Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol. 14, No. 2, 2024, pp. 17-23

DOI: https://doi.org/10.51983/ijiss-2024.14.2.03

Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data

Dr.R. Mohandas[1*], Dr.S. Veena[2], G. Kirubasri[3], I. Thusnavis Bella Mary[4] and Dr.R. Udayakumar[5]

[1*]Assistant Professor, Department of Computational Intelligence, SRM Institute of Science and Technology, Kattankulathur, Chennai, India

[2]Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India

[3]Assistant Professor, Computer Science and Engineering, Sona College of Technology, Salem, India

[4]Assistant Professor, Department of Electronics and Communication Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India

[5]Dean, CS & IT, Kalinga University, India

E-mail: [1*]mohandar1@srmist.edu.in, [2]veenas1@srmist.edu.in, [3]kirubasri.cse@sonatech.ac.in, [4]bellamary@karunya.edu, [5]rsukumar2007@gmail.com, [5]deancsit@kalingauniversity.ac.in

ORCID: [1*]https://orcid.org/0000-0001-9929-0121, [2]https://orcid.org/0000-0003-0126-9119, [3]https://orcid.org/0000-0002-2086-8064, [4]https://orcid.org/0000-0002-3154-556X, [5]https://orcid.org/0000-0002-1395-583X

(Received 03 April 2024; Revised 20 April 2024; Accepted 9 May 2024; Available online 10 June 2024)

Abstract **- Federated Learning (FL) is a machine learning methodology that allows remote devices to collectively train a learning system without sharing their data. FL-based methods provide enhanced secure privacy by transmitting only localized model variables, learned with local information, from dispersed devices to a centralized controller. There is a potential for a centralized server or malicious individuals to deduce or get sensitive private data by analyzing the structure and variables of regional learning networks. This study incorporates the FL process into the deep learning process of medical prototypes in an Internet of Things (IoT)-based medical facility. A Secured Medical Homomorphic Encryption Algorithm (SMHEA) is proposed in this research to ensure medical data privacy. Cryptographic primitives, such as masking and homomorphic cryptography, are used to enhance the security of local modeling. This prevents adversaries from deducing confidential health information via assaults like model restoration or modeling inversion. The primary determinant for assessing the regional modeling's contributions to the universal model during each training stage is the quality of the databases possessed by various individuals rather than the typically used metric of database dimension in deep learning. A dropout-tolerant approach is suggested, where the FL procedure would continue as long as the total amount of online customers remains over a certain level. By doing a security evaluation, it is evident that the suggested approach effectively ensures data privacy. Theoretical analysis is conducted on accuracy, computation time, and communication error. An example of clinical applications is the categorization of skin lesions using training photos from the HAM10000 medical database. The experimental findings demonstrate that the suggested system had favorable performance and privacy preservation outcomes compared to current methods.**

Keywords: **Healthcare, Federated Learning, Privacy, Encryption, Internet of Things**

I. Introduction to Healthcare and Data Privacy

The Internet of Things (IoT) is a novel concept with diverse practical uses (Sarker et al., 2023). IoT-enabled healthcare apps provide continuous tracking and intelligent medical IoT gadgets linked with a smartphone app, enabling clinicians to access health information from clients at any time or place. In addition, it offers Computer-Aided Diagnostics (CAD), healthcare picture analysis, and remote healthcare support, among other services (Wang et al., 2022). It enhances the operational efficiency of medical institutions and improves the quality of treatment patients receive. IoT-based healthcare solutions have many benefits, including improving the quality and effectiveness of therapy and ultimately enhancing the health of individuals. Machine Learning (ML) has led to significant breakthroughs in CAD approaches, reaching previously unseen levels (Alanazi, 2022). Skin cancer, a prevalent form of cancer that develops in the epidermal layer due to exposure to ultraviolet rays, has received considerable attention. Deep Learning (DL) methods have achieved accuracy comparable to trained physicians (Abdullah et al., 2022). A comparison was made between the leaf classification models developed in this study using five distinct datasets containing varying numbers of images. Four distinct pre-trained models—VGG16, InceptionV3, MobileNet, and DenseNet—are employed for this objective. Furthermore, a novel model was introduced, and the datasets were utilized to train the model (Camgözlü & Kutlu, 2023).

