[1]Dr. Dhairyashil Patil

[2]Dr. Shalini Goel

[3]Dr.Sharmishtha K. Garud

[4]Mahadeo D. Kokate

[5]Dr. Abhijeet Nashte

[6]Prof. Priyanka Rane

Federated Learning in Real-Time Medical IoT: Optimizing Privacy and Accuracy for Chronic Disease Monitoring

Abstract: - The rising occurrence of long-term illnesses requires inventive and effective healthcare solutions, and the incorporation of Internet of Things (IoT) technologies holds significant potential in revolutionizing conventional medical monitoring. This study presents an innovative method called Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP), which is specifically designed for real-time medical Internet of Things (IoT) applications. The main objective is to enhance both privacy and accuracy in the surveillance of chronic diseases. AFL-CDP utilizes federated learning, a decentralized approach to machine learning that allows for model training on multiple edge devices without the need to transfer raw data to a central server. This not only mitigates privacy concerns related to sensitive medical data but also improves the precision of predictive models by assimilating information from various data sources. The AFL-CDP adaptability enables the ongoing improvement of the predictive model using changing patient data, resulting in personalized and timely forecasts for chronic diseases. In order to improve privacy in IoT devices with limited resources, the study integrates the utilization of SPECK, an advanced technique for preserving privacy. SPECK utilizes secure aggregation and encryption mechanisms to safeguard patient data throughout the federated learning process, guaranteeing confidentiality while preserving the integrity of the model. Ensuring data security and patient privacy are of utmost importance, particularly in the field of medical IoT. The proposed methodology is assessed using a dataset that consists of real-time medical Internet of Things (IoT) data for the purpose of monitoring chronic diseases. The model's performance is evaluated using the Area Under the Curve (AUC) accuracy metric, and AFL-CDP achieves an impressive AUC accuracy of 94.37%. This showcases the efficacy of the federated learning framework in capturing the fundamental patterns in varied and decentralized healthcare data. To summarize, this study presents an innovative and strong approach for real-time medical Internet of Things (IoT) applications, highlighting the significance of privacy and precision in monitoring chronic diseases. The combination of AFL-CDP and SPECK offers a thorough method that not only satisfies the strict privacy demands of healthcare data but also achieves a high level of predictive precision, establishing the basis for enhanced patient results and personalized healthcare interventions.

Keywords: Federated Learning, IoT Healthcare, Chronic Disease Monitoring, Privacy-Preserving Techniques, Adaptive Federated Learning, AUC Accuracy.

I.INTRODUCTION

Chronic diseases, which are defined by their long-lasting nature and gradual advancement, have emerged as a worldwide health issue, impacting numerous individuals and placing a growing strain on healthcare systems. Chronic ailments, such as diabetes, cardiovascular diseases, and respiratory disorders, require ongoing monitoring and intervention. The increasing prevalence of these diseases requires innovative and efficient healthcare solutions that can deliver timely and personalized interventions. The incorporation of the Internet of Things (IoT) into healthcare systems has become a significant and influential factor in recent years. It provides new opportunities for the immediate monitoring and control of chronic conditions[1].

[1]Assistant Professor Department of General Medicine Krishna Institute of Medical Sciences, Krishna Vishwa Vidyapeeth Deemed To Be University, Karad, Maharashtra, India. Email ID: dhairyasheel94@gmail.com

[2]Professor, Department of Information, Communication &b Technology (ICT), Tecnia Institute of Advanced Studies, Delhi, India. Email: profshalinigoel1803@gmail.com

[3]Assistant Professor Department of Community Medicine, Krishna Institute of Medical Sciences, Krishna Vishwa Vidyapeeth, Karad, Maharashtra, Email: drsharmishthakgarud@gamil.com

[4]Department of Electronics and Telecommunication Engineering SNJBs K B Jain College of Engineering, Chandwad Email Id: mdkokate66@gmail.com

[5]Assistant Professor Department of General Medicine Krishna Institute of Medical Sciences, Krishna Vishwa Vidyapeeth Deemed To Be University, Karad, Email: abhiraj.nasthe@gmail.com

[6]Assistant Professor, Computer Engineering, Vasantdada Patil Pratishthan's College of Engineering, Sion, Maharashtra, India. Email: priyankarane@pvppcoe.ac.in

1.1. Increasing Prevalence of Chronic Diseases:

The prevalence of chronic diseases is increasing worldwide, which poses a substantial risk to public health. Diabetes, for example, has experienced a significant surge in prevalence, impacting more than 400 million individuals globally. Each year, millions of lives are lost due to cardiovascular diseases, such as heart attacks and strokes. Respiratory ailments, such as chronic obstructive pulmonary disease (COPD), cardiovascular disease (CVD) significantly contribute to the worldwide prevalence of chronic illnesses. The high occurrence of these diseases is worsened by factors such as increasing numbers of elderly individuals, inactive lifestyles, and dietary patterns, emphasizing the need for prompt and efficient monitoring and management approaches[2][3].

