

[14] M. V. Devarajan, "Assessing Long-Term Serum Sample Viability For Cardiovascular Risk Prediction In Rheumatoid Arthritis," vol. 8, no. 2, 2020.

[15] B. R. Gudivaka, A. Izang, I. O. Muraina, and R. L. Gudivaka, "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.*, vol. 1, no. 01, Art. no. 01, Dec. 2024.

[16] R. K. Gudivaka, R. L. Gudivaka, B. R. Gudivaka, D. K. R. Basani, S. H. Grandhi, and F. khan, "Diabetic foot ulcer classification assessment employing an improved machine learning algorithm," *Technol. Health Care*, p. 09287329241296417, Jan. 2025, doi: 10.1177/09287329241296417.

[17] M. V. Devarajan, "Enhancing Trust And Efficacy In Healthcare Ai: A Systematic Review Of Model Performance And Interpretability With Human-Computer Interaction And Explainable AI," *Int. J. Eng. Res. Sci. Technol.*, vol. 19, no. 4, pp. 9–31, 2023.

[18] R. K. M. K. Yalla, A. R. G. Yallamelli, and V. Mamidala, "A Distributed Computing Approach to IoT Data Processing: Edge, Fog, and Cloud Analytics Framework," *Int. J. Inf. Technol. Comput. Eng.*, vol. 10, no. 1, pp. 79–94, Jan. 2022.

[19] H. Nagarajan, Z. Alsalami, S. Dhareshwar, K. Sandhya, and P. Palanisamy, "Predicting Academic Performance of Students Using Modified Decision Tree based Genetic Algorithm | IEEE Conference Publication | IEEE Xplore." Accessed: Feb. 28, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10594426

[20] M. V. Devarajan, "Data-Driven Techniques For Real-Time Safety Management In Tunnel Engineering Using Tbm Data," vol. 7, no. 3.

[21] G. C. Markose, S. R. Sitaraman, S. V. Kumar, V. Patel, R. J. Mohammed, and C. Vaghela, "Utilizing Machine Learning for Lung Disease Diagnosis | IEEE Conference Publication | IEEE Xplore." Accessed: Mar. 01, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/10797552

[22] D. R. Natarajan, "A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection," *Int. J. Eng. Res. Sci. Technol.*, vol. 14, no. 4, pp. 198–213, Dec. 2018.

[23] M. V. Devarajan, M. Al-Farouni, R. Srikanteswara, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594070.

[24] A. R. G. Yallamelli, "Cloud Computing And Management Accounting In Smes: Insights From Content Analysis, Pls- Sem, And Classification And Regression Trees," *Int. J. Eng.*, vol. 11, no. 3.

[25] S. Peddi, S. Narla, and D. T. Valivarthi, "Advancing Geriatric Care: Machine Learning Algorithms and AI Applications for Predicting Dysphagia, Delirium, and Fall Risks in Elderly Patients," *Int. J. Inf. Technol. Comput. Eng.*, vol. 6, no. 4, pp. 62–76, Nov. 2018.

[26] A. R. G. Yallamelli, "Improving Cloud Computing Data Security with the RSA Algorithm," vol. 9, no. 2, 2021.

[27] 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.

[28] S. S. Kethu, K. Corp, and S. Diego, "AI and IoT-Driven CRM with Cloud Computing: Intelligent Frameworks and Empirical Models for Banking Industry Applications," vol. 8, no. 1, 2020.

[29] A. R. G. Yallamelli, "A Cloud-based Financial Data Modeling System Using GBDT, ALBERT, and Firefly Algorithm Optimization for High-dimensional Generative Topographic Mapping," vol. 8, no. 4, 2020.

[30] "Comprehensive Approach for Mobile Data Security in Cloud Computing Using RSA Algorithm.pdf." Accessed: Mar. 06, 2025. [Online]. Available: https://jcsonline.in/admin/uploads/Comprehensive%20Approach%20for%20Mobile%20Data%20Security%20in%20Cloud%20Computing%20Using%20RSA%20Algorithm.pdf

[31] G. Thirusubramanian, "Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments," *Int. J. HRM Organ. Behav.*, vol. 8, no. 4, pp. 1–16, Oct. 2020.

[32] Thirusubramanian Ganesan, "Dynamic Secure Data Management with Attribute-Based Encryption for Mobile Financial Clouds," Oct. 2024, doi: 10.5281/ZENODO.13994646.

[33] T. Ganesan, "Securing Iot Business Models: Quantitative Identification Of Key Nodes In Elderly Healthcare Applications," vol. 12, no. 3.

[34] A. R. G. Yallamelli and M. V. Devarajan, "Hybrid Edge-Ai And Cloudlet-Driven Iot Framework For Real-Time Healthcare," vol. 7, no. 1, 2023.

[35] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. K. Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "An Enhanced IOMT and Blockchain-Based Heart Disease Monitoring System Using BS-THA and OA-CNN," *Trans. Emerg. Telecommun. Technol.*, vol. 36, no. 2, p. e70055, 2025, doi: 10.1002/ett.70055.

[36] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. Kanta Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "Attacks classification and data privacy protection in cloud-edge collaborative computing systems," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 0, no. 0, pp. 1–20, doi: 10.1080/17445760.2024.2417875.

[37] M. V. Devarajan, "Improving Security Control in Cloud Computing for Healthcare Environments," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[38] A. R. G. Yallamelli, "Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis," *Curr. Sci.*, 2021.

[39] M. V. Devarajan, "A Comprehensive AI-Based Detection and Differentiation Model for Neurological Disorders Using PSP Net and Fuzzy Logic-Enhanced Hilbert-Huang Transform," *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 3, pp. 94–104, Jul. 2019.

[40] M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Bengaluru, India: IEEE, Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.