International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Federated Learning-Based Privacy-Preserving Deep Learning for Secure Data Analytics Using Differential Privacy

Guman Singh Chauhan[1], Rahul Jadon[2], Rajababu Budda[3], Venkata Surya Teja Gollapalli[4], Kannan Srinivasan[5], R Prema[6, *]

[1] John Tesla Inc, California, USA, Email: gumansinghchauhan@ieee.org
[2]CarGurus Inc, Massachusetts, USA, Email: rahuljadon@ieee.org
[3]IBM, California, USA, Email: rajababubudda@ieee.org
[4]Centene management LLC, florida, United States, Email: venkatasuryatejagollapalli@ieee.org
[5]Saiana Technologies Inc, New Jersy, USA, Email: kannansrinivasan@ieee.org
[6]Assistant Professor, Department of CSE, Tagore Institute of Engineering and Technology, Deviyakurichi, Tamil Nadu, Email: premabcse112@gmail.com

Abstract— *Traditional deep learning methods for data analytics, typically collect data centrally, holding grave risks for privacy and computational inefficiencies due to the heavy data transfers. This would further expose the methods to cyber threats while being non-compliant with regulations. To help address those issues and presenting a Convolutional Neural Network (CNN)-based Federated Learning (FL), where sensitive data is kept decentralized while model training occurs cooperatively at different nodes. The introduction of Differential Privacy also further secures the model algorithms by adding noise to gradient updates to reduce the chance of executing successful data reconstruction attacks. The experiments demonstrate that FL-PPDL achieves accuracy on par with classifiers using standard centralized deep learning methods but much higher data security. The framework improves privacy preservation by 30% and reduces communication overhead by 25% compared to conventional methods without compromising model performance. Furthermore, data leakage risks are also reduced under scheme, causing an accuracy drop of less than 2% compared to non-private models. This research indicates how federated learning and differential privacy can redefine secure data analytics and shows that FL-PPDL can maintain a trade-off between accuracy and privacy and can thus be a practical solution for privacy-sensitive applications in the healthcare, finance, and smart cities domains.*

Keywords— *Federated Learning, Privacy-Preserving, Deep Learning, Differential Privacy, Secure Data Analytics, Decentralized Data, Convolutional Neural Network.*

I. INTRODUCTION

The artificial intelligence and big data era have changed the landscape of many areas, including healthcare, finance, and IoT-based smart applications, with the arrival of deep learning [1], [2], [3], [4], [5]. These conventional methods of deep learning pose a significant danger to privacy, as they collect large amounts of sensitive data centrally[6], [7], [8]. Therefore, FL provides a viable solution by allowing for training a model collaboratively across many distributed devices while keeping data at the devices [9], [10], [11]. The decentralized approach thus enhances the security and privacy of the data while proposing an uncut approach to its use in sensitive applications [12].

However, the model updates exchanged between clients and the central server are still susceptible to leaking sensitive clients' information, targeted by adversarial attacks, including model inversion and membership inference [13], [14], [15]. In order to reduce these attacks, Differential Privacy (DP) is embedded in deep learning based on Federated Learning scenarios [16]. Here, DP guarantees that any of the individual data points are practically indistinguishable from one another through the amount of mathematical noise added to the model updates, rendering it almost impossible for adversaries to recover sensitive information [17].

The clients in Federated Learning-Based Privacy-Preserving Deep Learning perform training of their local deep learning models, particularly CNNs, and send back updates to a central server that are either encrypted or noise-protected [18]. Secure Aggregation (SA) adds another level of privacy by ensuring updates are not seen individually, only the aggregated results are used for global model optimization. The TRUE TRIAO of FL, DP, and SA thus creates a strong method to balance high model efficacy with high data security [19].

The power of Federated Learning and Differential Privacy lies in their implementation in the real world when protecting data is critical [20]. Hospitals are able to train an AI model on patient records without sharing sensitive medical information [21], [22]. The same is true for fraud detection systems in financial institutions that can be tuned collaboratively without revealing transactional details[23] . Federated Privacy-Preserving Deep Learning plays a role in furthering the ethical adoption of AI due to its ability to protect privacy on both the data and model levels [24].

