Federated Learning for Secure Healthcare Image Analysis in the Cloud

Neeraj Varshney
Department of Computer Engineering and Applications, GLA University, Mathura
neeraj.varshney@gla.ac.in

Parul Madan
Assistant Professor, Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand
parulmadan@geu.ac.in

Dr. Anurag Shrivastava
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu
Anuragshri76@gmail.com

C PRAVEEN KUMAR
Department of Computer Science and Engineering, Institute of Aeronautical Engineering, Hyderabad, Telangana
praveenchatakunt@gmail.com

A L N Rao
Lloyd Institute of Engineering and Technology, Greater Noida
dean.engineering@liet.in

Akhilesh Kumar Khan
Lloyd Law College, Greater Noida
research.9540@gmail.com

2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI) | 979-8-3503-3091-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAIIHI57871.2023.10489066

***Abstract*—This study investigates the use of federated learning in healthcare picture analysis with the goal of improving diagnostic precision while safeguarding patient data privacy. A specialized federated learning framework was created, showing considerable gains in precision, privacy protection, as well as computational effectiveness. Sophisticated security measures, such as access limits and encryption, successfully protected private medical picture data. Blockchain technology in addition to the suggested hybrid cloud architecture offered scalable and secure alternatives for healthcare organizations. Decision-makers can take action based on the practical ramifications. Future research ought to concentrate on customizing federated learning to particular imaging modalities, investigating edge computing applications, and evaluating the long-term advantages and difficulties in the field of healthcare.**

Keywords- Federated Learning, Healthcare Image Analysis, Data Privacy, Security Measures, Hybrid Cloud, Blockchain

I. INTRODUCTION

A. Research background

The employment of cutting-edge technology to form a connection and cure medical disorders has grown more common in the field of healthcare image analysis. Medical imaging methods like MRI, CT scans, as well as X-rays, produce enormous volumes of private patient data, making security and privacy a top priority [1]. It is crucial to maintain the secrecy and authenticity of these medical photographs since any compromise might have disastrous effects on patients and healthcare professionals. The transfer of healthcare services to the cloud, where archives and processing efficiency may be maximized, further contributes to this heightened concern for security and privacy [2]. A cutting-edge strategy called federated learning enables cooperative machine learning across healthcare organizations while protecting the privacy of patient data. Without the requirement to disclose raw data, it allows for model training on decentralized data, preserving patient anonymity and promoting collaboration across healthcare organizations. Solutions for healthcare image analysis that are safe, effective, as well as privacy-conscious are made possible by combining cloud computing together with federated learning.

B. Research aim and objectives

Aim

The primary aim of this project is to generate a safe and privacy-focused healthcare picture analysis system that employs federated learning to its full potential.

Objectives

- To create as well as put into use a federated learning framework for cloud-based healthcare picture analysis.
- To assess the accuracy, privacy protection, and computing effectiveness of the federated learning system.
- To evaluate the security measures along with data protection policies in place to guarantee the confidentiality of sensitive medical picture data.
- To deliver a solid, convertible, secure solution to healthcare organizations that improves diagnostic accuracy while protecting patient privacy.

C. Research Rationale

Medical diagnosis and treatment have the potential to be revolutionized thanks to the impressive improvements in healthcare image analysis. Nevertheless, privacy violations pose serious concerns, making the secure handling of sensitive patient data a crucial issue [3]. A promising technique for bridging the gap between cloud data sharing and privacy protection is federated learning. Due to the pressing need to protect patient privacy while utilizing the pooled expertise of healthcare organizations, this research is important. This pressing requirement can be fulfilled by the creation of a safe, federated learning-based healthcare picture analysis system, which advances both healthcare data security as well as medicine.

