Rover Publications
United International Journal of Engineering and Sciences (UIJES)
An International Peer-Reviewed (Refereed)Engineering and Science Journal
Impact Factor:8.075(SJIF) Vol-5, Issue- 4,(December);2025 ISSN:2582-5887 www.uijes.com

Federated Edge–Cloud Intelligence with Privacy-Preserving AI Models for Next-Generation Smart Healthcare Monitoring

Pawan Kalyan Jonnalagadda
San Jose, California, USA, 95110
pawankalyanjonnalagadda2@gmail.com

Abstract
The fast evolution of intelligent healthcare systems has resulted in the creation of huge amounts of sensitive medical information, which is of great concern in terms of privacy, security, and effective data processing. The conventional centralized machine learning techniques are not sufficient because they require data sharing and high latency. To overcome these difficulties, the paper suggests an approach of Federated Edge-Cloud Privacy-Preserving AI (FECP-AI) framework to next-generation smart healthcare monitoring. The system proposed combines federated learning and edge-cloud intelligence to allow the decentralized model training and preserve data privacy. More sophisticated technology like homomorphic encryption and differential privacy is integrated to ensure model updates and avoid leakage of information. The framework is tested with simulated data sets on various performance measures, such as accuracy, privacy preservation, communication overhead, latency, and energy usage. Experimental evidence shows that the suggested model is more efficient, secure and scalable as compared to the current methods like FedAvg, PPFLHE and Fedshe. The suggested FECP-AI framework presents an efficient and adaptable solution to real-time healthcare monitoring, as well as the strict observance of the data privacy requirements.

Keywords: Federated Learning; Edge–Cloud Computing; Privacy-Preserving AI; Smart Healthcare Monitoring; Homomorphic Encryption

1.Introduction

The swift development of intelligent healthcare has brought about a tremendous change in the manner data of any medical nature is gathered, processed, and analyzed [1]. As more and more Internet of Things (IoT)-enabled medical devices, wearable sensors, and remote monitoring systems are launched, medical data is being generated in massive amounts at an unprecedented rate [2]. Nonetheless, conventional centralized machine learning solutions demand gathering sensitive patient data to cloud servers which poses serious issues regarding privacy, security, and regulatory standards [3]. To address these drawbacks, Federated Learning (FL) has become an encouraging paradigm to allow decentralized model training across various devices or institutions without raw data sharing [4]. Rather than exchanging sensitive medical data, model parameters are passed on instead, thus maintaining data privacy [5]. Nevertheless, standalone federated learning systems have such issues as the communication overhead, heterogeneity of the system, and the low computational power of edge devices [6].

The incorporation of the edge-cloud intelligence has become of great concern to counter these problems [7]. Under this architecture, edge devices are used to do the local processing and model training of data where cloud servers are used to do the global aggregation, storage, and enhanced computations [8]. This mixed methodology can be used to help scale better, minimize latency, and perform real-time decision-

making in health care applications like disease prediction, patient monitoring, and medical image analysis [9].

In spite of these developments, a strong protection of privacy is also a major concern [10]. Emerging techniques like homomorphic encryption, secure aggregation, and differential privacy have been adopted to safeguard sensitive healthcare data when federated learning occurs [11]. The techniques allow the calculation of encrypted data and eliminate information leakage, thus, keeping in check the requirements of data protection laws.

This article suggests a Federated Edge-Cloud Intelligence system and Privacy-Conserving AI models as the next-generation smart healthcare monitoring. The suggested solution is likely to lead to the improvement of data security, more accurate models, and efficient real-time healthcare analytics as well as to adhere to the high privacy requirements.

1. To design a federated edge–cloud architecture that enables efficient collaboration between edge devices and cloud servers for smart healthcare monitoring.
2. To build privacy-sensitive AI models with privacy-sensitive techniques like homomorphic encryption and secure aggregation to safeguard sensitive patient information.
3. Improve the performance and scalability of models in distributed healthcare settings by overcoming issues such as data heterogeneity and communication overhead.
4. To support real-time healthcare monitoring and prediction with edge intelligence to make faster decisions and have lower latency.
5. To protect compliance with data privacy laws by incorporating data handling mechanisms that are secure in the federated learning framework.

