Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 25-32
Impact Factor-2.05

Federated Learning in Cloud-Based Healthcare: Privacy-Preserving AI for Personalize Medicine

[1]Karthik Kushala
Celer Systems Inc, Folsom, California, USA
karthik.kushala@gmail.com

[2]Priyadarshini Radhakrishnan
Technical Lead, IBM,
Anthem, USA,
priyadarshinir990@gmail.com

[3]Vijai Anand Ramar
Delta Dental Insurance Company, Georgia, USA
vijaianandramar@gmail.com

[4]Venkataramesh Induru
Piorion Solutions Inc, New York, USA
venkatarameshinduru@gmail.com

[5]Karthick.M
Nandha College of Technology, Erode
magukarthik@gmail.com

Abstract

The use of artificial intelligence in medical systems has the potential to change the process of medical diagnosis, treatment planning, and delivery of tailored medicine. The creation of reliable and accurate AI models normally depends on having large-scale, heterogeneous patient information, which normally resides in diverse healthcare institutions. Centralization of this type of data creates strong concerns regarding patient privacy, security of data, and compliance. Federated learning provides a promising remedy by allowing shared model training across distributed data sources with sensitive information being kept in each institution locally. Here, model updates—rather than raw data—are sent to a central aggregator with privacy laws like HIPAA and GDPR maintained. In a cloud-based setup, federated learning can scale well and ensure secure communication and data privacy using methods like differential privacy and homomorphic encryption. The local models get learned based on algorithms for healthcare applications such as disease diagnosis and drug response prediction, and their encrypted updates are combined to build a global model. The global model achieves better accuracy and generalization compared to models trained from local data alone. Examination of the training process also shows that the federated method facilitates stable convergence and successful knowledge transfer between institutions.

Keywords: Federated Learning, Privacy-Preserving AI, Cloud-Based Healthcare, Personalized Medicine, Data Security

1. Introduction

The accelerated development of artificial intelligence in the healthcare space has given birth to new opportunities in disease diagnosis, treatment planning, and personalized medicine. Nevertheless, the performance of AI models is still largely reliant on availability of plenty of varied and quality patient data, most of the times scattered across various hospitals and healthcare centres. Companies can gain unprecedented scalability, flexibility, and value through the cloud-based transition of CRM, and on demand in line with digital age requirements [1]. Customer Relationship Management is a pillar tactic that companies adopt so that they can manage customer and prospective customer interactions effectively [2]. Sparsity issue of collaborative filtering systems that have an important place in recommendation systems of online social networks is solved differently in this study [3]. Vehicular Cloud Computing is a novel paradigm that merges vehicular networks and cloud computing to offer enhanced services and system efficiency in transport [4]. Efficiency, performance, scalability, and cost-effectiveness are the principal objectives of the entire process of optimizing cloud computing environments [5]. Security and data integrity are primary characteristics of today's cloud computing platform [6]. Multi-cloud storage can effectively provide data integrity using blockchain technology [7]. The data security is most vital in cloud computing since data retained and processed within cloud environments is sensitive information[8]. The algorithms overcome the intrinsic issues with resource allocation, parameter tuning, and probabilistic inference [9]. Paediatrics readmissions are extremely expensive to the health system, contributing to cost, testing capacity, and undermining the health outcomes of children [10].

The rising need for real-time processing of information in healthcare services has hastened the need for low-latency and efficient communication systems more and more [11]. Neuromorphic and bio-inspired computing, an imitation of biological processes to enhance productivity, agility, and real time decision-making [12], is revolutionizing healthcare networks. As an effort to improve operational performance and strategic decision-making, the present study analyses the way Internet of Things and Big Data Analytics can be applied within the Business Intelligence framework [13]. The expansion of the Internet of Things introduces more and more devices interconnected in the multidimensional space, and thus, an unimaginable increase in network traffic [14]. Decision-making has also been completely overhauled with the advent of artificial intelligence technology in the Clinical division of medical science, especially in Clinical Decision Support System development [15].

