Communication-Efficient and Privacy-Preserving Edge-Cloud Framework For Smart Healthcare

Armando B. Mpembele
Department of Computer Science
Tennessee State University
Nashville, TN 37209 USA
ampembel@tnstate.edu

Tamara Rogers
Department of Computer Science
Tennessee State University
Nashville, TN 37209 USA
trogers@tnstate.edu

Uttam Ghosh
Department of Computer Science and Data Science
Meharry Medical College
Nashville, TN 37203 USA
ghosh.uttam@ieee.org

Sachin Shetty
Electrical Engineering Department
Old Dominion University
Norfolk, VA 23529, USA
sshetty@odu.edu

2023 IEEE Globecom Workshops (GC Wkshps) | 979-8-3503-7021-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/GCWKSHPS58843.2023.10464501

***Abstract*—The healthcare industry has experienced a remarkable digital transformation through the adoption of IoT technologies, resulting in a significant increase in the volume and variety of medical data generated. Challenges in processing, analyzing, and sharing healthcare data persist. Traditional cloud computing approaches, while useful for processing healthcare data, have drawbacks, including delays in data transfer, data privacy concerns, and the risk of data unavailability. In this paper, we propose a software-defined 5G and AI-enabled distributed edge-cloud collaboration platform to classify healthcare data at the edge devices, facilitate real-time service delivery, and create AI/ML-based models for identifying patients' potential medical conditions. In our architecture, we have incorporated a federated learning scheme based on homomorphic encryption to provide privacy in data sharing and processing. The proposed framework ensures secure and efficient data communication and processing, ultimately fostering effective collaboration among healthcare institutions. The models will be validated by performing a comparative time analysis, and the interplay between edge and cloud computing will be investigated to support real-time healthcare applications.**

***Index Terms*—Cloud Computing, Edge Computing, Federated Learning, 5G SDN, Healthcare, IoT, Privacy**

I. Introduction

The rapid advancement of technology, particularly Internet of Things (IoT), has transformed the healthcare industry by enabling real-time patient monitoring and remote medical support. Wearable medical IoT devices allow doctors to collect medical data from patients through smartphone applications, enabling remote medical treatment. The modernization of smart devices, wireless communication, and computational facilities have significantly improved the efficiency, accuracy, and accessibility of healthcare data management, leading to better patient outcomes and an overall enhancement of the healthcare system. More than 100-million people are using wearable medical devices globally as estimated in [1]. Forbes predicted that the compound annual growth rate of data for healthcare would reach 36% of the world's data volume by 2025 [2], which is faster than other industries, including media and entertainment, manufacturing, and financial services.

However, the continuous use of medical IoT devices and applications generates vast and diverse data artifacts that require efficient processing and analysis to deliver high-quality care. Traditional cloud computing approaches used for healthcare data processing have drawbacks, including delays in data transfer, data privacy concerns, and the risk of data unavailability due to system failures. Effective data sharing among healthcare institutions faces challenges due to geographical dispersion, different ethical rules and data sharing regulations, and the risks of data breaches. These factors result in isolated data islands that hinder the development of the healthcare industry. To overcome these challenges, a secure framework is needed to enable healthcare institutions to share data while preserving data privacy.

In this paper, we propose to develop an edge-cloud collaboration platform that enhances efficient data communication and processing for intelligent medical systems. Leveraging software-defined 5G [3] and AI-enabled distributed edge-cloud technologies [4], [5], the proposed platform ensures the secure management and availability of critical healthcare data. The approach involves an SDN-driven architecture that classifies healthcare data at edge devices, facilitates real-time service delivery, and creates models based on AI/ML algorithms to identify potential medical conditions in patients. It also utilizes homomorphic encryption [6] with federated learning to provide privacy without disclosing the raw and sensitive health data [7]. The proposed platform ensures secure and efficient data communication and processing, thereby fostering effective collaboration among different healthcare institutions and ultimately enhancing the overall quality of patient care.

979-8-3503-7021-8/23/$31.00 ©2023 IEEE

The rest of this paper is organized as follows: In Section II, we provide a literature review on federated learning, 5G networking, cloud computing, edge computing, SDN (Software Defined Networking), IoT (Internet of Things), AI (Artificial Intelligence), and data privacy in healthcare applications. Section III provides a detailed description of the proposed framework for communication-efficient and privacy-preserving healthcare data sharing and processing. Section IV introduces the concepts of 5G and SDN. In Section V, we elaborate on how data privacy is ensured through federated learning. Lastly, in Section VI, we conclude the paper and provide a direction for future work.