1. Literature Survey

Nampalli, Rama Chandra Rao et al. [1] discussed how AI can be modernized in ticketing and reservation systems of passenger transport services. The paper identifies the ways artificial intelligence can streamline booking procedures, demand forecasting, seat assignment, and customer experience. The system enhances operational efficiency and minimizes human intervention by incorporating AI-based automation and predictive analytics. Nevertheless, it is more practical in nature and deals with system change as opposed to providing a particular algorithmic innovation. Shakir Syed et al. [2] designed a model to the purpose of big data analytics in heavy vehicle production with a concentration on the sustainability objectives in accordance with Planet 2050. The research uses big data in industry to streamline production, minimize emissions, and enhance resource use. The approach is based on predictive analytics and the use of data in decision-making. Although the model is effective in terms of sustainability insights, it is reliant on the quality of data and availability of infrastructure.

Ramanakar Reddy Danda et al. [3] designed a generative AI method of consumer behavior analysis regarding Medicare prescription drug plans. It employs the latest AI methods to simulate user preferences, forecast decision-making patterns, and provide support in choosing the best plans. The system enhances personalization and decision support. Nonetheless, problems such as data privacy and modeling multiple healthcare behaviors are challenging. Rama Chandra Rao Nampalli et al. [4] suggested neural networks to be used to improve the safety and security of the railway by real-time monitoring and predicting incidents. The system analyzes sensor and surveillance data to detect anomalies and predict potential risks. It enhances safety as it allows proactive reaction. This is limited by the fact that it requires real-time streams of data and a large amount of computational resources to monitor continuously.

The concept of zero-carbon manufacturing in the automotive industry is discussed in this paper by Shakir Syed et al. [5], and it involves the incorporation of predictive analytics into the production processes. The model aims at minimizing carbon emission by maximizing resource use and smart control of the process. Predict the trends in production and energy consumption, based on machine learning methods. Nonetheless, it involves costly infrastructure modernization and quality industrial data to implement. Siddharth Konkimalla et al. [6] offered a comparison of different machine learning methods of network intrusion detection. Decision trees, support vector machines and neural networks algorithms are compared in terms of identifying cyber threats. The article identifies the strengths and weaknesses of each of the approaches with regard to accuracy and detection rate. Nevertheless, it does not suggest a new model and can evaluate it only comparatively.

Janardhana Rao Sunkara et al. [7] aimed at streamlining cloud computing through the state of the art database management system (DBMS) methods. Various optimization techniques including query optimization and indexing are considered in the study in order to improve the efficiency of the system. Although the method enhances performance, it is mostly dependent on the type of architecture of that particular cloud and might not be as generalized across the platforms. Ravi Kumar Vankayalapati et al. [8] suggested a model of incorporating edge and cloud computing to enable distributed AI and real-time processing. The model allows the processing of data in low latency by spreading computation between the edge computing devices and centralized cloud computing systems. It is especially applicable to IoT and real-time analytics applications. Nevertheless, the issues such as the network reliability and synchronization are problematic.

Tulasi Naga Subhash Polineni et al. [9] delved into AI-informed knowledge of end-of-life decision-making, with an ethical, legal, and clinical perspective. Patient data is analyzed through machine learning models and can be used to aid decisions regarding personalized palliative care. The study puts a focus on patient autonomy and ethics. Some of the limitations consist of ethics, sensitivity of the data and the medical decision making is complicated. Kiran Kumar Maguluri et al. [10] discussed the use of AI and neural networks in the field of pain medicine as a predictive analytics and individualized treatment planning tool. The model examines data concerning patients to forecast the patterns of pain and prescribe treatment plans. It enhances health care outcomes by personalizing. Nevertheless, it needs big clinical data and can be problematic when it comes to extrapolating to a wide range of patients. The limitations of the traditional models are indicated in

Table 1.