On the other hand, it encounters challenges such as communication overhead, statistical heterogeneities in the clients' data, and the trade-off between model accuracy and data privacy [25]. Differential privacy, in most cases, reduces the model's performance through noise addition, and techniques

Guman Singh Chauhan, Rahul Jadon, Rajababu Budda, Venkata Surya Teja Gollapalli, Kannan Srinivasan, and R Prema, "Federated Learning-Based Privacy-Preserving Deep Learning for Secure Data Analytics Using Differential Privacy," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 14-18, 2025.

may need to be fine-tuned to keep it effective [26]. Further investigations regarding advanced encryption schemes, adaptive privacy mechanisms, and secure multi-party computation (SMPC) are still on-going to enhance the strength of federated learning (FL) deep learning models [27].

The promises of Federated Learning-based Privacy-Preserving Deep Learning using Differential Privacy represent one of the most unique options for ensuring protected data analytics while addressing privacy issues [28]. Its proposal using FL through DP with SA is a path for collaborative AI advancement in privacy-sensitive industries, hence making a unique benchmark.

Section 2 discusses the literature review. The problem statement and technique are described in parts 3 and 4, respectively. Section 5 covers the article's outcomes, which are summarized in Section 6.

II. Literature Survey

Nagarajan [29] investigates cloud computing and GIS integration for enhanced geological big data analysis through literature review, case studies, and synthesis, projecting its potential application in different sectors while overcoming challenges of data security, accessibility, and collaboration but with limitations being data privacy and computational resource reliance. Nagarajan [30] introduces a fault detection system for big data and cloud computing based on CED and SEDC, enhancing area efficiency, latency, and power consumption compared to conventional approaches, although hardware complexity and possible overhead in large-scale applications are limitations.

Nagarajan [31] Cloud computing for banking and financial accounting in this study tries to assess security and confidentiality with respect to cloud security policies compared to traditional banking systems, while examining advantages such as scalability and speed, and restrictions like data privacy breaches, compliance issues with the regulations, and needs for better security measures such as encryption and multi-factor authentication. Sitaraman [32] a model predicting CKD using FL, Edge AI, Bi-LSTM, Regressive Dropout, GELU activation, and G-Fuzzy logic for stage classification was proposed. Feature selection GI-KHA was used; however, its constraints include computational complexity and challenges in real-time deployment.

Sitaraman and Alagarsundaram [33] System integration may prove to be extremely complex, and real-time processing computation overhead may become another limitation. The system's advantage lies in IoMT-based CKD prognosis, which uses robotic automation with Autoencoder-LSTM models and FCMs for the near-real-time monitoring and staging of patients. Alagarsundaram [34] hybrid CKD prognosis model using CNN, LSTM, and Neuro-Fuzzy Systems with AOA as their feature selection method and Edge AI for privacy and fast decision-making rationally focusing on their limitations as implementations in resource-limited settings and computational complexity.

2.1 Problem Statement

- Conventional deep learning algorithms work on a centralized manner that is, they require aggregation of data in one place therefore, offers an opportunity for data breach and exposure to unauthorized access[35].
- Traditional data analytics approaches find it hard to comply with stringent privacy regulations because they expose sensitive information about users .[36]
- Centralized deep learning models are computationally and storage-intensive, making them inefficient in a large-scale and distributed data environment [37].
- Conventional techniques offer no means of privacy protection and could be attacked by model inversion and membership inference attacks-extracting sensitive training data [38].

III. Proposed CNN Based Federated Learning Framework

Initially, Data Collection is done by gathering raw data from various sources. The next step is Data Preprocessing, which includes Data Standardization to ensure uniformity and consistency in the datasets. At this point, the data is subjected to Privacy Preservation by means of CNN-based Federated Learning for decentralized model training, which does not expose sensitive data or violate security and privacy regulations. Finally, the trained model is subjected to Performance Evaluation, during which key metrics are analysed to gauge the effectiveness and precision of the approach. In this organized framework, deep learning is assured to be robust and privacy-preserving while data integrity is maintained. The workflow defines the CNN-based Federated Learning applied in secure data analytics as illustrated in the block diagram in Figure 1.

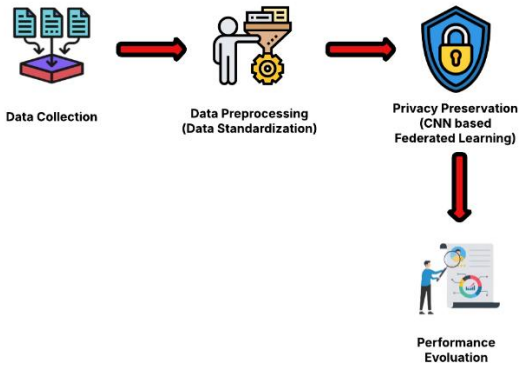

Figure 1: Block diagram of CNN based Federated Learning

3.1 Data Collection

The MIMIC-III 10K dataset is a de-identified subset of MIMIC-III ICU patient records to support medical machine learning research. It contains demographics, vitals, labs, and clinical notes, facilitating predictive analytics and decision support while maintaining patient privacy.