II. Related Works

The Internet of Things has transformed the healthcare industry by enabling real-time patient monitoring and remote medical support. Several studies have investigated the potential of IoT in healthcare applications such as remote patient monitoring, telehealth, and robotic surgeries. Here is an example: The work proposed in [8] provides a comprehensive overview of IoT, including its application in healthcare.

Cloud computing has also been extensively used in healthcare for data storage, processing, and analysis. Several works have highlighted the benefits and challenges associated with using cloud computing in healthcare, particularly with respect to data privacy, security, and latency. These studies have laid the groundwork for understanding the limitations of cloud computing in handling the vast and diverse data generated by IoT devices and applications in healthcare. The authors in [9] discuss the potential benefits and challenges of using cloud computing in healthcare services, including data storage, processing, and analysis. The work proposed in [10] discusses the opportunities, challenges, and innovations in using cloud computing for healthcare services, with a focus on data privacy, security, and latency.

To overcome the limitations of cloud computing, researchers have explored edge computing and 5G networking as promising solutions for efficient data communication and processing in healthcare applications. These works have demonstrated the potential of edge computing and 5G networks in reducing latency, improving data privacy and security, and enhancing the overall performance of healthcare systems. The authors in [11] present a comprehensive study that explores the role of 5G, edge computing, and IoT in healthcare. This study also analyses the use of cutting-edge artificial intelligence-based classification and prediction techniques employed for edge intelligence. The work presented in [12] proposes an edge computing framework for IoT based healthcare services, focusing on efficient data communication and processing, as well as addressing the limitations of cloud computing in healthcare applications.

In addition, SDN-driven architectures have been proposed as a means to efficiently manage healthcare data and deliver real-time services in intelligent medical systems. These studies have examined the potential of SDN in enabling better network management, resource allocation, and service delivery in healthcare applications. The authors in [13] propose an SDN-based multi-tier computing and communication architecture composed of end-user devices, edge servers, and legacy cloud data-center for pervasive healthcare. The work presented in [14] proposes a novel on-demand e-Healthcare dynamic network slice architecture that uses the machine learning algorithms at the edge server for real-time classification and access of the offloaded data from the central SDN controller. The authors in [15] present a smart healthcare framework that uses SDN-based slicing backup algorithm for leveraging deep learning neural network to orchestrate network latency and load efficiently. The work presented in [16] proposes a load-balancing mechanism based on SDN-SFC for the optimization of hospital remote-monitoring network planning to eliminate the need for large amounts of hardware.

Moreover, AI and machine learning algorithms have been widely used in healthcare for identifying potential medical conditions and improving the quality of care provided to patients. Several works have explored the development and validation of AI/ML-based models for various healthcare applications, including diagnostics, treatment planning, and personalized medicine. The authors in [17] demonstrate the use of deep neural networks for classifying skin cancer, achieving dermatologist-level performance in diagnostics, showing the potential of AI in improving the quality of care.

Finally, federated learning has emerged as a promising technique for preserving privacy in healthcare data sharing and processing. The work presented in [18] introduce the concept of fully homomorphic encryption, offering a potential solution for preserving data privacy and security in healthcare. The work in [19] discusses the system design of federated learning, ensuring data privacy and security in healthcare applications.

The existing literature provides insights into the various aspects of IoT, cloud computing, edge computing, 5G networking, SDN, AI, and data privacy in healthcare applications. However, there remains a need for a comprehensive edge-cloud collaboration platform that addresses the limitations of traditional approaches while ensuring efficient data communication, processing, and privacy in intelligent medical systems [20]. This paper aims to build upon the existing body of knowledge and develop a novel platform that leverages software-defined 5G, AI-enabled distributed edge-cloud technologies, and federated learning to overcome the challenges faced in healthcare data sharing and processing.