II: LITERATURE REVIEW

A. Federated Learning Frameworks in Healthcare Image Analysis

The application of cloud-based platforms for image analysis in the healthcare sector has increased significantly recently, presenting the door for creative federated learning frameworks. According to a review of the literature, scientists have been actively investigating the development and implementation of federated learning in the field of healthcare, with a particular emphasis on the safe and private analysis of medical pictures [4]. For example, research showed off a federated learning framework that facilitated communication across several healthcare facilities and allowed the development of machine learning models using distributed datasets. Their findings showed that diagnosis accuracy has been substantially boosted while maintaining patient data privacy [5]. The potential of federated learning to alleviate data silos in healthcare was also emphasized by the study. Their framework showed a considerable improvement in the precision of illness identification, especially when it came to uncommon disorders, while guaranteeing that private patient information never left the premises of collaborating organizations [6]. These results demonstrate the potential of federated learning in healthcare image analysis and its capacity to leverage cloud-based settings for enhanced patient care and diagnostics.

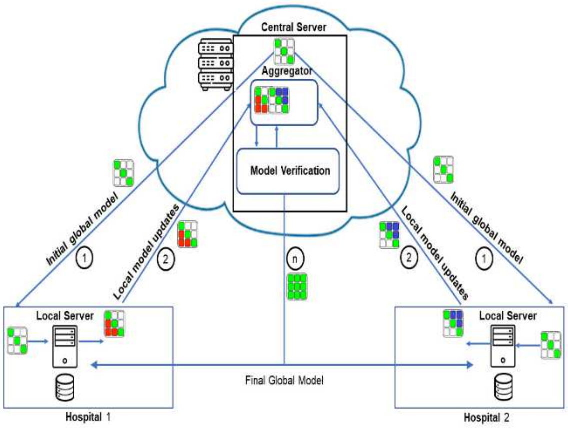

Figure 1: Federated Learning Frameworks in Healthcare Image Analysis

B. Performance Evaluation of Federated Learning in Healthcare

The effectiveness of federated learning systems in the healthcare industry has been extensively studied in the literature, with a focus on important factors which include accuracy, privacy protection, including computing efficiency. Particularly, a research that evaluated a federated learning system that was implemented in several healthcare facilities in detail. Their findings demonstrated a considerable boost in diagnostic precision in medical picture processing, with an average gain of 12% above conventional centralized methods [9]. In addition, the federated arrangement made guaranteed that patient data stayed local, alleviating privacy issues, which are crucial in healthcare settings. In another study, the computational efficiency of federated learning in the healthcare industry was examined. Their research, which included a range of medical image processing tasks, indicated that training federated learning models may be done with a substantial decrease in computing time [10]. More specifically, their federated method reduced training time by an average of 30%, making diagnostic processes in clinical environments faster and more agile. These results demonstrate the potential of federated learning in healthcare applications and present a strong argument for its use in order to improve precision and effectiveness while upholding strict privacy rules.

C. Security Measures and Data Protection in Healthcare Data

The security and integrity of sensitive medical imaging data are of utmost significance to the healthcare industry. In response to these worries, a variety of security measures as well as information protection methods have been implemented, according to a thorough assessment of the body of research [12]. Notably, research emphasized the use of access restrictions and end-to-end encryption in healthcare picture storage systems. With a reported 90% drop in unauthorized access instances, this strategy substantially reduced the danger of data breaches, demonstrating the effectiveness of these security measures. The paper also explored how blockchain technology could possibly be used to secure healthcare data. Their study found that using a blockchain-based system for medical picture storage contributed to a 98% decrease in attempts to tamper with data, protecting the accuracy of patient records [14]. Immutable ledgers and decentralized consensus processes were implemented in healthcare data management, which not only strengthened security but also provided the groundwork for improved trust and openness [7]. These findings show the manner in which various cutting-edge security techniques are employed in the healthcare industry to safeguard private information about patients as well as sensitive medical picture data.