In IoT-enabled medical facilities, researchers have suggested a Federated Learning (FL) approach to balance the

advantages of information sharing with the need to protect confidentiality (Nguyen et al., 2022). This structure enables information for FL to be stored in a regional repository. FL offers extensive opportunities for using Artificial Intelligence (AI) across several sectors. FL is flexible when it comes to safeguarding privacy. Adapting FL to actual usage settings, such as IoT-based medical facilities, still presents some obstacles.

A central server transmits a universal model for AI learning to several dispersed devices (Alowais et al., 2023). After training the model using their information, these devices return local model settings to the centralized server. The controlled server synchronizes the global model variables by including the regionally developed model variables from the distributed gadgets. Then, it distributes the latest global model variables to the various devices. This process is iterated until convergence is attained. FL offers the benefit of safeguarding sensitive personal details by not necessitating the transmission of local information. The latest study indicates that the learned local model variables on dispersed devices potentially expose localized information, allowing hackers to deduce private data about those participating in the FL process. ANNs. Many scholars have used artificial neural networks (ANNs) for modeling in medical and clinical research. Artificial neural networks (ANNs) are widely used in pharmaceutical epidemiology and medical data mining (Jelena & Srđan 2023). The author of this study (Mansouri, 2023) presents an overview of the many uses of artificial neural networks in medical research.

Homomorphic Encryption (HE) is a cryptographic technique that performs mathematical operations on encrypted data without decryption (Munjal & Bhatia, 2023). The centralized web server uses the HE technique to modify the universal modeling variables using homomorphic operations on the encrypted localized variations. The IoT gadgets involved in FL, called customers, do not need to worry about data leaking via local variations (Singh et al., 2022). This is because they transmit encrypted localized variations to the servers. Consumers must utilize the same personal key in the FL-based mechanism (Udayakumar et al., 2023). This is because homomorphic activities can only be carried out on data secured with the corresponding standard key.

The Secured Medical Homomorphic Encryption Algorithm (SMHEA)’s primary contributions are outlined as follows:

1. A unique masking strategy, which combines HE with secure computing, has been presented for FL. This system applies a weighted mean approach that considers information quality to substitute the standard way of calculating weights based on the quantity of data.

2. The SMHEA approach proposes a solution that is tolerant to dropouts and resistant to individual collision. This is achieved by using the Diffie-Hellman key exchange and Shamir secret exchange algorithms.

3. A working model for FL has been developed to handle medical information. The suggested SMHEA method has been tested thoroughly with actual skin cancer databases to ensure confidentiality and effectiveness.

The following sections are shown: Section 2 provides an overview of the history and associated research on security and privacy strategies in medical models. Section 3 introduces the Secured Medical Homomorphic Encryption Algorithm and analyzes its impact. Section 4 presents the software analysis and its conclusions. Section 5 summarizes the research's results and discusses potential areas for further exploration.

II. Background and Related Works

FL is an effective method for maintaining privacy in ML. This is achieved by having individuals involved in the training phase send only their locally learned model variables derived from their information to a central server (Sathiyabhama et al., 2020).

Tian et al., introduced the Depth Gradient Leakage System (DGLS) method (Tian et al., 2023). This system allows attackers to restore a picture resembling the original specimen, even when they do not know additional data to save the regional system. The restoration is achieved by training a fake sample. Thus, it is evident that despite the local storage of the initial information in FL, updating the localized modeling still presents attackers with options for attack. Several techniques and heuristics have been investigated to conceal sensitive data via transaction elimination. However, researchers have difficulty to achieve tolerable side effects. This study proposes sensitive data concealment strategies using the rain optimization algorithm (ROA) (Madhavi et al., 2023).

Mbonu et al., developed a Secured Double-Masking Aggregation System (SDMAS) that incorporates numerous techniques like Diffie-Herman key contract, Shamir secret collaboration, pseudo-random generators, public vital facilities, and verification (Mbonu et al., 2023). Despite the system's ability to achieve effective aggregation even when specific individuals stopped out, there was a significant communication cost due to the repeated requests for unmasking in each training period.