III. Proposed Framework

In this section, we discuss the architecture of our proposed framework. It aims to address existing challenges in sharing and processing big data among healthcare institutions, particularly focusing on data privacy preservation and efficient data communication. Figure 1 shows the architecture of our proposed framework, which comprises three layers: the infrastructure and IoT-devices layer, the edge computing layer, and the cloud computing layer. Each of these layers

plays a crucial role in the overall system, and they will be discussed in detail in the subsequent subsections.

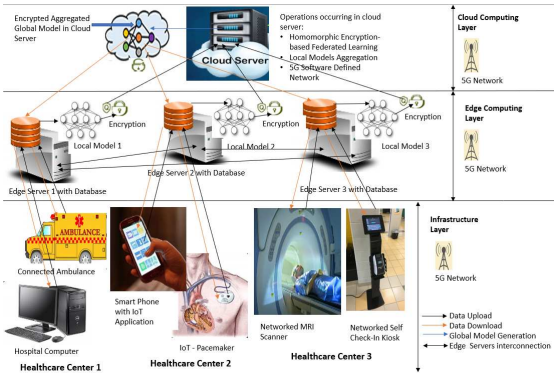

Fig. 1. Architecture for Communication-Efficient and Privacy-Preserving Edge-Cloud Framework For Smart Healthcare

A. Infrastructure and IoT-devices Layer

This layer encompasses all the networked and IoT devices utilized in the participating healthcare institutions. These devices include, but are not limited to, desktop computers, intelligent medical transportation systems, smart pacemakers, smart insulin pumps, smartphones, intelligent surgery robots, networked imaging scanners, embedded systems, hospital self-check-in stations, and more. These devices play a crucial role in both generating and consuming data within the healthcare ecosystem.

The infrastructure and IoT devices within this layer generate a vast array of data artifacts, each with its own unique characteristics. These data artifacts are then directed to the edge server, where they undergo processing and storage. By means of an application programming interface (API), the infrastructure devices are able to retrieve the processed data from the edge server and conduct further data analysis.

B. Edge Computing Layer

In the proposed framework, we leverage edge computing to address the challenges associated with centralized cloud computing by bringing data storage, computing, and processing closer to the devices that generate and consume the data. This is achieved by deploying intelligent edge servers at each participating healthcare center. By performing computations locally, edge computing offers several advantages over traditional cloud computing:

1) Latency: Edge computing significantly reduces the time taken for data to travel between the data source and the processing unit.
2) Bandwidth: Local processing at the edge server increases the network bandwidth, thus preventing network congestion.
3) Privacy and security: Edge computing enhances data privacy and security by processing sensitive data locally instead of sending it to a centralized data center.
4) Scalability and resilience: The edge servers are interconnected in a full mesh topology. This distributed architecture prevents single points of failure and ensures system continuity, even in the presence of compromised or disconnected nodes.

C. Cloud Computing Layer

Within this layer, cloud computing is utilized through the utilization of a centralized cloud server. This server plays a crucial role in coordinating the heavy computing tasks associated with federated learning. One advantage of employing cloud computing is the ability to leverage its vast data storage capabilities. In contemporary times, elastic cloud services allow for dynamic increases in data storage capacity on an as-needed basis.

Moreover, the centralized cloud server serves as a platform for harnessing the power of software-defined 5G and AI-enabled distributed edge-cloud technologies. These advancements ensure the secure management and responsive availability of critical healthcare data. Additionally, the cloud server assumes the role of the control center for the entire architecture. Within this layer, other network functions, such as NFV (Network Function Virtualization) and SDN (Software-Defined Networking), can be deployed in conjunction with 5G technology, facilitating the implementation of network slicing.

IV. 5G Network

The emergence of 5G network technology represents the latest generation of mobile communication networks, revolutionizing various industries such as autonomous vehicles, remote surgery, smart cities, and immersive entertainment experiences. It comprises several key components, including the Radio Access Network (RAN), Massive MIMO technology, 5G New Radio (NR), Core Network, Network Slicing, Edge Computing, Backhaul and Fronthaul, and Device Support. Together, these components collaborate to provide notable benefits such as faster data speeds, reduced latency, increased capacity, and enhanced reliability.

The 5G Core, a central part of the 5G network, serves as the hub for managing and orchestrating various network functions, such as NFV and SDN. It plays an important role in enabling advanced features and capabilities within 5G networks, such as ultra-low latency communication, network slicing, and edge computing. These advancements are instrumental in supporting a wide range of new applications and services across diverse industries.