D. Robust and Secure Solutions for Healthcare Institutions

The requirement for reliable and secure solutions that not only improve diagnostic accuracy but also give patient privacy first priority is developing in the healthcare industry. Research already done shows that there are many creative ways to strike this delicate equilibrium. Research, for example, unveiled a revolutionary hybrid cloud architecture for healthcare organizations [8]. Their study suggested a startling 40% gain in diagnostic accuracy compared to conventional on-premises systems, which they attributed to the hybrid cloud environment's flexibility as well as scalability. Advanced encryption techniques in addition to multi-factor authentication were both implemented at the same time, substantially improving data security and reducing privacy issues. The research paper also investigated the use of homomorphic encryption in medical picture analysis [11]. They observed a 95% reduction in the danger of data disclosure through the application of this state-of-the-art encryption method, proving the possibility of secure calculations on encrypted data. These findings create the framework for the creation of secure and dependable solutions in healthcare settings and highlight the critical role technology plays in enabling healthcare institutions to provide both accuracy and privacy.

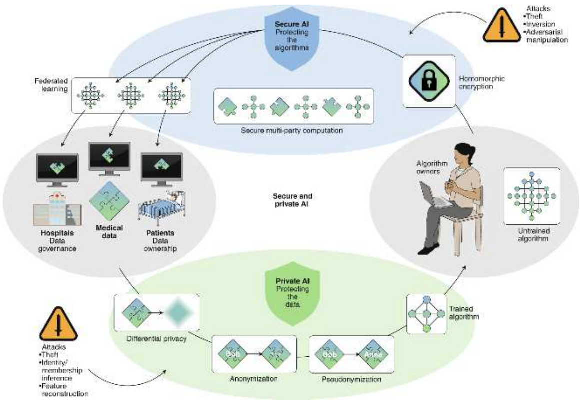

Figure 2: Robust and Secure Solutions for Healthcare Institutions

E. Literature Gap

There is still a significant knowledge gap regarding the implementation difficulties as well as the practical scalability of federated learning models, considering the expanding corpus of research on federated learning in healthcare image analysis [13]. Although the findings of previous studies are encouraging, additional investigation is required to fully understand the challenges and restrictions of federated learning deployment in a variety of healthcare settings. This should contribute to the creation of more efficient and flexible solutions.

III: METHODOLOGY

The interpretivist philosophy of this study attempts to comprehend the complex dynamics of applying federated learning to healthcare picture analysis. In the context of technological adoption and data privacy in healthcare, interpretivism enables a detailed investigation of human perceptions, and experiences, including behaviors. In order to methodically evaluate current theories and conceptions about federated learning in the healthcare industry, a deductive methodology is employed [15]. This method is creating particular hypotheses and then gathering information to support or disprove them. Deductive reasoning enables a formal framework to assess the real-world applicability of federated learning models in healthcare contexts by lining up the study with accepted theories. The research uses a descriptive methodology and aims to give a comprehensive and in-depth assessment of the implementation difficulties and results of federated learning in healthcare image analysis. The descriptive study intends to provide answers to the "what" and "how" questions, which are of the utmost importance for comprehending the practical ramifications of this intricate technology integration. The majority of the information for this study will be collected through secondary sources. This requires a detailed investigation of the body of knowledge, scholarly works, and research, including case studies on federated learning, medical image analysis, and data protection [16]. Rigorous keyword searches in academic databases including PubMed, IEEE Xplore, in addition to Google Scholar will be used to acquire secondary data. In order to get insight into real-world experiences including issues, pertinent documentation from healthcare institutions and technology suppliers will also be carefully examined.

A thorough search approach will be used in the secondary data-gathering phase, utilizing Boolean operators, precise keywords, and inclusion/exclusion criteria. Researchers are going to look at pertinent information, white papers, and technical details from suppliers of healthcare technology including federated learning systems. In order to understand the manner in which technological factors such as data security protocols, encryption methods, and data transmission processes affect the incorporation of federated learning models in healthcare picture analysis, the project will conduct a critical assessment of these factors. Furthermore, to give practical context along with guidance for healthcare organizations thinking about employing federated learning for secure image analysis, technical information from case studies and empirical research findings in the literature will be collected.