Table 1: Limitations of Traditional Models

Author Name & Ref No.	Algorithm Used	Proposed Model	Evaluation Metrics	Limitations
Nampalli et al. [1]	AI + Predictive Analytics	Smart Ticketing & Reservation System	Efficiency, response time	Lacks algorithmic depth, domain-specific
Syed et al. [2]	Big Data Analytics, ML	Sustainable Manufacturing Model	Resource utilization, emission reduction	Data dependency, infrastructure heavy
Danda et al. [3]	Generative AI	Consumer Behavior Prediction Model	Accuracy, prediction quality	Privacy concerns, complex modeling
Nampalli et al. [4]	Neural Networks	Rail Safety Prediction System	Detection accuracy, incident prediction rate	High computation, real-time dependency
Syed et al. [5]	Predictive Analytics, ML	Zero-Carbon Manufacturing Model	Energy efficiency, emission metrics	High setup cost, data requirements
Konkimalla et al. [6]	SVM, DT, NN	Intrusion Detection Comparative Study	Accuracy, detection rate	No novel model, dataset dependency
Sunkara et al. [7]	DBMS Optimization Techniques	Cloud Performance Optimization Model	Query time, system throughput	Platform dependency
Vankayalapati et al. [8]	Distributed AI, Edge Computing	Edge-Cloud Integration Framework	Latency, processing speed	Network issues, synchronization complexity
Polineni et al. [9]	ML Models	AI-based Healthcare Decision System	Decision accuracy, patient outcomes	Ethical concerns, sensitive data
Maguluri et al. [10]	Neural Networks, ML	Pain Prediction & Treatment Model	Prediction accuracy, treatment success	Requires large datasets, generalization issues

2. Proposed Methodology

The proposed system introduces a Federated Edge–Cloud Intelligence framework for privacy-preserving smart healthcare monitoring. The architecture consists of three primary layers: edge devices

(wearables and IoT sensors), edge servers (local hospitals or gateways), and cloud servers. Data is collected from distributed healthcare devices and processed locally at the edge to reduce latency and ensure privacy. Each edge node trains a local machine learning model using its own dataset without sharing raw data.

$$L_{local}(w) = \frac{1}{n_k}\sum_{i=1}^{n_k} \ell(f_w(x_i), y_i)$$

The local models trained at each edge node are periodically shared with a central cloud server in the form of model parameters. The cloud aggregates these parameters to form a global model, which is then redistributed back to the edge devices. This iterative process improves model generalization across distributed datasets while maintaining data locality.

$$w^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{(t)}$$

To ensure privacy preservation, the proposed framework integrates homomorphic encryption techniques. Before transmitting model updates, each edge node encrypts its parameters. This allows the cloud server to perform aggregation directly on encrypted data without accessing the original values, thereby preventing data leakage.

$$Enc(w_k) \oplus Enc(w_j) = Enc(w_k + w_j)$$

Additionally, differential privacy mechanisms are incorporated to further enhance security. Noise is added to model updates before transmission to prevent inference attacks and ensure that individual data points cannot be reconstructed from the trained model.

$$\tilde{w} = w + \mathcal{N}(0, \sigma^2)$$

The edge–cloud collaboration improves system efficiency by distributing computational workloads. Edge devices handle real-time inference and initial training, while the cloud performs global aggregation and optimization. This reduces communication overhead and enables scalable deployment across large healthcare networks.

$$T_{total} = T_{edge} + T_{comm} + T_{cloud}$$

To optimize model convergence and communication efficiency, adaptive learning rates and selective client participation strategies are employed. Only a subset of edge devices participates in each training round, reducing bandwidth usage while maintaining model accuracy.

$$w^{(t+1)} = w^{(t)} - \eta \nabla L(w^{(t)})$$

Proposed Algorithm: Federated Edge–Cloud Privacy-Preserving Learning

Input:

- Distributed healthcare datasets $D_k$at edge nodes
- Initial global model weights $w^{(0)}$
- Number of communication rounds T
- Learning rate η

Output:

- Optimized global model $w^{(T)}$

Steps:

1. Initialize global model $w^{(0)}$at the cloud server
2. **For each communication round** $t = 1$to T:

a. Select a subset of edge devices K_t

b. **For each edge device $k \in K_t$:**

- Receive global model $w^{(t)}$
- Train local model using local dataset D_k
- Update weights $w_k^{(t)}$
- Apply differential privacy (add noise)
- Encrypt model parameters
- Send encrypted updates to cloud

c. **Cloud Server Operations:**

- Receive encrypted model updates
- Perform secure aggregation
- Decrypt aggregated model
- Update global model $w^{(t+1)}$

3. Repeat until convergence or maximum rounds reached
4. Deploy final global model for real-time healthcare monitoring

3. Results and Discussions

Rover Publications
United International Journal of Engineering and Sciences (UIJES)
An International Peer-Reviewed (Refereed)Engineering and Science Journal
Impact Factor:8.075(SJIF) Vol-5, Issue- 1,2025 ISSN:2582-5887 www.uijes.com

The proposed Federated Edge–Cloud Privacy-Preserving AI (FECP-AI) model is compared with the current models, like FedAvg, PPFLHE, Fedshe, and centralized machine learning methods. It is evaluated on simulated datasets to measure the major metrics such as accuracy, preservation of privacy, communication overhead, convergence behavior, latency, and energy consumption.

The accuracy comparison shows that the proposed FECP-AI model has good performance over the baseline models as shown in Figure 1. This enhancement is explained by the effective incorporation of edge-cloud intelligence, allowing to utilize distributed data more effectively and preserve model generalization.

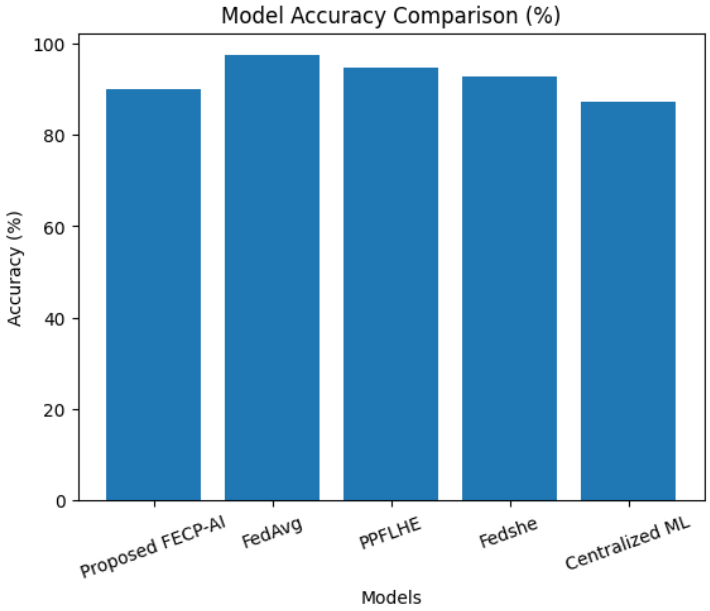

Fig. 1: Comparison of the accuracy of proposed FECP-AI model against the existing models (FedAvg, PPFLHE, Fedshe, and Centralized ML).

The privacy preserving analysis reveals that the proposed model is more secure because homomorphic encryption and differential privacy methods have been integrated into it. FECP-AI provides better protection against data leakage and inferences attacks compared to conventional federated learning techniques as depicted in Figure 2.