Within the healthcare industry, a vast amount of data is generated by devices and applications. To ensure efficient and reliable communication, it is essential to address potential issues related to high latency and data bottlenecks. To overcome these challenges, our architecture leverages 5G network and communication technology. This approach ensures ubiquitous connectivity, supporting a high number of connected devices with various services. Additionally, it offers very high-speed connections, enabling faster data

transmission, and provides extremely low latency, supporting real-time data transmission and reception.

V. Privacy Preservation

PP Federated learning proceeds as follows: Assuming there are *N* clients participating, each client trains a local model using the data contained in its dataset through several iterations with the stochastic gradient descent (SGD) algorithm. Once this task is complete, the client uploads its local model to the server, which then aggregates all the local models submitted by *N* clients and generates a global model using the weighted average algorithm. Subsequently, the global model is distributed to each participating client *i* for further training until the model converges. This means, given the aggregation weight W_i for the client *i*, where $i \in N$, the global model M_{global} is calculated by summing the weighted local models, as shown in Equation (1).

$$M_{global} = \sum_{i=1}^{N} W_i M_i \quad (1)$$

Federated learning is proven to be an efficient technique for sharing and processing data among multiple healthcare institutions [21]. However, some existing federated learning schemes overlook privacy preservation [22], [23], while others rely on homomorphic encryption schemes to address data security and privacy concerns [7], [24]. Nevertheless, some of these privacy-preserving federated learning schemes have limitations, such as clients' dropout [24], [25].

A. Proposed Scheme

Motivated by the work of Zhang et al. [7], we proposed a federated learning scheme with related concepts. This scheme combines various cryptographic primitives, including the homomorphic encryption scheme [6], the Shamir secret sharing algorithm [26], and the Diffie-Hellman key exchange [27], to ensure both privacy and security. It also tackles the challenge of clients' dropout.

We have incorporated this scheme in our architecture to provide privacy in data sharing and processing. Our architecture consists of a model aggregation server located in the cloud and distributed clients, which represent healthcare institutions with substantial raw healthcare data stored in their edge servers. The responsibility of the clients is to train local models on their respective healthcare datasets, then submit only the encrypted local models along with their relevant encrypted data quality values to the server, which then securely aggregates them to generate the global model. Finally, each client downloads the global model from the cloud server and continues with iterative training until its local model converges.

During training, each client keeps its dataset private and does not share it with the server. Clients may attempt to infer sensitive raw data from the other clients; however, they are unable to learn the models of the other clients. While our scheme specifically focuses on resisting passive collusion attacks, deliberate attacks on model training are not taken into consideration.

B. Clients Contribution Weight Computation

In many cases, model aggregation is performed based on data size, resulting in all clients contributing to the global model training with the same weight, which can impact model accuracy. To address this challenge, our federated learning scheme considers the data quality in the submitted local models to determine their contribution weight. This technique enables effective collaboration in federated learning, as clients with higher data quality make more substantial contributions to the global model, resulting in improved accuracy and convergence.

Our scheme incorporates the use of the truth discovery algorithm and SGD algorithm to calculate the data quality to determine the weight of each client in the global model. Past works, such as [28] and [29], have utilized the truth discovery algorithm in crowd sensing systems to assess the reliability of data sources by comparing observed values to true values. This algorithm has demonstrated effectiveness in evaluating the quality of heterogeneous data.

Furthermore, [30] leveraged the local gradient amplitude in the SGD algorithm to measure the proportion of the local model in the global model. However, the gradient amplitude primarily reflects the convergence speed and can be influenced by factors such as dataset size and learning rate. As in Zhang et al. [7], to address these limitations, our scheme employs the truth discovery algorithm to calculate the distance between the local gradient and the global gradient in each training epoch. This approach provides a more comprehensive measure of the contribution of local models.