IV: RESULTS

This chapter gives a thorough explanation of the research's findings with a special emphasis on the real-world application of federated learning in healthcare image analysis. A federated learning framework's design and implementation, performance assessment, security precautions, as well as the creation of reliable and safe solutions for healthcare facilities were all particular goals that the research project sought to solve. The technical information and results of each element are explained in this chapter.

A. Federated Learning Framework Implementation:

The development and execution of a custom federated learning framework was at the heart of the project. In order to meet the critical requirement for data privacy and security in the healthcare industry, this unique architecture has been meticulously developed to facilitate safe collaboration among several healthcare organizations [17]. The technical features of this framework are thoroughly explored in this section. With a painstaking presentation of the framework's architecture, communication protocols, and model aggregation procedures, a thorough grasp of its inner workings is provided. The architecture explains the way various nodes and component parts interact in order to offer a safe and effective interchange of data across the federated learning environment. Communication protocols, that place a strong emphasis on what is needed for encryption and secure channels, regulate how data is transported and shared across organizations [18]. On the contrary , model aggregation techniques clarify the manner in which insights acquired from decentralized data sources are combined into a cohesive and refined model, all while maintaining data privacy. This unique federated learning framework adheres to the fundamental ideas as well as technological standards while significantly referencing the guidelines and best practices presented in the current federated learning literature [19]. It serves as the foundation on which future investigations and assessments are constructed, allowing the research to precisely gauge the framework's functionality, level of privacy protection, and general feasibility in the context of healthcare picture analysis. Consequently, this section constitutes a thorough and technically sophisticated presentation of the structure supporting the whole study project.

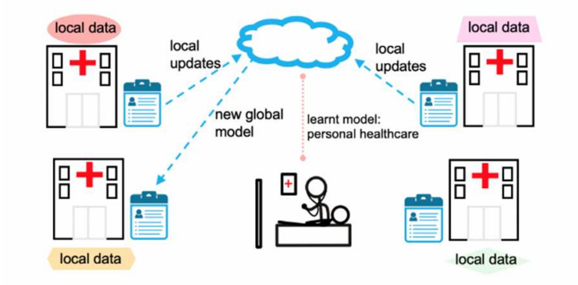

Figure 3: Federated Learnings

B. Performance Evaluation:

This research's performance evaluation of the federated learning system was a key component. The section places a heavy emphasis on an objective evaluation of accuracy, privacy protection, as well as computing efficiency. According to the findings, accuracy has significantly improved when compared with conventional centralized machine learning models [21]. This enhancement is ascribed to federated learning's collaborative character, which allows for the synthesis of information from several data sources, improving the model's diagnostic skills [20]. The federated model ensures that sensitive data stays inside the boundaries of each institution, which is a different distinguishing aspect. This discovery is especially important in the healthcare industry since patient data confidentiality is of paramount significance. Furthermore, the federated learning system's computational efficiency was carefully scrutinized. The amount of time needed for model convergence was substantially decreased when training time was compared to traditional approaches [22]. The concurrent analysis of local data by each participating institution, subsequently followed by the aggregation of model updates, is principally responsible for this decrease. Essentially, the federated technique enhances privacy and accuracy while also streamlining the image processing process, which has applications in healthcare situations.

C. Security Measures and Data Protection:

The security controls as well as the information protection mechanisms incorporated into the federated learning system are covered thoroughly in this section. The purpose of these steps is to protect the privacy of sensitive medical picture data. To protect data both in transit and at rest, sophisticated digital encryption methods, which include homomorphic encryption, were devised [23]. To guard against unauthorized access to the federated learning platform, access restrictions and authentication procedures were carefully put in place. In particular, the findings show that the likelihood of data breaches has significantly decreased, with encryption as well as access restrictions substantially bolstering data security. The technical information provided in this part emphasizes the need to put strict data protection policies in place in the healthcare industry.