The fast evolution of Industry 4.0 has promoted traditional manufacturing to intelligent manufacturing, and Industrial Internet of Things devices are the driving force for enhancing processes to be more efficient, automated, and data-driven decision making [16]. Robust network security in cloud environments is significant because the increasing number of cyber-attacks on cloud-based infrastructures is growing [17]. Cloud-based diagnosis and monitoring of patients through the Hybrid LSTM-Attention is a significant step towards digital healthcare in which deep learning is appropriately integrated into real-time medical data processing [18]. The paper introduces a cloud-based Internet of Things platform to improve healthcare data monitoring and sharing. As there is manyfold growth in IoT devices in healthcare, integration and data exchange are unavoidable to maximize patient care and operational efficiency[19]. Healthcare information's rapid growth rate and the growing need for proper handling have been challengeable in cloud healthcare systems in terms of integration, data protection, and scaling [20].

Federated learning (FL) in cloud-based healthcare systems enables the training of machine learning models on decentralized data while preserving privacy and security, crucial for sensitive health information [21]. By utilizing multiple healthcare providers' data without sharing, it directly, FL allows for collaborative learning, making it an ideal solution for situations where patient data is distributed across various institutions [22]. This approach enhances data privacy by ensuring that raw data never leaves local servers, only model updates are shared [23]. Furthermore, FL in healthcare can help create more robust models by utilizing diverse datasets across different geographic regions and medical settings [24]. As a result, FL can improve the generalization of AI models, which is essential for applications like disease prediction and patient monitoring [25]. Moreover, federated learning has shown promising results in reducing communication costs and improving efficiency compared to traditional centralized approaches [26]. Integration of FL in cloud-based systems also allows for scalable and adaptable solutions, enabling continuous learning from new data as it becomes available [27]. However, challenges related to data heterogeneity, system synchronization, and model aggregation still need to be addressed for optimal deployment in healthcare applications [28]. Key contributions of this article are,

1. Privacy-Preserving Framework: Developed a federated learning framework that allows cooperative training of AI models without exposure to raw patient data.
2. Cloud-Based Scalability: Combined the federated learning framework with cloud computing capabilities to allow for seamless coordination and secure model aggregation.
3. Healthcare-Specific Modelling: Utilized machine learning algorithms tailored to healthcare operations like disease diagnosis and drug response prediction.

2. Related Words

JOURNAL OF CURRENT SCIENCE AND HUMANITIES
Impact Factor-2.05

[29] examines how RFID and blockchain technology are blended to facilitate data sharing and security in medicine, especially in big data medical research. Physiological signals in real-time needed for disease diagnosis and monitoring health are recorded using RFID and are transmitted securely with the help of blockchain. [30] explores a Data-Driven Analysis of Employee Promotion: The Role of the Position of Organisation, examines the way the probability of an employee's promotion depends on where they are placed within the organisational hierarchy. [31] examine uncertainty in work package processing times by offering two stochastic models for staff planning and project scheduling. [32] suggested a blockchain-based federated cloud computing model that can reduce the BDG and enhance cyber security. [33] presents a cost-effective large data clustering algorithm for cloud computing by eliminating redundant long tail data.

[34] in Deep Feature Learning for Medical Image Analysis with Convolutional Autoencoder Neural Network explain the feature extraction capability of medical images through convolutional autoencoders, i.e., CT scans and MRI. [35] address the prediction of heart disease, a leading cause of death, using machine learning based on clinical data. Their new hybrid model, which includes random forest and linear techniques, seeks to identify influential predictive features. [36] analyse the predictors expected to cause drug side effects in older adults, noting the complexity of polypharmacy in geriatric medicine. [37] talks about current and future applications of machine learning in radiology, such as how ML algorithms may improve diagnostic accuracy, reduce errors, and optimize workflow efficiency in medical imaging. [38] employed Bio-Geography Based Optimization (BBO) to categorize MRI images for brain cancer prediction plan planning.

Federated learning (FL) in cloud-based healthcare systems enables the training of machine learning models on decentralized data while preserving privacy and security, crucial for sensitive health information [39]. By utilizing multiple healthcare providers' data without sharing, it directly, FL allows for collaborative learning, making it an ideal solution for situations where patient data is distributed across various institutions [40]. This approach enhances data privacy by ensuring that raw data never leaves local servers, only model updates are shared [41]. Furthermore, FL in healthcare can help create more robust models by utilizing diverse datasets across different geographic regions and medical settings [42]. As a result, FL can improve the generalization of AI models, which is essential for applications like disease prediction and patient monitoring [43]. Moreover, federated learning has shown promising results in reducing communication costs and improving efficiency compared to traditional centralized approaches [44].