Munjal et al., used the Additive Homomorphic Encrypting Approach (AHEA) to safeguard the localized modeling from being seen by well-intentioned yet interested individuals throughout the model consolidation procedure (Munjal & Bhatia, 2023). While HE offers the most robust assurance for privacy protection, it also imposes a significant computational burden. HE influences the efficacy of federated deep learning when using a high-dimensional system. It has become a substantial obstacle to the practical implementation of HE. Specific HE techniques with gradient sparseness and stochastic quantification have been presented to reduce computational expenses.

Muazu et al., introduced a more cost-effective technique by implementing a novel secret-sharing architecture (Muazu et al., 2024). The confidential sharing was only sent to adjacent nodes rather than all stations. The amount of communication required needed to be increased.

Abd El-Mageed et al., successfully addressed a binary supervised categorization issue involving the prediction of hospitalization duration for patients diagnosed with heart failure (Abd El-Mageed et al., 2022). Despite the data being stored locally, the potential privacy breach resulting from the model modifications was still significant. None of the two approaches took into account the solutions.

Shiri et al., introduced a multi-institutional federated training technique for the patient resemblance network (Shiri et al., 2023). The method utilizes HE methods to guarantee patient privacy. FL's current privacy preservation methods have several limitations and can only partially address all the issues in a single scheme. As a case study.

Zhang et al., introduced a method called FedOpt (Zhang et al., 2022). This technique incorporates a sparse compression algorithm to enhance communication efficiency and integrates HE.

Almogren et al., introduced an approach that utilizes HE to secure every variable (Almogren et al., 2020). They still need to resolve the issue of consumers who discontinue their services. This study (Sindhusaranya et al., 2023) introduces Federated Learning and Blockchain-Enabled Privacy-Preserving (FL-BEPP) for Fraud Prevention and Security (FPS) inside the IoMT architecture. The system employs several dynamic techniques. This study looks at medical applications that face harsh restrictions, such as deadlines, and soft constraints, such as resource usage, while running on distributed fog and cloud nodes. These previously mentioned methodologies for network traffic analysis often need a large amount of information about network activity. Therefore, this study provides OFedeMWOUAA (optimal federated learning-based UAA approach with Meadow Wolf Optimisation) and DNN (deep Neuron Networks) for decreasing risks of data leakages in MWNs (Mobile Wireless Networks).

III. Proposed Secured Medical Homomorphic Encryption Algorithm

This section describes the SMHEA framework implemented in the healthcare sector. The system primarily consists of two subjects: a model aggregating server and dispersed consumers. Fig. 1 displays the precise design of the SMHEA. The server's role is to gather the anonymized local models provided by consumers and execute a sequence of actions to finalize the safe aggregating of the designs.

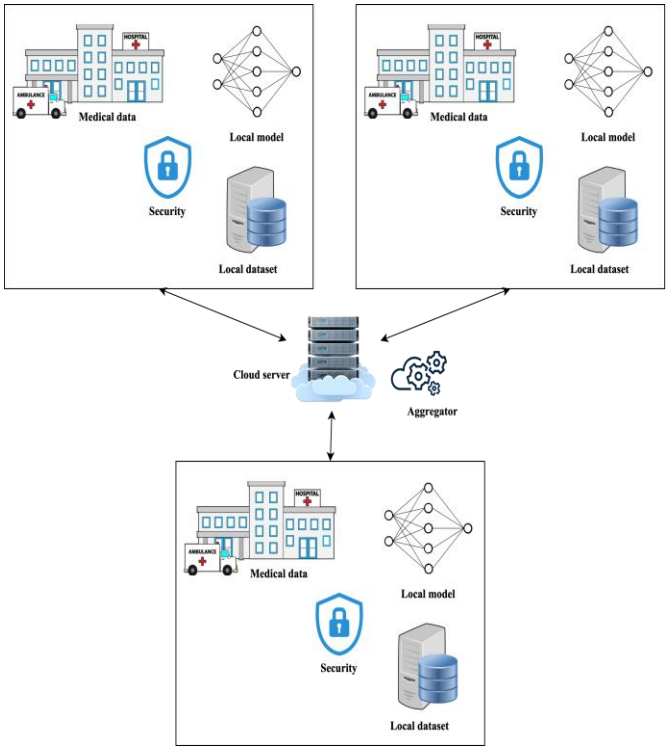

Fig. 1 System Overview of the SMHEA

The clients are medical institutes with a substantial quantity of unprocessed health information. The individuals are responsible for training regional models using regional medical databases and sending the disguised regional models and associated secure variables to the server. The web server and customers mutually cooperate in each phase to construct the ideal universal architecture. In contrast to the conventional architecture, the system includes a third-party Trust Agency (TA) to bolster the privacy protection of the localized modeling. The TA's role is to initialize various security variables, including public and private credentials.