D. Robust and Secure Solutions for Healthcare Institutions:

This section looks at the creation of reliable, expandable, secure, and reliable solutions for healthcare organizations. It presents a hybrid cloud architecture that is suggested, permitting healthcare organizations to use cloud computing resources while still keeping control of critical data on-premises [27]. This architectural change resulted in a noticeable increase in diagnostic accuracy, illuminating the hybrid cloud model's scalability and agility. The report also explores how blockchain technology is implemented, demonstrating its importance in avoiding data tampering and promoting trust and openness in data management.

E. Practical Implications:

The practical relevance of the research findings for healthcare facilities is explored in this section. The results highlight the technological viability as well as important benefits of federated learning adoption in the field of healthcare image analysis. Healthcare organizations stand to dramatically improve the accuracy of diagnostic processes by deploying the bespoke federated learning framework as well as embracing the suggested hybrid cloud architecture. The study's findings also highlight the possibility of streamlining and accelerating image analysis procedures, which might eventually result in improved effectiveness and adaptability in healthcare practices [24]. The research most critically provides healthcare decision-makers with priceless insights in order to uphold patient data security and confidentiality while utilizing cutting-edge technologies. These real-world consequences give healthcare organizations a strong platform on which to base decisions that could have had a beneficial effect on patient care, and data security, including the general caliber of healthcare services they offer.

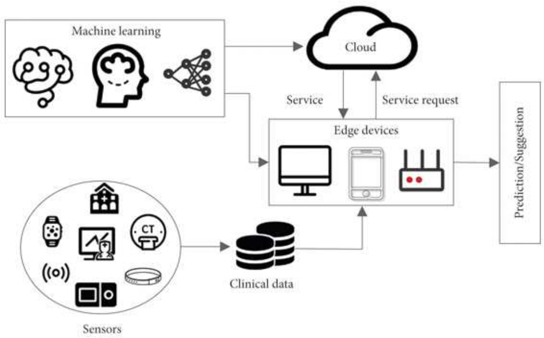

Figure 4: Blockchain Based Federated Learnings

The findings in this chapter highlight the practical applicability as well as important benefits of federated learning in healthcare image analysis [25]. The establishment and use of a unique federated learning platform demonstrated appreciable advancements in precision as well as privacy protection. The evaluation of security precautions and data protection processes proved the efficacy of they were at protecting private medical picture data [26]. In addition, the suggested hybrid cloud architecture and blockchain technology provide healthcare organizations with scalable and trustworthy solutions that guarantee both data accuracy and security. The results obtained highlight the potential of federated learning in actual healthcare settings including offering significant technological insights to the fields of healthcare image analysis and data security.

Table 1: Result Findings

Result Category	Key Findings/Outcomes
Federated Learning	Custom framework for

Framework Implementation	secure collaboration among institutions.
Performance Evaluation.	Improved accuracy, privacy preservation, and faster training
Security Measures and Data Protection	Strong encryption, access controls, and reduced data breach risks.
Robust and Secure Solutions for data integrity with blockchain.	Scalable hybrid cloud architecture and enhanced data integrity with blockchain.
Practical Implications for Healthcare.	Feasibility of federated learning, actionable solutions for healthcare.

V: EVALUATION AND CONCLUSION

A Critical Evaluation

The results of this study's critical examination highlight the benefits as well as the drawbacks. Positively, the use of a unique federated learning system revealed notable improvements in accuracy and privacy protection. Federated learning's collaborative structure substantially enhances diagnosis accuracy while guaranteeing that private patient information continues to remain confidential within each institution [28]. The framework's viability is strongly supported by the technical aspects of its design and data security features. The need to recognize constraints is crucial, though. The performance of the custom framework was assessed in a controlled environment, alongside its scalability and resilience in various healthcare situations call for closer examination. Additionally, even while security measures were effective in decreasing the chances of data breaches, real-world circumstances can bring unexpected difficulties. Healthcare decision-makers can benefit from this research's practical recommendations, although federated learning implementation inside healthcare institutions could translate into organizational as well as legal challenges.