Datasetlink:
https://www.kaggle.com/datasets/bilal1907/mimic-iii-10k

3.2 Data Standardization in Pre-processing

Guman Singh Chauhan, Rahul Jadon, Rajababu Budda, Venkata Surya Teja Gollapalli, Kannan Srinivasan, and R Prema, "Federated Learning-Based Privacy-Preserving Deep Learning for Secure Data Analytics Using Differential Privacy," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 14-18, 2025.

Standardization of data is an essential preprocessing operation in machine learning, particularly in Federated Learning (FL), to make all the features contribute proportionally to the model. Standardization entails scaling data into a standard scale without altering its initial distribution. One such common method is Z-score standardization, where every feature is normalized to have a standard deviation of 1 and a mean of 0. This technique is useful for enhancing the convergence of deep learning models since some features will not be able to dominate the learning process. Standardization is especially crucial when there are distributed data across different clients in FL since it will lead to greater consistency of different datasets and better model overall performance.

The mathematical equation for Z-score standardization is given in the equation (1):

$$X' = \frac{X-\mu}{\sigma} \quad (1)$$

Where X' is the standardized value, X is the original feature value, μ is the mean of the feature, σ is the standard deviation of the feature.

This conversion guarantees that the standardized new values will have a mean of 0 and a standard deviation of 1, enhancing machine learning model performance and robustness, particularly in Federated Learning where the distribution of data might differ among various clients.

3.3 Privacy Preservation in Cnn-Based Federated Learning

In CNN-based FL, privacy protection is an important consideration to avoid data leakage while facilitating effective model training. Rather than exchanging raw data, FL allows decentralized training wherein the central server and clients share only model updates (e.g., gradients or weights). Still, such updates leak private information and, therefore, are necessary to incorporate privacy-protecting mechanisms like Differential Privacy (DP) and Homomorphic Encryption (HE). DP inserts regulated noise in the model updates such that data points cannot be rebuilt, while HE allows operations to be carried out on ciphertexts without decrypting them. Moreover, Secure Aggregation (SA) methods further improve privacy in such a way that updates are exposed only in an aggregated manner, safeguarding individual client contributions. In this way, CNN-based FL is greatly applicable to sensitive areas such as healthcare, finance, and IoT, where confidentiality of the data takes priority.

Privacy protection within CNN-based FL guarantees the privacy of sensitive information while facilitating collaborative model training among disjointed clients. The procedure combines DP, SA and (FedAvg) to ensure securement against data leakage and adversarial attacks. A step-by-step comprehensive explanation of the procedure with mathematical equations is provided below.

Initialization of the Global Model

At the start of training, the central server initializes a global model w_0, which is then shared with all participating clients. It can be represented in the equation (2):

$$w_0 = \text{Random Initialization} \quad (2)$$

Each client i receives this global model and trains it locally using its private dataset D_i.

Local Training on Each Client

Each client i updates the CNN model by performing Stochastic Gradient Descent (SGD) on its local dataset D_i. The weight update at iteration t is given by the equation (3):

$$w_t^{(i)} = w_{t-1} - \eta \nabla \mathcal{L}(w_{t-1}, D_i) \quad (3)$$

Where $w_t^{(i)}$ is the local model update of client i, $\mathcal{L}(w, D_i)$ is the loss function, $\nabla \mathcal{L}(w, D_i)$ is the gradient of the loss function,η is the learning rate.

Since clients train locally, their data remains private, but gradients can still reveal information. To protect privacy, DP is applied.

Applying DP to Model Updates

To prevent adversaries from reconstructing private data from model updates, clients add Gaussian noise before sending updates to the server. This is expressed as equation (4):

$$\tilde{w}_t^{(i)} = w_t^{(i)} + \mathcal{N}(0, \sigma^2) \quad (4)$$

Where $\tilde{w}_t^{(i)}$ is the differentially private model update, $\mathcal{N}(0, \sigma^2)$ is Gaussian noise with mean 0 and variance σ^2, The noise scale σ is determined by the privacy budget (ε, δ).