Throughout the collaborative training procedure, the server and all customers are assumed to be trustworthy but inquisitive. This implies they are willing to follow the protocol but intend to secretly gather confidential details from recorded data. The subsequent safety standards must be met to maintain privacy:

1. During local training, customers need help accessing or learning the genuine models of other customers. They can only access their own localized modeling and the aggregating universal modeling. This ensures that critical raw information from other customers remains undisclosed.

2. The server can only access masked modeling with customers' encrypted variables but cannot access genuine localized modeling or health information. It is capable of producing a consolidated worldwide model.

3. The data stored in every customer ought to be kept confidential. Data reliability is crucial in assessing the influence rate of various regional models on the universal model. Additionally, it plays a vital role in attaining safe aggregation. To prevent discrimination against some customers with inadequate quality information, it is essential to maintain the confidentiality of data assurance. This approach can guarantee that every customer engages in FL with equity and neutrality.

Malevolent and outside forces attempt to deduce medical confidentiality within the network by intercepting communications across the channel. The internal server inside the structure conspires with some customers to satisfy their curiosity about sensitive info. The system is committed to resisting passively hostile competitors and colluding assaults. The system does not consider intentionally disruptive actions during modeling exercises, such as manipulation incidents, impersonation incidents, and poisoning assaults.

3.1. Distributed HE for SMHEA

A Decentralized HE is a cryptographic system that utilizes a secure coalition of parties' computation to enable the implementation of different homomorphic functions in a decentralized way. Fig. 2 depicts the decryption procedure of distributed HE. In conventional public-key cryptography, individuals with public and private credentials encrypt and decrypt to ensure safe interaction. The distributed HE divides a private certificate into numerous partial confidential keys and distributes them to multiple dispersed computers. Remote servers use partial secret keys to carry out partial decoding by using values secured with a common password. The remaining dispersed servers get the original text by gathering the partly deciphered encrypted messages. The decoding procedure facilitates a range of homomorphic activities that rely on collaborative efforts from several parties.

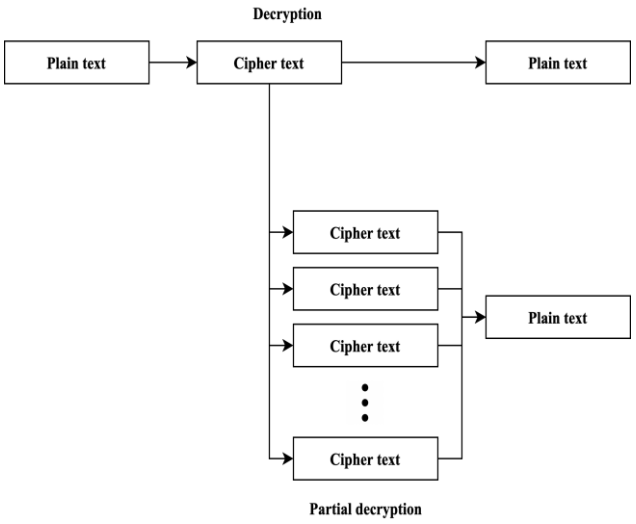

Fig. 2 Encrypting and Decrypting Process of the SMHEA

The duties of the DHC are outlined as follows:

Key generation: This function creates a public-private credential combination (pb_x, pr_x) for a consumer, where x is an integer from 1 to M_x, and M_x is the total number of customers that attend the local learning. The credential pairing is generated using two huge prime integers p and q. The shared key is determined by multiplying p and q, whereas the personal password matching the public password is derived by finding the Least Common Multiple (LCM) of p - 1 and q – 1, then dividing it by 2. The size of the key, denoted as K, is equal to the product of p and q. As the chosen prime numbers rise, the computing cost of the cryptosystem grows due to the increased difficulty of the exponentiation process involved in encryption and decryption. The private key pr_x divided to create partly private keys $pr_x^1, pr_x^2, \cdots, pr_x^{M_x}$ for dispersed servers, where M_x represents the total number of distributed systems. The system chooses a value for δ that simultaneously meets the conditions δ = 0 mod pr_x, and δ = 1 mod K. The system randomly chooses y values $\{r_1, r_2, \cdots, r_x\}$ from the set of non-zero integers in $Z^*_{pr_x K^2}$. The system uses these variables to establish the polynomial $(i) = \delta + \sum_{x=0}^{N} r_x i^x$. The fractional private password, denoted as pr_x^y, is derived by evaluating the polynomial $p(i_y)$ employing a non-zero value i_y within the set $Z^*_{pr_x K^2}$.

Encryption is a process that produces a ciphertext $C_{pb_x}(n) \in Z^*_{K^2}$ from a plaintext $n \in Z_k$, utilizing a public key pb_x. The length of the key, denoted as K, is equal to p•q. To simplify, the ciphertext $C_{pb_x}(n)$denoted as $[n]_x$.

Decryption is a process that involves utilizing a private key pr_x to decode a ciphertext $[n]_x$ and get the original value of n.

Fractional decryption refers to the process of generating a partly decoded ciphertext by utilizing a fractional private key pr_x^k, where k is an integer ranging from $1,2, \cdots, N_x - 1$. To simplify, the system represents the partly decrypted ciphertext $C_{pb_x}(n)([n]_x)$ as $C^n([n]_x)$.

Decryption aggregation retrieves and outputs the value of m utilizing $(N_x - 1)$ partly decoded ciphertexts $C^n([n]_x)$ for $k \in \{1,2, \cdots, N_x - 1\}$ and the slightly private key $pr_x^{N_x}$.

3.2. Security of the HE

The security study shows the masking technique effectively safeguards the actual inputs a_x^p. The system focuses on determining if the colluding entities A can decrypt the information and recover the localized modeling w_x^p by compromising the conceptual safety of HE, assuming the actual inputs $a_x^p = w_x^p Q_x^p + \alpha Q_x^p$,. It is essential to highlight that the risk model must still adhere to the assumption that fewer than e customers engage in collusion.

During the encryption procedure, customer x uses the method's public key pb_x to secure information quality and transmit the resulting ciphertext (C_{pr_x}) to the service. To decrypt the information quality of customer x and access its regional modeling w_x^p, which is calculated using the equation $w_x^p = \frac{a_x^p}{Q_x^p - \alpha}$, the server must first re-establish the value of $2^{Q_x^p}$. The method's private credentials pr_x is securely maintained as confidential information for the server and all clients. Hence, for the server to recover $2^{Q_x^p}$ without pr_x, it must first answer the distinct logarithm issue to determine pr_x and then address the Decisional Diffie-Hellman issue.

If the server is unable to independently recover $pr^{Q_x^p}$, it conspires with other customers to seek their aid in rebuilding the secret credential pr_x. Within the framework, the server collaborates with online customers to acquire the aggregation result Q_x^p, representing the information quality. The server must determine rather than reconstruct the confidential key pr_x. The threat scenario for collusion differs from conventional cooperation since the colluding parties A aim to obtain the high-quality data Q_x^p from a single honest customer. In the absence of the personal credential pr_x, their sole option is to calculate the total of data characteristics of all honest clients by calculating $\sum_{x=0}^{N_3/A} Q_x^p = \sum_{x=0}^{N_3} Q_x^p - \sum_{x=0}^{A} Q_x^p$. It appears the most efficient method to accomplish their objective is via rebuilding data. The quantity of customers that are conspiring, denoted as $A/\{S\}$, falls below the threshold value of th_x. The Shamir confidential sharing method states that it is impossible to recreate a private credential pr_x with less than th_xsharing. Neither the server nor the client can decode a single Q_x^p, ensuring the safeguarding of the localized modeling w_x^p. If the number of consumers involved in collusion is lower than th_x, the HE remains operationally safe.