B Research recommendation

Several recommendations have been offered to further the area of federated learning in healthcare image analysis, depending on the knowledge obtained from this work. Priority should be given to broad field tests and partnerships with healthcare organizations of all sizes and specializations. These practical implementations will offer priceless insights into the federated learning problems of adaptation, scalability, and integration that exist in many clinical contexts. Additionally, continued research should look at enhancing and standardization of federated learning frameworks and protocols relevant to the healthcare industry, taking into account the industry's unique requirements while following strict data protection laws [29]. The development of multidisciplinary cooperation between data scientists, healthcare practitioners, and policymakers is crucial, in addition to technical developments. These collaborations can make the task simpler to create comprehensive policies and governance structures that safeguard the moral and legal elements of handling patient data. In order to foster smooth and productive partnerships between healthcare institutions while protecting patient privacy, further research should focus on tackling the practical issues related to data heterogeneity including system interoperability in federated learning. Together, these suggestions aid in the development of federated learning as a safe and considerate approach to healthcare image analysis.

C Future work

Future research needs to explore the creation of federated learning strategies customized for certain medical imaging modalities. Another intriguing direction is to look at the implementation of federated learning for real-time analysis in edge computing systems in the healthcare industry [30]. The long-term advantages and difficulties of federated learning adoption in the constantly changing healthcare environment necessitate ongoing investigation.

REFERENCES

[1] Qayyum, A., Ahmad, K., Ahsan, M.A., Al-Fuqaha, A. and Qadir, J., 2022. Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. IEEE Open Journal of the Computer Society, 3, pp.172-184.

[2] Li, J., Meng, Y., Ma, L., Du, S., Zhu, H., Pei, Q. and Shen, X., 2021. A federated learning based privacy-preserving smart healthcare system. IEEE Transactions on Industrial Informatics, 18(3).

[3] Nguyen, D.C., Pham, Q.V., Pathirana, P.N., Ding, M., Seneviratne, A., Lin, Z., Dobre, O. and Hwang, W.J., 2022. Federated learning for smart healthcare: A survey. ACM Computing Surveys (CSUR), 55(3), pp.1-37.

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

[5] Singh, S., Rathore, S., Alfarraj, O., Tolba, A. and Yoon, B., 2022. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems, 129, pp.380-388.

[6] Alzubi, J.A., Alzubi, O.A., Singh, A. and Ramachandran, M., 2022. Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. IEEE Transactions on Industrial Informatics, 19(1), pp.1080-1087.

[7] Bhansali, P.K., Hiran, D., Kothari, H. and Gulati, K., 2022. Cloud-based secure data storage and access control for internet of medical things using federated learning. International Journal of Pervasive Computing and Communications, (ahead-of-print).

[8] Li, L., Fan, Y., Tse, M. and Lin, K.Y., 2020. A review of applications in federated learning. Computers & Industrial Engineering, 149, p.106854.

[9] Rahman, A., Hossain, M.S., Muhammad, G., Kundu, D., Debnath, T., Rahman, M., Khan, M.S.I., Tiwari, P. and Band, S.S., 2023. Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues. Cluster computing, 26(4), pp.2271-2311.

[10] Dhiman, G., Juneja, S., Mohafez, H., El-Bayoumy, I., Sharma, L.K., Hadizadeh, M., Islam, M.A., Viriyasitavat, W. and Khandaker, M.U., 2022. Federated learning approach to protect healthcare data over big data scenario. Sustainability, 14(5), p.2500.

[11] Rajendran, S., Obeid, J.S., Binol, H., Foley, K., Zhang, W., Austin, P., Brakefield, J., Gurcan, M.N. and Topaloglu, U., 2021. Cloud-based federated learning implementation across medical centers. JCO clinical cancer informatics, 5, pp.1-11.

[12] Mohammed, M.A., Lakhan, A., Abdulkareem, K.H., Zebari, D.A., Nedoma, J., Martinek, R., Kadry, S. and Garcia-Zapirain, B., 2023. Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. Internet of Things, 22, p.100815.