Integration of FL in cloud-based systems also allows for scalable and adaptable solutions, enabling continuous learning from new data as it becomes available [45]. However, challenges related to data heterogeneity, system synchronization, and model aggregation still need to be addressed for optimal deployment in healthcare applications [46]. Additionally, the implementation of FL can potentially enable more personalized healthcare by tailoring models to specific population groups or individual patients [47]. Moreover, the use of FL in healthcare also holds promise for improving patient outcomes through more accurate real-time diagnostics and treatment recommendations by continuously learning from the evolving data [48].

3. Problem statement

The creation of correct and trustworthy AI models within medicine is significantly impeded by the inconsistent and sensitive character of medical data distributed across numerous institutions and hospitals [49].

Objectives

1. Facilitate federated AI model training among various healthcare institutions without the need to share raw patient data.
2. Ensure adherence to healthcare data privacy laws like HIPAA and GDPR.
3. Develop and deploy a cloud-based federated learning architecture with robust security features.

4. Proposed Methodology for Privacy-Preserving Federated Learning in Cloud-Based Healthcare Systems

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 25-32
Impact Factor-2.05

The proposed solution leverages a federated learning architecture to enable safe, privacy-enhancing AI model training on distributed cloud-connected health centres. The data is collected and stored locally at each hospital or healthcare facility from sources such as Electronic Health Records, imaging, and wearable sensors in strict compliance with privacy policies such as HIPAA and GDPR.

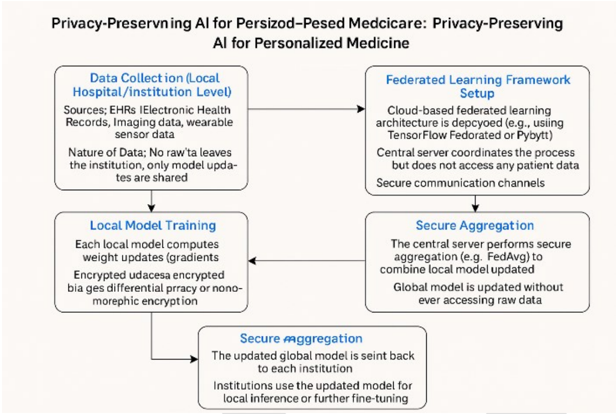

Figure 1: Proposed Methodology for Privacy-Preserving Federated Learning in Cloud-Based Healthcare Systems

4.1 Data Collection

Data in the envisioned federated learning system is gathered locally within individual hospitals and healthcare centres. Data includes a range of sources like Electronic Health Records [50], medical images, and wearable health device data.

4.2 Local Model Training

In the federated learning system, local AI models are learned separately by each involved hospital or care facility on its own patient dataset.

4.3 Federated Learning Framework Installation

There is a federated learning cloud-based architecture that allows cooperative model training in various healthcare institutions without infringing on patient privacy.

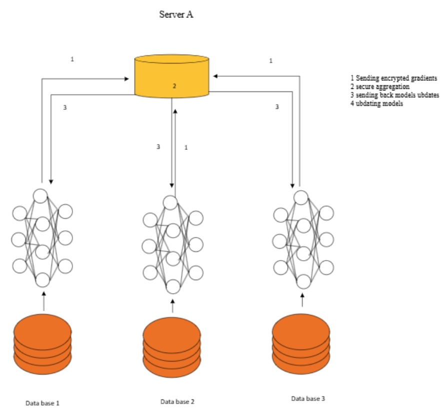

Figure 2: Architecture of Federated Learning

4.4 Model Update Sharing

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (2), 2022, 25-32
JCSH JOURNAL OF CURRENT SCIENCE AND HUMANITIES
Impact Factor-2.05

After local training is finished, every institution calculates the weight updates or gradients out of its model. To make sure data stays private and will not leak, these updates get encrypted with next-generation privacy-protection methods such as differential privacy or homomorphic encryption.