The SGD provides a method for obtaining the global gradient through two global models trained in two adjacent epochs. Let G^t_{global} represent the global gradient in the *t-th* epoch, M^t_{global} represent the global model in the *t-th* epoch, and M^{t+1}_{global} represent the global model in the *(t + 1)-th* epoch. The global gradient can be obtained using Equation (2), where β represents the training rate. This gradient is essential for updating the global model and facilitating the convergence of the federated learning process.

$$G^t_{global} = \frac{M^t_{global} - M^{t+1}_{global}}{\beta} \quad (2)$$

Our scheme leverages the gradients to derive the data quality parameter. This involves calculating the distance between the local and global gradients. Let G^t_i represent the local gradient in the *t-th* epoch, G^{t-1}_{global} represent the global gradient in the *(t-1)*th epoch, the data quality K^t_i in the *t-th* epoch, can be obtained using Equation (3), where γ represents a scaling coefficient.

$$K^t_i = \frac{\gamma}{\|G^t_i - G^{t-1}_{global}\|_2} \quad (3)$$

In our approach, we utilize the global gradient from the previous epoch, G^{t-1}_{global} in the *(t - 1)-th* epoch, to calculate

the data quality K_i^t in the current (*t-th*) epoch, as depicted in Equation (3). The calculation incorporates a scaling coefficient, γ, which is determined based on the Chi-squared distribution, denoted as χ^2. This coefficient is obtained by evaluating the significance level α and the dimension of the gradient vector, represented as $|d|$. Importantly, γ=χ^2(1-α/2, $|d|$) can be considered a public parameter, given the known values of α and $|d|$ [31]. Incorporating γ enables us to assess and utilize the data quality in the federated learning process accurately.

When the data quality value is known, the weighted average algorithm performs well. Given the data quality K_i^t and the local model M_i^t of each client *i* in the *t*-th epoch, the global model M_{global}^t in the *t*-th epoch can be obtained using Equation (4), where *N* represents the number of clients participating in the federated learning process.

$$M_{global}^t = \frac{\sum_{i=1}^{N} K_i^t M_i^t}{\sum_{i=1}^{N} K_i^t} \quad (4)$$

From Equation (4), we can deduce that the clients with higher data quality contribute more to the global model.

C. Secure Aggregation Process

In this section, we show how homomorphic encryption techniques are used to mask the local models and their data quality values in order to provide privacy in federated learning . The following four parts outline the process.

1) System Initialization: Before the federated learning starts, the cloud server confirms the clients that will take part in the training and the neural network model, such as deep neural network (DNN) or convolutional neural network (CNN). At the same time, it sets the learning rate β, the maximum number of epochs *E* for training convergence, the initial global model M_{global}^0, and the threshold *e* in the Shamir secret sharing algorithm, which sets the maximum number of clients that can either dropout or maliciously collude during the training. After this, some secure parameters and pairwise keys are generated to assure privacy and security.
2) Local Model Masking: Once all the participating clients receive the information above, the federated learning process starts. Each client starts to train their local model M_i^t, then computes the data quality value K_i^t. For privacy preservation, some encrypted data need to be shared among all clients to safeguard their local models from eavesdropping by any potential malicious entities. Furthermore, all local models and their associated data quality values are masked (encrypted) before being uploaded to the server. The local model masking process is completed first, then the encryption process of the data quality follows, utilizing the enhanced ElGamal homomorphic encryption algorithm proposed by Zhang et al. [7].
3) Local Models Aggregation: The server starts to aggregate the masked models once it receives the masked models and the ciphertexts of the data quality from at least *e* clients. Sometimes, there are clients that drop out during the masked model upload process. In such an event, the server aggregates the masked models submitted by the active clients.
4) Global Model Generation: The process of decrypting the aggregate ciphertext of data quality is performed utilizing the enhanced ElGamal homomorphic encryption algorithm. Lastly, knowing the total data quality value $\sum_{i\in\mathcal{P}_3} K_i^t$ of online clients, the value of all aggregated masked local models $\omega = \phi \sum_{i\in\mathcal{P}_3} K_i^t + \sum_{i\in\mathcal{P}_3} M_i^t K_i^t$, and the scale factor ϕ, the server can generate the global model by aggregating the local models of the active clients, as per Equation (5)

$$M_{global}^t = \frac{\omega - \phi \sum_{i\in\mathcal{P}_3} K_i^t}{\sum_{i\in\mathcal{P}_3} K_i^t} = \frac{\sum_{i\in\mathcal{P}_3} M_i^t K_i^t}{\sum_{i\in\mathcal{P}_3} K_i^t} \quad (5)$$

D. Proposed Scheme Security Analysis

The purpose of masking the models is to protect them so that no adversary can snoop on them. This is performed by adding a random number to the real inputs. In this way , the masked result becomes unpredictable. The adversary may see the sum of the real inputs but they will be unable to tell the individual real input of every client because it is hidden.