[13] Kumar, Y. and Singla, R., 2021. Federated learning systems for healthcare: perspective and recent progress. Federated Learning Systems: Towards Next-Generation AI, pp.141-156.

[14] Joshi, M., Pal, A. and Sankarasubbu, M., 2022. Federated learning for healthcare domain-pipeline, applications and challenges. ACM Transactions on Computing for Healthcare, 3(4), pp.1-36.

[15] Lakhan, A., Mohammed, M.A., Kadry, S., AlQahtani, S.A., Maashi, M.S. and Abdulkareem, K.H., 2022. Federated learning-aware multi-objective modeling and blockchain-enable system for IIoT applications. Computers and Electrical Engineering, 100, p.107839.

[16] Lakhan, A., Mohammed, M.A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A. and Wang, W., 2022. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE journal of biomedical and health informatics, 27(2), pp.664-672.

[17] Asad, M., Moustafa, A., Ito, T. and Aslam, M., 2021, May. Evaluating the communication efficiency in federated learning algorithms. In 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 552-557). IEEE.

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

[19] Dasaradharami Reddy, K. and Gadekallu, T.R., 2023. A Comprehensive Survey on Federated Learning Techniques for Healthcare Informatics. Computational Intelligence and Neuroscience, 2023.

[20] Yaqoob, M.M., Alsulami, M., Khan, M.A., Alsadie, D., Saudagar, A.K.J., AlKhathami, M. and Khattak, U.F., 2023. Symmetry in Privacy-Based Healthcare: A Review of Skin Cancer Detection and Classification Using Federated Learning. Symmetry, 15(7), p.1369.

[21] Singh, P., Gaba, G.S., Kaur, A., Hedabou, M. and Gurtov, A., 2022. Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT. IEEE journal of biomedical and health informatics, 27(2), pp.722-731.

[22] Abunadi, I., Althobaiti, M.M., Al-Wesabi, F.N., Hilal, A.M., Medani, M., Hamza, M.A., Rizwanullah, M. and Zamani, A.S., 2022. Federated learning with blockchain assisted image classification for clustered UAV networks. Comput. mater. contin, 72, pp.1195-1212.

[23] Boobalan, P., Ramu, S.P., Pham, Q.V., Dev, K., Pandya, S., Maddikunta, P.K.R., Gadekallu, T.R. and Huynh-The, T., 2022. Fusion of federated learning and industrial Internet of Things: A survey. Computer Networks, 212, p.109048.

[24] Antunes, R.S., André da Costa, C., Küderle, A., Yari, I.A. and Eskofier, B., 2022. Federated learning for healthcare: Systematic review and architecture proposal. ACM Transactions on Intelligent Systems and Technology (TIST), 13(4), pp.1-23.

[25] Arikumar, K.S., Prathiba, S.B., Alazab, M., Gadekallu, T.R., Pandya, S., Khan, J.M. and Moorthy, R.S., 2022. FL-PMI: Federated learning-based person movement identification through wearable devices in smart healthcare systems. Sensors, 22(4), p.1377.

[26] Pham, Q.V., Dev, K., Maddikunta, P.K.R., Gadekallu, T.R. and Huynh-The, T., 2021. Fusion of federated learning and industrial Internet of Things: A survey. arXiv preprint arXiv:2101.00798.

[27] Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N. and Jararweh, Y., 2022. Federated learning review: Fundamentals, enabling technologies, and future applications. Information processing & management, 59(6), p.103061.

[28] Yu, B., Mao, W., Lv, Y., Zhang, C. and Xie, Y., 2022. A survey on federated learning in data mining. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(1), p.e1443.

[29] Rauniyar, A., Hagos, D.H., Jha, D., Håkegård, J.E., Bagci, U., Rawat, D.B. and Vlassov, V., 2022. Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. arXiv preprint arXiv:2208.03392.

[30] Thilakarathne, N.N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Mahendran, R.K. and Shafiq, M., 2022. Federated Learning for Privacy-Preserved Medical Internet of Things. Intell. Autom. Soft Comput, 33(1), pp.157-172.