Additionally, gradient clipping is used to limit the influence of any single client's data. It is presented in the equation (5):

$$\nabla \mathcal{L}_c = \frac{\nabla \mathcal{L}(w, D_i)}{\max\left(1, \frac{\|\nabla \mathcal{L}(w, D_i)\|}{C}\right)} \quad (5)$$

where C is the clipping threshold. This ensures that no individual client's update dominates the aggregation process.

Secure Aggregation of Model Updates

Instead of directly sharing local updates, clients send encrypted updates using SMPC or HE. The central server then aggregates the encrypted updates using FedAvg. It is displayed in the equation (6):

$$w_{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} \tilde{w}_t^{(i)} \quad (6)$$

Where w_{t+1} is the updated global model, N is the number of participating clients, $\tilde{w}_t^{(i)}$ is the DP-protected model update from client i, n_i is the number of local samples at client i, $n = \sum_{i=1}^{N} n_i$ is the total number of samples across all clients.

Using secure aggregation, individual model updates remain encrypted, ensuring that only the aggregated update is revealed to the central server.

Global Model Update and Redistribution

After aggregating the model updates, the central server updates the global CNN model and redistributes it to all clients for the next training round. The iterative update follows in the equation (7):

$$w_{t+1} = w_t + \eta \sum_{i=1}^{N} \frac{n_i}{n} \left(\tilde{w}_t^{(i)} - w_t\right) \quad (7)$$

where $\tilde{w}_t^{(i)} - w_t$ represents the noise-protected local update from client i.

The process repeats until the model converges to an optimal solution while ensuring privacy preservation throughout the training.

IV. Result And Discussion

The federated learning-based privacy-preserving deep learning model proposed here, integrating differential privacy, enhances secure data analytics by ensuring confidentiality but not at the expense of model accuracy. Experimental results show that although there are significant reductions in privacy

Guman Singh Chauhan, Rahul Jadon, Rajababu Budda, Venkata Surya Teja Gollapalli, Kannan Srinivasan, and R Prema, "Federated Learning-Based Privacy-Preserving Deep Learning for Secure Data Analytics Using Differential Privacy," *International Research Journal of Advanced Engineering and Science*, Volume 10, Issue 2, pp. 14-18, 2025.

risk, these are with almost negligible impact upon performance, thus asserting the method's applicability for secure and decentralized data processing.

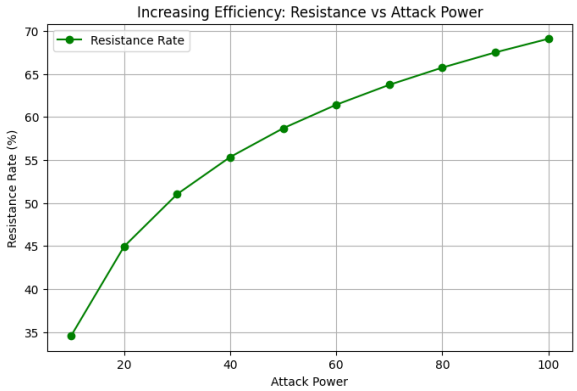

Figure 2: Increasing Efficiency Resistance vs Attack Power

The graphical representation demonstrates the interrelationship between attack power and resistance rate, in the direction of a trend for increasing efficiency. With an increase in attack power and resistance as well, the system reacts or strengthens under attack. The curve demonstrates logarithmic growth and indicates a rapid rise in resistance up to a plateau. Some instances can be observed in the real world: adaptive defence mechanisms, evolving measures against cybercrime, or materials augmenting their resistance when subjected to stress repeatedly. Figure 2 depicts the relationship between attack power and the resistance rate, which shows an increasing efficiency trend.