We consider two cases for analysis purpose:

1) Case 1: Inter Clients Collusion: Let $C_{collude}$ denote the set of clients participating in collusion, *Server* denote the cloud server, and *e* the threshold set according to the Shamir secret sharing algorithm [26]. Let us consider that the server is honest and does not temper with the data and that the cardinality of $C_{collude}$ is less than *e*. Assume there is an adversary *Advers* that wants to break the masking scheme with the assistance of $C_{collude}$. All the information that *Advers* can see is equal to the data that $C_{collude}$ possesses. *Advers* cannot see the data of the honest clients.
2) Case 2: Server-Clients Collusion: Here again, let us consider that the server is honest and does not temper with the data. Assume there is an adversary *Advers* that wants to break the masking scheme with the assistance of $C_{collude}$. Once again, all the information that *Advers* can see is equal to the sum of data that the colluding clients possess because *Advers* cannot see the data of the honest clients.

In both cases, it is demonstrated that the information that an adversary can view is limited to what the colluding clients can see. The masking scheme is secure against collusion as long as the number of colluding clients remains below the threshold *e*. Therefore, the masking scheme is secure.

VI. Conclusion

In this paper, we have proposed a comprehensive framework for healthcare data sharing and processing, centered

around an edge-cloud collaboration platform. The platform utilizes software-defined 5G and AI-enabled distributed edge-cloud technologies to facilitate efficient data communication for smart healthcare systems. Motivated by Zhang et al., we incorporated a related federated learning scheme in our framework to provide privacy in data sharing and processing in IoT-based healthcare applications.

Future work will involve refining and validating the proposed models, exploring the interplay between edge and cloud computing, and identifying additional applications and use cases for the developed platform. While federated learning offers promising benefits in terms of privacy preservation and collaborative model training, it also presents its own set of challenges, especially when dealing with high-dimensional data in sensitive domains such as healthcare. By addressing these challenges, we can further unlock the full potential of federated learning in advancing collaborative, efficient, secure and privacy-preserving, and patient-centric healthcare system.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation, under award number 2219741.

REFERENCES

[1] T. Murallie, "5 edge computing use cases in the healthcare industry." https://www.the-analytics.club/edge-computing-in-healthcare. Online; accessed 29 November 2022.

[2] N. Culbertson, "The skyrocketing volume of healthcare data makes privacy imperative." https://www.forbes.com/sites/forbestechcouncil/2021/08/06/the-skyrocketing-volume-of-healthcare-data-makes-privacy-imperative/?sh=3944f606555c. Online; accessed 30 November 2022.

[3] D. Basu, S. Kal, U. Ghosh, and R. Datta, "Drive: Dynamic resource introspection and vnf embedding for 5g using machine learning," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18971–18979, 2023.

[4] U. Ghosh, D. Das, P. Chatterjee, and N. Shillingford, "Federated edge-cloud framework for heart disease risk prediction using blockchain," in *Internet of Things. Advances in Information and Communication Technology* (D. Puthal, S. Mohanty, and B.-Y. Choi, eds.), (Cham), pp. 309–329, Springer Nature Switzerland, 2024.

[5] A. Makkar, U. Ghosh, and P. K. Sharma, "Artificial intelligence and edge computing-enabled web spam detection for next generation iot applications," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25352–25361, 2021.

[6] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[7] L. Zhang, J. Xu, P. Vijayakumar, P. K. Sharma, and U. Ghosh, "Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system," *IEEE Transactions on Network Science and Engineering*, pp. 1–17, 2022.

[8] K. K. Patel and S. M. Patel, "Internet of things-iot: Definition, characteristics, architecture, enabling technologies, application & future challenges," 2016.

[9] K. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *Journal of Medical Internet Research*, vol. 13, no. 3, 2011.

[10] R. Sultan, "Cloud computing for health care: Opportunities, challenges, and innovations," *International Journal of E-Health and Medical Communications*, vol. 10, no. 3, pp. 1–15, 2019.