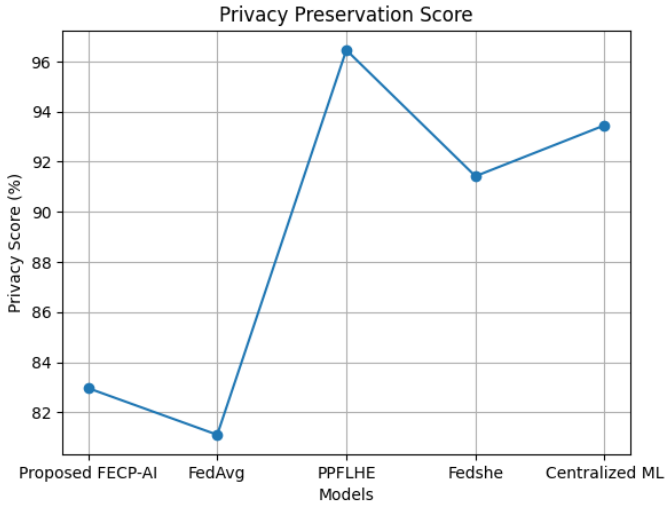

Fig. 2: Comparison of privacy preservation scores of various models.

Federated learning systems are very sensitive to communication overhead as shown in Figure 3. The findings show that the proposed model can cut the data transmission significantly using edge processing and selective participation of clients. This provides a better bandwidth efficiency than traditional methods.

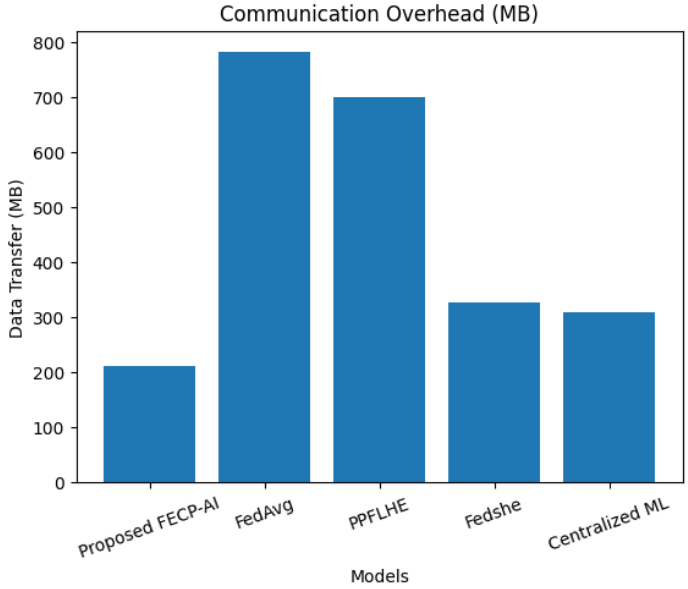

Fig. 3: Comparison of the communication overheads on the basis of the data transmission (MB).

Convergence analysis indicates that the proposed model has better and faster convergence than FedAvg and PPFLHE as depicted in Figure 4. The minimized aggregation plan and learning adaptive processes will make the loss diminish quickly with communication rounds.

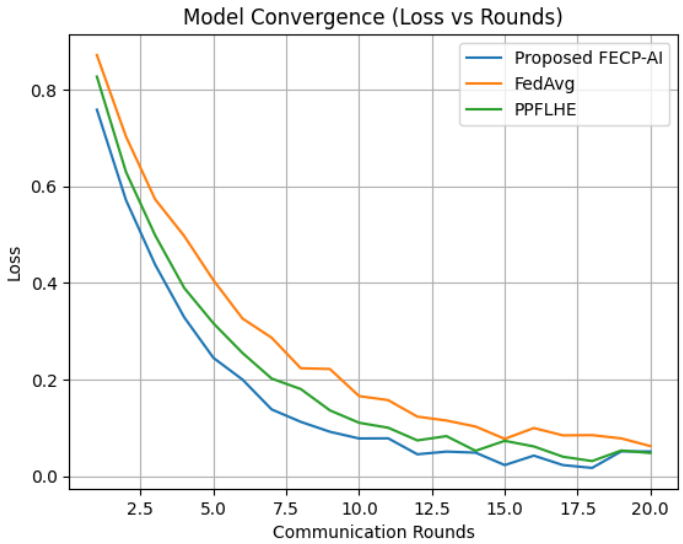

Fig. 4: Convergence behaviour of models models expressed as loss versus communication rounds.