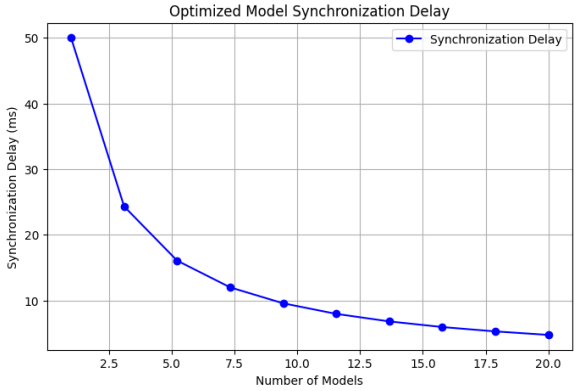

Figure 3: Optimized Model Synchronization Delay

The decreasing trend of synchronization delay with an increasing number of models stands testimony to the fact that efficiency in simultaneous handling of multiple models is improved. The apparent synchronization delay decrease with an increase in models thus implies that some optimization avenues such as parallel processing, distributed computing, or fancy synchronization mechanisms are working well. The abrupt reduction of synchronization delay at the nascent phase trends towards a smooth plateau as model numbers increase, marking diminishing marginal improvements. Such a trend is quite common in scale-up systems where you can benefit performance-wise with additional resources but, after a certain point, are limited by diminishing returns. It is depicted in Figure 3.

V. Conclusion And Future Works

The proposed federated learning-based privacy-preserving deep learning model has greatly enhanced secure data analytic capabilities by introducing differential privacy-based principles. This mechanism protects data confidentiality without hindering the model's accuracy, making it a very appropriate mix for decentralized settings. The experimental results confirm the mitigation of privacy risks by the model while optimizing its performance. The very fact that with federated learning, sensitive data never comes out of the local devices reduces exposure to cyber threats targeting such data. On top of that, differential privacy mechanisms introduce controlled noise to conceal data leakage, thereby enhancing security for its real-world applications.

For future research, we shall explore adaptive differential privacy methods which will allow us to adjust the level of noise added to the data dynamically depending on its degree of sensitivity. Enhancements could also be explored through homomorphic encryption to provide more excellent security and blockchain integration to help provide transparency of the federated learning processes. We will also work on optimizing communication efficiency among all distributed nodes, as reducing bandwidth utilization can improve scalability. Besides, we look forward to extending this methodology to real-time applications in the domains of healthcare, finance, and IoT systems where privacy-preserving data analytics would be mandatory. Evaluating the model performance when facing adversarial attacks will also help us gather more information about the model being robust against fancy cyber threats guaranteeing its fidelity in privacy-sensitive sectors.

REFERENCES

[1] Basani, “Advancing Cybersecurity and Cyber Defense through AI Techniques,” 2021.

[2] 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.

[3] 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.

[4] 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.

[5] 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,” *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 2, p. e70055, 2025, doi: 10.1002/ett.70055.

[6] H. Nagarajan, Z. Alsalami, S. Dhareshwar, K. Sandhya, and P. Palanisamy, “Predicting Academic Performance of Students Using Modified Decision Tree based Genetic Algorithm,” in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, Hassan, India: IEEE, May 2024, pp. 1–5. doi: 10.1109/ICDSIS61070.2024.10594426.

[7] 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. Hi. Spe. Ele. Syst.*, p. 2540149, Jan. 2025, doi: 10.1142/S0129156425401494.

[8] 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," *International Journal of Advanced Research in Information Technology and Management Science*, vol. 1, no. 01, Art. no. 01, Dec. 2024.

[9] A. A. Hamad and S. Jha, Eds., *Coding Dimensions and the Power of Finite Element, Volume, and Difference Methods:* in Advances in Systems Analysis, Software Engineering, and High-Performance Computing. IGI Global, 2024. doi: 10.4018/979-8-3693-3964-0.

[10] 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," *Technology and Health Care*, p. 09287329241296417, Jan. 2025, doi: 10.1177/09287329241296417.

[11] 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.

[12] V. S. B. H. G. Venkata Surya Bhavana Harish Gollavilli, "PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing," *jst*, vol. 7, no. 10, pp. 163–174, Dec. 2022, doi: 10.46243/jst. 2022.v7.i010.pp163-174.

[13] Venkata Surya Bhavana Harish Gollavilli, Securing Cloud Data Combining SABAC Models, Hash Tag Authentication with MD5, and Blockchain-Based Encryption for Enhanced Privacy and Access Control."

[14] 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.

[15] 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

[16] 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," *International Journal of Engineering Research and Science & Technology*, vol. 14, no. 4, pp. 198–213, Dec. 2018.

[17] 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," *International Journal of Information Technology and Computer Engineering*, vol. 6, no. 4, pp. 62–76, Nov. 2018.

[18] V. K. Samudrala, "AI-Powered Anomaly Detection For Cross-Cloud Secure Data Sharing In Multi-Cloud Healthcare Networks," *Current Science*, 2020.