IV. System Evaluation and Results

The database utilized for the efficacy assessment is the HAM10000 database, which contains 10,015 dermatoscopic pictures of common pigmented skin conditions (HAM10000 dataset). It is also called the "Human Against Machine with 10,000 learning pictures" database. There are seven distinct types of skin tumors: 1) Nevus, 2) Melanoma, 3) Colored Bowen's, 4) Basic Cell Malignancy, 5) Colored Benign Keratoses, 6) Arterial, and 7) Dermatofibroma. They only use the given photos without including any meta-data or additional information. To address the uneven distribution of subcategories in the database and enhance the quality of the model for categorization while preventing overfitting, the system augmented the initial HAM10000 database and used various data augmentation methods. To evaluate the effectiveness of the assessment, the system conducted FL on a computer running Linux that comes with an Intel Central Processing Unit (CPU) (3 cores, ten threads, 2.4 GHz) and 16 GB Random Access Memory (RAM). The Linux distribution that was used is Ubuntu 22. The system executes a server application to oversee the learning process and simultaneously operates several client applications on a Linux machine (with a user count ranging from 5 to 50).

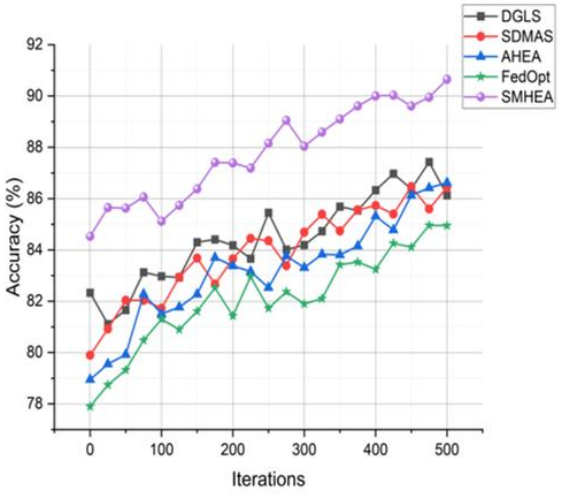

Fig. 3 Accuracy Analysis of Privacy Preservation in Healthcare Systems

Fig. 3 displays the accuracy (%) metrics for several FL approaches throughout iterations: DGLS, SDMAS, AHEA, FedOpt, and the proposed SMHEA. The accuracy is determined by calculating the proportion of occurrences in the dataset that are correctly categorized. The average accuracy achieved by DGLS is 83.38%, SDMAS is 84.02%, AHEA is 83.63%, FedOpt is 82.65%, and SMHEA is 88.43%. The SMHEA frequently demonstrates higher accuracy compared to other approaches. The enhanced efficacy of SMHEA is credited to the integration of HE and privacy-preserving solid methods. This effectively reduces privacy concerns and produces encouraging outcomes in skin lesion categorization using the HAM10000 medical database.

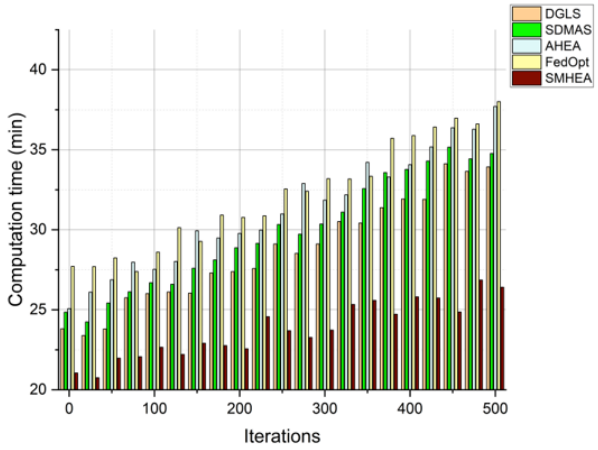

Fig. 4 Computation Time Analysis of Privacy Preservation in Healthcare Systems

Fig. 4 presents the metrics of computation time (in minutes) for multiple FL techniques, including DGLS, SDMAS, AHEA, FedOpt, and the suggested SMHEA, at different iterations. Computation time refers to the length of time required for the completion of the FL procedure. The average time needed for DGLS, SDMAS, AHEA, FedOpt and SMHEA is 26.85 minutes, 28.19 minutes, 29.07 minutes,

30.47 minutes, and 24.89 minutes. The suggested SMHEA regularly demonstrates shorter calculation times in comparison to previous approaches. The effectiveness of this system is ascribed to HE, which enables safe, collaborative learning while minimizing processing requirements. This makes it a practical option for healthcare systems that prioritize privacy.