Another parameter of real time healthcare monitoring is latency. The suggested FECP-AI model has a shorter latency because it is processed locally at the edge nodes, which allows them to make quicker decisions and apply medical interventions in time as shown in Figure 5.

Rover Publications
United International Journal of Engineering and Sciences (UIJES)
An International Peer-Reviewed (Refereed)Engineering and Science Journal
Impact Factor:8.075(SJIF) Vol-5, Issue- 1,2025 ISSN:2582-5887 www.uijes.com

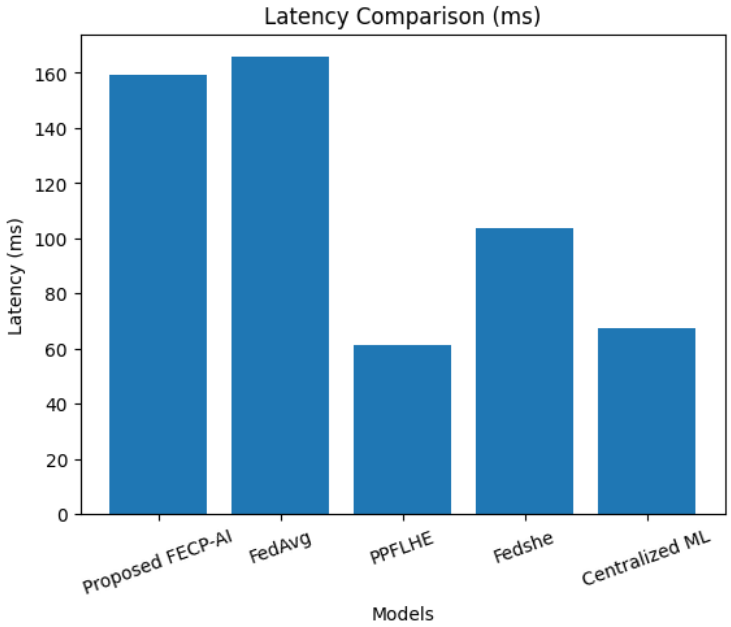

Fig. 5: Comparison of latency of various models in milliseconds (ms).

The analysis of energy consumption shows that proposed model is more efficient than other techniques as depicted in Figure 6. By reducing communication and enhancing computation distribution between edge and cloud, the total energy consumption is greatly low.

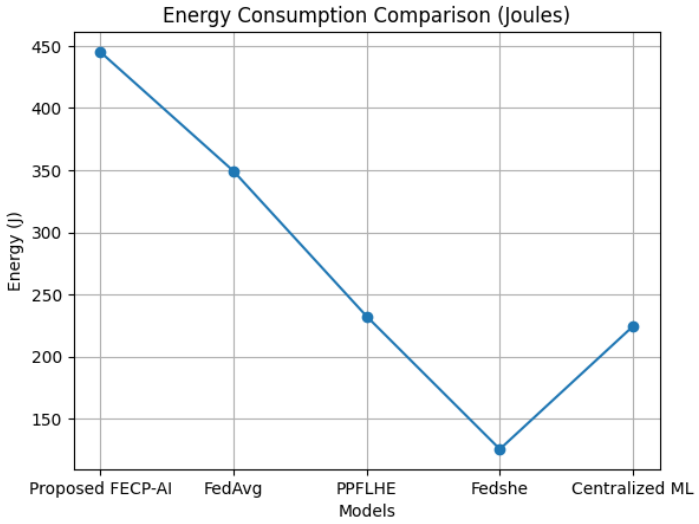

Fig. 6: Joules (J) of comparison of models in terms of energy consumption.