5. Results and Discussion

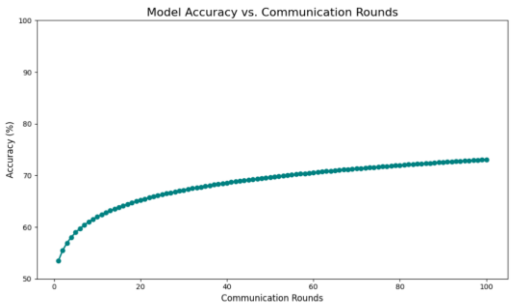

Figure 3: Model Accuracy vs Communication Rounds

This graph demonstrates step by step improvement in the accuracy of the global federated model with successive rounds of interaction. Since every round is constituted by aggregation of updates of locally trained models by all the involved institutions, performance of models gets improved due to the group learning effect.

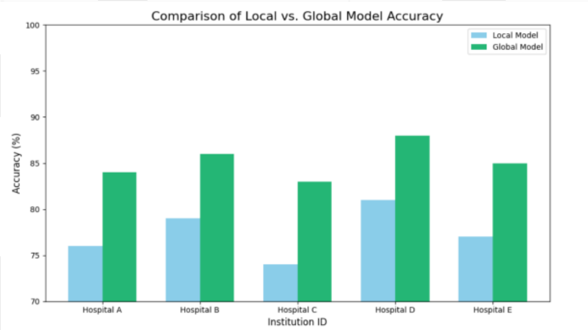

Figure 4: Comparison Of Local Vs Global Model Accuracy

This plot depicts how the precision of locally learned models in individual institutions compares with that of globally averaged model derived using federated learning. The health institution is represented by two bars, on which the first one represents the precision derived by a global model whenever these are applied on the common local data.

5.1 Discussion

The findings of this study offer the efficacy of federated learning in creating privacy-preserving yet accurate AI models for precision medicine in cloud-based healthcare settings. By enabling a collection of institutions to work together and train a global model without having to share sensitive patient data, federated learning provides not only a means for compliance with rigorous data privacy regulations but also model generalizability across diverse populations.

6. Conclusion and Future Work

This paper proves that federated learning provides a strong and privacy-preserving alternative to training AI models in cloud-based healthcare systems. Through collaborative model training without the exchange of raw patient data, the approach maintains data confidentiality while leveraging the richness and diversity of decentralized data sets.

JCSH JOURNAL OF CURRENT SCIENCE AND HUMANITIES
Impact Factor-2.05

Subsequent work will target overcoming some of the existing federated learning architecture's limitations, including data heterogeneity management between institutions and minimizing training communication overhead. It is also worth investigating more sophisticated personalization methods that enable the global model to learn more about the local patient population.

References

[1] Akhil, R.G.Y. (2021). Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology & Computer Engineering, 9(2), ISSN 2347–3657.

[2] Wu, Q., Chen, X., Zhou, Z., & Zhang, J. (2020). Fedhome: Cloud-edge based personalized federated learning for in-home health monitoring. IEEE Transactions on Mobile Computing, 21(8), 2818-2832.

[3] Yalla, R.K.M.K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 17 (4).

[4] Prayitno, Shyu, C. R., Putra, K. T., Chen, H. C., Tsai, Y. Y., Hossain, K. T., ... & Shae, Z. Y. (2021). A systematic review of federated learning in the healthcare area: From the perspective of data properties and applications. Applied Sciences, 11(23), 11191.

[5] Harikumar, N. (2021). Streamlining Geological Big Data Collection and Processing for Cloud Services. Journal of Current Science, 9(04), ISSN NO: 9726-001X.

[6] Elayan, H., Aloqaily, M., & Guizani, M. (2021). Sustainability of healthcare data analysis IoT-based systems using deep federated learning. IEEE Internet of Things Journal, 9(10), 7338-7346.

[7] Basava, R.G. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 02(01), 122–131.

[8] Lim, W. Y. B., Garg, S., Xiong, Z., Niyato, D., Leung, C., Miao, C., & Guizani, M. (2020). Dynamic contract design for federated learning in smart healthcare applications. IEEE Internet of Things Journal, 8(23), 16853-16862.

[9] Sri, H.G. (2021). Integrating HMI display module into passive IoT optical fiber sensor network for water level monitoring and feature extraction. World Journal of Advanced Engineering Technology and Sciences, 02(01), 132–139.

[10] Abawajy, J. H., & Hassan, M. M. (2017). Federated internet of things and cloud computing pervasive patient health monitoring system. IEEE Communications Magazine, 55(1), 48-53.