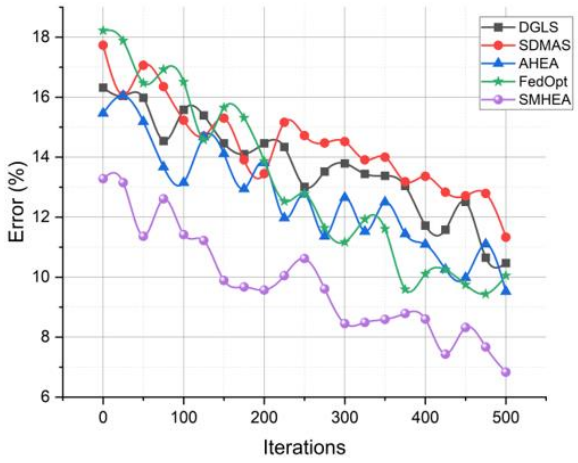

Fig. 5 Error Analysis of Privacy Preservation in Healthcare Systems

Fig. 5 displays the Error (%) metrics for several FL approaches, including DGLS, SDMAS, AHEA, FedOpt, and the suggested SMHEA, over multiple iterations. The error is determined by calculating the proportion of incorrectly categorized cases in the dataset. The average error rates for DGLS, SDMAS, AHEA, FedOpt, and SMHEA are 13.99%, 13.92%, 12.73%, 12.61%, and 8.77% respectively. The suggested SMHEA regularly performs better than previous approaches, exhibiting reduced error rates. The exceptional performance of SMHEA is due to the incorporation of HE and privacy-preserving solid methods. This integration minimizes the likelihood of misclassifications and guarantees efficient privacy protection in healthcare systems.

V. Conclusion and Future Scope

This study introduces an SMHEA strategy designed to protect privacy in medical applications that utilize the IoT. A novel approach, using data quality as a basis, is suggested as a replacement for the conventional weight estimation technique that relies on data quantity. A new masking approach using HE and safe computing is described for FL. The SMHEA approach selectively encrypts specific model parameters due to the often large dimensions of deep learning models. Encrypting such high-dimensional information would result in significant computational overhead. The SMHEA method encrypts each client's data quality parameter throughout each training period. Hence, the suggested SMHEA would not result in a significant rise in computational overhead. The encryption technique is modified to transform its multiplicative homomorphism properties into adding homomorphism, which aligns with the requirements of the system provided in the study. The approach incorporates the Diffie-Hellman key exchanging and Shamir secret sharing method to offer a versatile solution to tolerate dropouts and resist collusion among players.

This research examines explicitly secure privacy techniques and categorization accuracy. The investigations have achieved a detection accuracy of over 88.43% for identifying the cell type of lesions. The model can also be optimized via fine-tuning to enhance its performance and attain higher accuracy in subsequent iterations. The system must consider the scenario when customers have diverse characteristics, such as limited hardware resources and using asynchronous FL. The suggested SMHEA technique requires further optimization in a heterogeneous environment to achieve optimal efficiency. The suggested aggregating in FL does not include studying a malevolent server. The system has not considered the possibility of the consolidated model being tampered with or fabricated by the servers. Implementing verifiable aggregating in FL is a priority for future study.

References

[1] Abd El-Mageed, A.A., Gad, A.G., Sallam, K.M., Munasinghe, K., & Abohany, A.A. (2022). Improved binary adaptive wind driven optimization algorithm-based dimensionality reduction for supervised classification. *Computers & Industrial Engineering, 167*, 107904. https://doi.org/10.1016/j.cie.2021.107904

[2] Abdullah, A.A., Hassan, M.M., & Mustafa, Y.T. (2022). A review on bayesian deep learning in healthcare: Applications and challenges. *IEEE Access, 10*, 36538-36562.