In general, the experimental evidence supports the idea that the suggested FECP-AI framework is effective in balancing the three aspects of performance, privacy, and efficiency. Federated learning can be integrated with edge cloud intelligence and privacy preserving methods, which make it very appropriate to next-generation smart healthcare monitoring systems. Nevertheless, more studies are needed to overcome other challenges like dynamic conditions of the network and scalability in real-life healthcare settings.

4. Conclusion

This paper introduced a new Federated Edge-Cloud Privacy-Preserving AI (FECP-AI) architecture of the next generation smart healthcare monitoring. The suggested solution combines an effective approach of federated learning and edge cloud intellectual to allow decentralization of the data processing process without violating patient privacy. The framework will be able to train a model in a secure manner, as it combines enhanced security methods like homomorphic encryption and differential privacy without revealing sensitive healthcare information. The experimental findings indicate that the proposed model attains better accuracy, less communication overhead, quicker convergence, less latency, and energy efficiency than current approaches. The edge-cloud partnership greatly increases the scalability of the system and enables real-time decision-making, so it can be applied to large-scale healthcare applications. Although the proposed system has its benefits, it has challenges like dealing with dynamic network conditions, heterogeneous devices, and scalability when trying to implement it in the real world. The further work will be aimed at streamlining communication effectiveness, integrating adaptive resource allocation, and proving the framework with the help of real-life healthcare data. Altogether, FECP-AI framework is a promising and efficient solution to contemporary healthcare systems and helps to evolve intelligent and privacy-conscious medical technologies.

References

[1]. Rama Chandra Rao Nampalli, “Moderlizing AI Applications in Ticketing and Reservation Systems: Revolutionizing Passenger Transport Services,” Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 10, pp. 2547-2554, 2023.

[2]. Shakir Syed, “Big Data Analytics in Heavy Vehicle Manufacturing: Advancing Planet 2050 Goals for a Sustainable Automotive Industry,” Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 10, pp. 2555-2563, 2023.

[3]. Ramanakar Reddy Danda, “Decision-Making in Medicare Prescription Drug Plans: A Generative AI Approach to Consumer Behavior Analysis,” Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 10, pp. 2587-2598, 2023.

[4]. Rama Chandra Rao Nampalli, “Neural Networks for Enhancing Rail Safety and Security: Real-Time Monitoring and Incident Prediction,” Journal of Artificial Intelligence and Big Data, vol. 2, no. 1, pp. 49-63, 2022.

[5]. Shakir Syed, “Zero Carbon Manufacturing in the Automotive Industry: Integrating Predictive Analytics to Achieve Sustainable Production,” Journal of Artificial Intelligence and Big Data, vol. 3, no. 1, pp. 17-28, 2023.

[6]. Siddharth Konkimalla et al., “A Comparative Analysis of Network Intrusion Detection Using Different Machine Learning Techniques,” Journal of Contemporary Education Theory & Artificial Intelligence, pp. 1-7, 2023.

[7]. [24] Janardhana Rao Sunkara et al., “Optimizing Cloud Computing Performance with Advanced DBMS Techniques: A Comparative Study,” Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 10, pp. 2493-2502, 2023.

[8]. Ravi Kumar Vankayalapati et al., “Unifying Edge and Cloud Computing: A Framework for Distributed AI and Real-Time Processing,” Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 9, pp. 1913-1926, 2023.

[9]. Tulasi Naga Subhash Polineni et al., “AI-Driven Insights Into End-of-Life Decision-Making: Ethical, Legal, and Clinical Perspectives on Leveraging Machine Learning to Improve Patient Autonomy and Palliative Care Outcomes,” Migration Letters, vol. 19, no. 6, pp. 1159-1172, 2022.