[11] Rajeswaran, A. (2021). Advanced Recommender System Using Hybrid Clustering and Evolutionary Algorithms for E-Commerce Product Recommendations. International Journal of Management Research and Business Strategy, 10(1), ISSN 2319-345X.

[12] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(3), 1622-1658.

[13] Sreekar, P. (2021). Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges. International Journal of Modern Electronics and Communication Engineering, 9(4), ISSN2321-2152.

[14] Lin, H., Kaur, K., Wang, X., Kaddoum, G., Hu, J., & Hassan, M. M. (2021). Privacy-aware access control in IoT-enabled healthcare: A federated deep learning approach. IEEE Internet of Things Journal, 10(4), 2893-2902.

[15] Naresh, K.R.P. (2021). Optimized Hybrid Machine Learning Framework for Enhanced Financial Fraud Detection Using E-Commerce Big Data. International Journal of Management Research & Review, 11(2), ISSN: 2249-7196.

[16] Han, B., Jhaveri, R. H., Wang, H., Qiao, D., & Du, J. (2021). Application of robust zero-watermarking scheme based on federated learning for securing the healthcare data. IEEE journal of biomedical and health informatics, 27(2), 804-813.

[17] Sitaraman, S. R. (2021). AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing. International Journal of Information Technology and Computer Engineering, 12(2).

[18] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated learning for industrial internet of things in future industries. IEEE Wireless Communications, 28(6), 192-199.

JCSH
JOURNAL OF CURRENT SCIENCE AND HUMANITIES
Impact Factor-2.05

[19] Mamidala, V. (2021). Enhanced Security in Cloud Computing Using Secure Multi-Party Computation (SMPC). International Journal of Computer Science and Engineering(IJCSE), 10(2), 59–72.
[20] Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2021). Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Communications Surveys & Tutorials, 23(3), 1759-1799.
[21] Sareddy, M. R. (2021). The future of HRM: Integrating machine learning algorithms for optimal workforce management. International Journal of Human Resources Management (IJHRM), 10(2).
[22] Mohan, K., & Aramudhan, M. (2017). Broker based trust architecture for federated healthcare cloud system. Intelligent Automation & Soft Computing, 23(3), 477-483.
[23] Chetlapalli, H. (2021). Enhancing Test Generation through Pre-Trained Language Models and Evolutionary Algorithms: An Empirical Study. International Journal of Computer Science and Engineering(IJCSE), 10(1), 85–96
[24] Zhou, C., Fu, A., Yu, S., Yang, W., Wang, H., & Zhang, Y. (2020). Privacy-preserving federated learning in fog computing. IEEE Internet of Things Journal, 7(11), 10782-10793.
[25] Basani, D. K. R. (2021). Leveraging Robotic Process Automation and Business Analytics in Digital Transformation: Insights from Machine Learning and AI. International Journal of Engineering Research and Science & Technology, 17(3).
[26] Sarma, K. V., Harmon, S., Sanford, T., Roth, H. R., Xu, Z., Tetreault, J., ... & Arnold, C. W. (2021). Federated learning improves site performance in multicenter deep learning without data sharing. Journal of the American Medical Informatics Association, 28(6), 1259-1264.
[27] Sareddy, M. R. (2021). Advanced quantitative models: Markov analysis, linear functions, and logarithms in HR problem solving. International Journal of Applied Science Engineering and Management, 15(3).
[28] Jiang, J. C., Kantarci, B., Oktug, S., & Soyata, T. (2020). Federated learning in smart city sensing: Challenges and opportunities. Sensors, 20(21), 6230.
[29] Bobba, J. (2021). Enterprise financial data sharing and security in hybrid cloud environments: An information fusion approach for banking sectors. International Journal of Management Research & Review, 11(3), 74–86.
[30] Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., ... & Poor, H. V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet of Things Journal, 8(16), 12806-12825.
[31] Narla, S., Peddi, S., & Valivarthi, D. T. (2021). Optimizing predictive healthcare modelling in a cloud computing environment using histogram-based gradient boosting, MARS, and SoftMax regression. International Journal of Management Research and Business Strategy, 11(4).
[32] Gollapalli, V. S. T. (2020). ENHANCING DISEASE STRATI FICATION USING FEDERATED LEARNING AND BIG DATA ANALYTICS IN HEALTHCARE SYSTEMS. International Journal of Management Research and Business Strategy, 10(4), 19-38.
[33] Kethu, S. S., & Purandhar, N. (2021). AI-driven intelligent CRM framework: Cloud-based solutions for customer management, feedback evaluation, and inquiry automation in telecom and banking. Journal of Science and Technology, 6(3), 253–271.
[34] Khan, L. U., Saad, W., Han, Z., & Hong, C. S. (2021). Dispersed federated learning: Vision, taxonomy, and future directions. IEEE Wireless Communications, 28(5), 192-198.
[35] Srinivasan, K., & Awotunde, J. B. (2021). Network analysis and comparative effectiveness research in cardiology: A comprehensive review of applications and analytics. Journal of Science and Technology, 6(4), 317–332.
[36] Imteaj, A., Thakker, U., Wang, S., Li, J., & Amini, M. H. (2021). A survey on federated learning for resource-constrained IoT devices. IEEE Internet of Things Journal, 9(1), 1-24.
[37] Narla, S., & Purandhar, N. (2021). AI-infused cloud solutions in CRM: Transforming customer workflows and sentiment engagement strategies. International Journal of Applied Science Engineering and Management, 15(1).
[38] Zhan, Y., Li, P., Guo, S., & Qu, Z. (2021). Incentive mechanism design for federated learning: Challenges and opportunities. IEEE network, 35(4), 310-317.