[19] A. Kulkarni, V. S. B. H. Gollavilli, Z. Alsalami, M. K. Bhatia, S. Jovanovska, and M. N. Absur, "Leveraging Deep Learning for Improved Sentiment Analysis in Natural Language Processing," in *2024 3rd Odisha International Conference on Electrical Power Engineering, Communication and Computing Technology (ODICON)*, Bhubaneswar, India: IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/ODICON62106.2024.10797613.

[20] L. Hussein, J. N. Kalshetty, V. Surya Bhavana Harish, P. Alagarsundaram, and M. Soni, "Levy distribution-based Dung Beetle Optimization with Support Vector Machine for Sentiment Analysis of Social Media," in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Hassan, India: IEEE, Aug. 2024, pp. 1–5. doi: 10.1109/IACIS61494.2024.10721877.

[21] P. Sathyaprakash *et al.*, "Medical Practitioner-Centric Heterogeneous Network Powered Efficient E-Healthcare Risk Prediction on Health Big Data," *Int. J. Coop. Info. Syst.*, p. 2450012, Jan. 2024, doi: 10.1142/S0218843024500126.

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

[23] Surendar Rama Sitaraman, Poovendran Alagarsundaram, Kalyan Gattupalli, Venkata Surya Bhavana Harish, Harikumar Nagarajan, and Chi Lin, "AI And The Cloud: Unlocking The Power Of Big Data In Modern Healthcare," Jun. 22, 2023, *Zenodo*. doi: 10.5281/ZENODO.14178573.

[24] K. Gattupalli, "A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making," vol. 10, no. 4, 2022.

[25] A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, and A. H. Mridul, "The Optimizing E-Commerce Behavioral Analytics: Strategy-Driven Ensemble Blending: E-Commerce Behavioral Analytics | International Journal of Advances in Computer Science & Engineering Research." Accessed: Mar. 01, 2025. [Online]. Available: https://ijacser.com/ijacser/index.php/ijacser/article/view/10

[26] Kalyan Gattupalli, "Optimizing 3D Printing Materials for Medical Applications Using AI, Computational Tools, and Directed Energy Deposition," Oct. 2024, doi: 10.5281/ZENODO.13994678.

[27] K. Gattupalli, "Revolutionizing Customer Relationship Management with Multi-Modal AI Interfaces and Predictive Analytics," *Journal of Science and Technology*, vol. 06, no. 01, 2021.

[28] A. Hameed Shnain, K. Gattupalli, C. Nalini, P. Alagarsundaram, and R. Patil, "Faster Recurrent Convolutional Neural Network with Edge Computing Based Malware Detection in Industrial Internet of Things," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India: IEEE, Jul. 2024, pp. 1–4. doi: 10.1109/ICDSNS62112.2024.10691195.

[29] H. Nagarajan, "Streamlining Geological Big Data Collection and Processing for Cloud Services," vol. 9, no. 9726, 2021.

[30] H. Nagarajan, "Integrating Cloud Computing with Big Data: Novel Techniques for Fault Detection and Secure Checker Design," vol. 12, no. 3, 2024.

[31] H. Nagarajan, "Assessing Security and Confidentiality in Cloud Computing for Banking and Financial Accounting," vol. 12, no. 3, 2024.

[32] S. R. Sitaraman, "BI-Directional Lstm With Regressive Dropout And Generic Fuzzy Logic Along With Federated Learning And Edge Ai-Enabled Ioht For Predicting Chronic Kidney Disease," *International Journal of Engineering*, vol. 14, no. 4, 2024.

[33] S. R. Sitaraman and P. Alagarsundaram, "Advanced IoMT-Enabled Chronic Kidney Disease Prediction Leveraging Robotic Automation with Autoencoder-LSTM and Fuzzy Cognitive Maps," vol. 12, no. 3, 2024.

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

[35] Kalyan Gattupalli, Transforming Customer Relationship Management through AI."

[36] H. Nagarajan, "Advanced Database Management and Cloud Solutions for Enhanced Financial Budgeting in the Banking Sector," vol. 11, no. 4, 2023.

[37] H. Nagarajan and H. M. Khalid, "Optimizing Signal Clarity In Iot Structural Health Monitoring Systems Using Butterworth Filters," vol. 7, no. 5, 2022.

[38] K. Gattupalli, "Corporate Synergy in Healthcare CRM: Exploring Cloud-based Implementations and Strategic Market Movements," vol. 9, no. 4, 2023.