[11] S. U. Amin and M. S. Hossain, "Edge intelligence and internet of things in healthcare: A survey," *IEEE Access*, vol. 9, pp. 45–59, 2021.

[12] V. Singh Rohila, N. Gupta, A. Kaul, and U. Ghosh, "Towards framework for edge computing assisted covid-19 detection using ct-scan images," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6, 2021.

[13] A. C. Baktir, C. Tunca, A. Ozgovde, G. Salur, and C. Ersoy, "Sdn-based multi-tier computing and communication architecture for pervasive healthcare," *IEEE Access*, vol. 6, pp. 56765–56781, 2018.

[14] D. Basu, V. Krishnakumar, U. Ghosh, and R. Datta, "Softhealth: Softwarized 5g-driven network slicing for real-time e-healthcare applications using ml," in *2022 14th International Conference on COMmunication Systems NETworkS (COMSNETS)*, pp. 222–226, 2022.

[15] D. Basu, V. Krishnakumar, U. Ghosh, and R. Datta, "Deepcare: Deep learning-based smart healthcare framework using 5g assisted network slicing," in *2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 201–206, 2022.

[16] T.-M. Li, C.-C. Liao, H.-H. Cho, W.-C. Chien, C. F. Lai, and H.-C. Chao, "An e-healthcare sensor network load-balancing scheme using sdn-sfc," in *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–4, 2017.

[17] A. Esteva, B. Kuprel, R. A. Novoa, J. Ko, S. M. Swetter, H. M. Blau, and S. Thrun, "Dermatologist-level classification of skin cancer with deep neural networks," *nature*, vol. 542, no. 7639, pp. 115–118, 2017.

[18] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, (New York, NY, USA), p. 169–178, Association for Computing Machinery, 2009.

[19] K. A. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. M. Kiddon, J. Konečný, S. Mazzocchi, B. McMahan, T. V. Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards federated learning at scale: System design," in *SysML 2019*, 2019.

[20] Z. Min, R. E. Canady, U. Ghosh, A. S. Gokhale, and A. Hakiri, "Tools and techniques for privacy-aware, edge-centric distributed deep learning," in *Proceedings of the Workshop on Distributed Infrastructures for Deep Learning*, DIDL'20, (New York, NY, USA), p. 7–12, Association for Computing Machinery, 2021.

[21] M. J. Sheller, B. Edwards, G. A. Reina, J. Martin, S. Pati, A. Kotrotsou, M. Milchenko, W. Xu, D. Marcus, R. R. Colen, *et al.*, "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data," *Scientific reports*, vol. 10, no. 1, p. 12598, 2020.

[22] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *International Conference on Artificial Intelligence and Statistics*, 2016.

[23] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," CCS '17, (New York, NY, USA), p. 1175–1191, ACM, 2017.

[24] C. Fang, Y. Guo, N. Wang, and A. Ju, "Highly efficient federated learning with strong privacy preservation in cloud computing," *Computers Security*, vol. 96, p. 101889, 2020.

[25] M. Asad, A. Moustafa, and T. Ito, "Fedopt: Towards communication efficiency and privacy preservation in federated learning," *Applied Sciences*, vol. 10, no. 8, 2020.

[26] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, p. 612–613, nov 1979.

[27] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[28] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, and K. Ren, "Privacy-preserving truth discovery in crowd sensing systems," *ACM Trans. Sen. Netw.*, vol. 15, jan 2019.

[29] G. Xu, H. Li, C. Tan, D. Liu, Y. Dai, and K. Yang, "Achieving efficient and privacy-preserving truth discovery in crowd sensing systems," *Computers & Security*, vol. 69, pp. 114–126, 2017.

[30] K. Hsieh, A. Harlap, N. Vijaykumar, D. Konomis, G. R. Ganger, P. B. Gibbons, and O. Mutlu, "Gaia: Geo-distributed machine learning approaching lan speeds," in *Proceedings of the 14th USENIX Conference on Networked Systems Design and Implementation*, NSDI'17, (USA), p. 629–647, USENIX Association, 2017.

[31] X. Guowen, L. Hongwei, Z. Yun, X. Shengmin, N. Jianting, and D. R. H., "Privacy-preserving federated deep learning with irregular users," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1364–1381, 2022.