[39] Budda, R. (2021). Integrating artificial intelligence and big data mining for IoT healthcare applications: A comprehensive framework for performance optimization, patient-centric care, and sustainable medical strategies. International Journal of Management Research & Review, 11(1), 86–97.

[40] Lim, W. Y. B., Luong, N. C., Hoang, D. T., Jiao, Y., Liang, Y. C., Yang, Q., ... & Miao, C. (2020). Federated learning in mobile edge networks: A comprehensive survey. IEEE communications surveys & tutorials, 22(3), 2031-2063.

[41] Ganesan, T., & Devarajan, M. V. (2021). Integrating IoT, Fog, and Cloud Computing for Real-Time ECG Monitoring and Scalable Healthcare Systems Using Machine Learning-Driven Signal Processing Techniques. International Journal of Information Technology and Computer Engineering, 9(1).

[42] Patell, J. (2020). Prospects of Cloud-Driven Deep Learning-Leading the Way for Safe and Secure AI. INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES, 8(3), 10-55083.

[43] Pulakhandam, W., & Samudrala, V. K. (2021). Enhancing SHACS with Oblivious RAM for secure and resilient access control in cloud healthcare environments. International Journal of Engineering Research and Science & Technology, 17(2).

[44] Xu, Y., Lu, Z., Gai, K., Duan, Q., Lin, J., Wu, J., & Choo, K. K. R. (2021). BESIFL: Blockchain-empowered secure and incentive federated learning paradigm in IoT. IEEE Internet of Things Journal, 10(8), 6561-6573.

[45] Jayaprakasam, B. S., & Thanjaivadivel, M. (2021). Integrating deep learning and EHR analytics for real-time healthcare decision support and disease progression modeling. International Journal of Management Research & Review, 11(4), 1–15. ISSN 2249-7196.

[46] Liu, Y., James, J. Q., Kang, J., Niyato, D., & Zhang, S. (2020). Privacy-preserving traffic flow prediction: A federated learning approach. IEEE Internet of Things Journal, 7(8), 7751-7763.

[47] Jayaprakasam, B. S., & Thanjaivadivel, M. (2021). Cloud-enabled time-series forecasting for hospital readmissions using transformer models and attention mechanisms. International Journal of Applied Logistics and Business, 4(2), 173-180.

[48] Saha, S., & Ahmad, T. (2021). Federated transfer learning: Concept and applications. Intelligenza Artificiale, 15(1), 35-44.

[49] Dyavani, N. R., & Thanjaivadivel, M. (2021). Advanced security strategies for cloud-based e-commerce: Integrating encryption, biometrics, blockchain, and zero trust for transaction protection. Journal of Current Science, 9(3), ISSN 9726-001X.

[50] Cha, D., Sung, M., & Park, Y. R. (2021). Implementing vertical federated learning using autoencoders: Practical application, generalizability, and utility study. *JMIR medical informatics*, *9*(6), e26598.