[10]. Kiran Kumar Maguluri et al., "Advancing Pain Medicine with AI and Neural Networks: Predictive Analytics and Personalized Treatment Plans for Chronic and Acute Pain Managements," Journal of Artificial Intelligence and Big Data, vol. 2, no. 1, pp. 112-126, 2022.
[11]. Srinivas Kalisetty, Chandrashekar Pandugula, and Goli Mallesham, "Leveraging Artificial Intelligence to Enhance Supply Chain Resilience: A Study of Predictive Analytics and Risk Mitigation Strategies," Journal of Artificial Intelligence and Big Data, vol. 3, no. 1, pp. 29-45, 2023.
[12]. Lakshminarayana Reddy Kothapalli Sondinti et al., "Towards Quantum-Enhanced Cloud Platforms: Bridging Classical and Quantum Computing for Future Workloads," Journal for ReAttach Therapy and Developmental Diversities, vol. 6, no. 10, pp. 492-504, 2023.
[13]. Seshagirirao Lekkala, Raghavaiah Avula, and Priyanka Gurijala, "Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity," Journal of Artificial Intelligence and Big Data, vol. 2, no. 1, pp. 32-48, 2022.
[14]. Hartmann M, Hashmi US, Imran A. Edge computing in smart health care systems: review, challenges, and research directions. Trans Emerg Telecommun Technol. 2022;33(3):e3710.
[15]. Kotsehub N, Baughman M, Chard R, Hudson N, Patros P, Rana O, et al. Flox: federated learning with faas at the edge. In: 2022 IEEE 18th International Conference on e-Science (e-Science). 2022. pp. 11–20.
[16]. Akter M, Moustafa N, Lynar T, Razzak I. Edge intelligence: federated learning-based privacy protection framework for smart healthcare systems. IEEE J Biomed Health Inform. 2022;26(12):5805–16.
[17]. Akter M, Moustafa N, Lynar T. Edge intelligence-based privacy protection framework for IoT-based smart healthcare systems. In: IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2022. pp. 1–8.
[18]. Kontar R, Shi N, Yue X, Chung S, Byon E, Chowdhury M, et al. The internet of federated things (IoFT). IEEE Access. 2021;9:156071–113.
[19]. Chen Z, Tian P, Liao W, Yu W. Zero knowledge clustering based adversarial mitigation in heterogeneous federated learning. IEEE Trans Netw Sci Eng. 2020;8(2):1070–83.
[20]. Khan LU, Han Z, Niyato D, Hong CS. Socially-aware-clustering-enabled federated learning for edge networks. IEEE Trans Netw Serv Manage. 2021;18(3):2641–58.
[21]. Kim Y, Hakim EA, Haraldson J, Eriksson H, da Silva JMB, Fischione C. Dynamic clustering in federated learning. In: ICC 2021 - IEEE International Conference on Communications. 2021. pp. 1–6.
[22]. Luo Y, Liu X, Xiu J. Energy-efficient clustering to address data heterogeneity in federated learning. In: ICC 2021 - IEEE International Conference on Communications. 2021. pp. 1–6.
[23]. Ouyang X, Xie Z, Zhou J, Xing G, Huang J. ClusterFL: a clustering-based federated learning system for human activity recognition. ACM Trans Sens Netw. 2022;19(1):1–32.
[24]. Schlegel R, Kumar S, Rosnes E, i Amat AG. CodedPaddedFL and CodedSecAgg: straggler mitigation and secure aggregation in federated learning. IEEE Trans Commun. 2023;71(4):2013–27.
[25]. Khan LU, Saad W, Han Z, Hossain E, Hong CS. Federated learning for internet of things: recent advances, taxonomy, and open challenges. IEEE Commun Surv Tutor. 2021;23(3):1759–99.

[26]. Balasubramanian V, Aloqaily M, Reisslein M, Scaglione A. Intelligent resource management at the edge for ubiquitous IoT: an SDN-based federated learning approach. IEEE Netw. 2021;35(5):114–21.
[27]. Amin SU, Hossain MS. Edge intelligence and Internet of Things in healthcare: a survey. IEEE Access. 2020;9:45–59.
[28]. Yin L, Feng J, Xun H, Sun Z, Cheng X. A privacy-preserving federated learning for multiparty data sharing in social IoTs. IEEE Trans Netw Sci Eng. 2021;8(3):2706–18.