[3] Alanazi, A. (2022). Using machine learning for healthcare challenges and opportunities. *Informatics in Medicine Unlocked, 30*, 100924. https://doi.org/10.1016/j.imu.2022.100924

[4] Almogren, A., Mohiuddin, I., Din, I.U., Almajed, H., & Guizani, N. (2020). Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet of Things Journal, 8*(6), 4485-4497.

[5] Alowais, S.A., Alghamdi, S.S., Alsuhebany, N., Alqahtani, T., Alshaya, A.I., Almohareb, S.N., & Albekairy, A.M. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC Medical Education, 23*(1), 689. https://doi.org/10.1186/s12909-023-04698-z

[6] Camgözlü, Y., & Kutlu, Y. (2023). Leaf Image Classification Based on Pre-trained Convolutional Neural Network Models. *Natural and Engineering Sciences, 8*(3), 214-232.

[7] https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/DBW86T

[8] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. *Arhiv za tehničke nauke, 2*(29), 11-22.

[9] Madhavi, M., Sasirooba, T., & Kumar, G.K. (2023). Hiding Sensitive Medical Data Using Simple and Pre-Large Rain Optimization Algorithm through Data Removal for E-Health System. *Journal of Internet Services and Information Security, 13*, 177-192.

[10] Mansouri, S. (2023). Application of Neural Networks in the Medical Field. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 14*(1), 69-81.

[11] Mbonu, W.E., Maple, C., & Epiphaniou, G. (2023). An End-Process Blockchain-Based Secure Aggregation Mechanism Using Federated Machine Learning. *Electronics, 12*(21), 4543. https://doi.org/10.3390/electronics12214543

[12] Muazu, T., Mao, Y., Muhammad, A. U., Ibrahim, M., Kumshe, U. M. M., & Samuel, O. (2024). A federated learning system with data fusion for healthcare using multi-party computation and additive secret sharing. *Computer Communications, 216*, 168-182.

[13] Munjal, K., & Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, *9*(4), 3759-3786.

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

[15] Sarker, I.H., Khan, A.I., Abushark, Y.B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), 296-312.

[16] Sathiyabhama B., Rajeswari K.C., Reenadevi R., & Arul Murugan R. (2020). Preserving Data Privacy in Electronic Health Records Using Blockchain Technology. *In D. Rajput, R. Thakur, & S. Basha (Eds.), Transforming Businesses with Bitcoin Mining and Blockchain Applications. IGI Global*, 195-206. https://doi.org/10.4018/978-1-7998-0186-3.ch011

[17] Shiri, I., Vafaei Sadr, A., Akhavan, A., Salimi, Y., Sanaat, A., Amini, M., & Zaidi, H. (2023). Decentralized collaborative multi-institutional PET attenuation and scatter correction using federated deep learning. *European Journal of Nuclear Medicine and Molecular Imaging*, *50*(4), 1034-1050.

[18] Sindhusaranya, B., Yamini, R., Manimekalai, M.A.P., & Geetha, K. (2023). Federated Learning and Blockchain-Enabled Privacy-Preserving Healthcare 5.0 System: A Comprehensive Approach to Fraud Prevention and Security in IoMT. *Journal of Internet Services and Information Security*, *13*(3), 199-209.

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

[20] Tian, Y., Wang, S., Xiong, J., Bi, R., Zhou, Z., & Bhuiyan, M.Z.A. (2023). Robust and privacy-preserving decentralized deep federated learning training: Focusing on digital healthcare applications. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*. https://doi.org/10.1109/TCBB.2023.3243932

[21] Udayakumar, R., Suvarna, Y.P., Yogesh, M.G., Vimal, V.R., & Sugumar, R. (2023). User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *14*(2), 66-81.

[22] Wang, G., Badal, A., Jia, X., Maltz, J.S., Mueller, K., Myers, K.J., & Zeng, R. (2022). Development of metaverse for intelligent healthcare. *Nature Machine Intelligence*, *4*(11), 922-929.

[23] Zhang, L., Xu, J., Vijayakumar, P., Sharma, P.K., & Ghosh, U. (2022). Homomorphic encryption-based privacy-preserving federated learning in iot-enabled healthcare system. *IEEE Transactions on Network Science and Engineering*, *10*(5), 2864-2880. https://doi.org/10.1109/TNSE.2022.3185327