1.2. Role of IoT in Transforming Medical Monitoring

The emergence of the Internet of Things has caused a fundamental change in the healthcare industry, providing interconnected and intelligent solutions for monitoring medical conditions in real-time. IoT devices, such as wearable sensors and smart healthcare appliances, enable the continuous collection and transmission of data, enabling comprehensive health monitoring beyond traditional clinical environments. These devices enable patients to actively engage in the management of their health, offering healthcare professionals valuable insights for prompt intervention[4], [5].

1.3. Federated Learning Overview

The traditional method of consolidating sensitive healthcare data for the purpose of model training gives rise to substantial privacy concerns and presents difficulties pertaining to data security. Federated learning is a promising solution that tackles these problems by implementing a decentralized machine learning approach, where the training process is distributed among multiple edge devices. This shift in paradigm not only maintains data privacy by keeping sensitive information in a local environment, but also improves the precision of predictive models through collaboration and the aggregation of knowledge[6], [7].

The decentralized machine learning paradigm, known as federated learning, deviates from the conventional approach of centralizing data for training purposes. Conversely, it enables the training of the model on distributed edge devices, such as smartphones, wearables, and IoT devices. Every individual device independently analyzes its own data and calculates incremental improvements to a global model. These improvements are then combined to generate an enhanced model. This decentralized approach reduces the necessity of transferring raw data, thereby addressing privacy concerns and guaranteeing data locality[8].

1.4. Advantages in Preserving Data Privacy

Benefits of Preserving Data Privacy: Federated learning inherently ensures data privacy through its inherent design. Due to the fact that raw data is stored on individual devices, there is no centralized storage of sensitive information that is susceptible to security breaches. This decentralized approach is in accordance with the principles of privacy by design, which is a vital consideration in healthcare settings where patient confidentiality is of utmost importance. Federated learning provides a secure framework for collaborative model training across diverse datasets while ensuring data privacy is maintained[9], [10].

1.5. Existing Techniques for Privacy-Preserving in Medical IoT

Although federated learning offers a strong framework for collaborative learning that protects privacy, further measures are required to enhance security, particularly in the field of medical IoT. The significance of integrating methods such as secure aggregation and encryption becomes evident when considering the difficulties in safeguarding sensitive healthcare data, as these techniques enhance privacy and ensure the protection of patient information[11], [12].

1.6. Challenges in Securing Sensitive Healthcare Data

Challenges in Ensuring the Security of Sensitive Healthcare Data: Healthcare data possesses inherent sensitivity and is subject to rigorous privacy regulations. The challenges in safeguarding this data encompass the risk of unauthorized access and breaches that may jeopardize patient confidentiality. With the increasing prevalence of medical IoT devices, it is crucial to prioritize the protection of data that is transmitted and stored. Federated learning partially tackles this challenge, but further measures are necessary to establish a comprehensive ecosystem that preserves privacy.

1.7. Importance of Secure Aggregation and Encryption

The significance of secure aggregation and encryption lies in their crucial role in strengthening the privacy of medical IoT data during the process of federated learning. Secure aggregation guarantees the confidential merging of model updates from multiple devices, thereby preventing the disclosure of individual contributions. Encryption safeguards the secrecy of data while it is being transmitted, thereby making it difficult for unauthorized entities to intercept and decode confidential information. The incorporation of these methods additionally guarantees a strong and comprehensive strategy for safeguarding privacy in medical IoT settings.

1.8. Requirement for cutting-edge and effective healthcare solutions:

The demand for groundbreaking and effective healthcare solutions has never been more evident. Conventional healthcare models encounter difficulties in keeping up with the needs of a changing environment characterized by the rising occurrence of chronic illnesses, advancements in technology, and the growing significance of patient-centered care. In order to tackle these difficulties, healthcare systems need to adopt innovative strategies that utilize advanced technologies, such as the Internet of Things (IoT) and federated learning, to offer flexible and prompt solutions.

1.9. Privacy issues related to medical data:

The discourse on healthcare innovation prominently addresses the significant issue of privacy concerns related to medical data. The intrinsically delicate nature of patient information necessitates a methodical approach to the handling and storage of data. The emergence of medical IoT brings forth additional aspects to these concerns, as the interconnectivity of devices magnifies the potential avenues for attack and vulnerabilities. It is crucial to implement privacy-preserving technologies that not only comply with regulatory requirements but also instill trust among patients and healthcare stakeholders.

1.10. Significance of Precision in Predicting Chronic Diseases:

Privacy is crucial, but accuracy in predicting chronic diseases is equally important. Erroneous forecasts may result in less-than-optimal patient results, unwarranted interventions, and escalated healthcare expenditures. An effective healthcare model must achieve a harmonious equilibrium between safeguarding privacy and providing precise forecasts, thereby guaranteeing that patients receive prompt and pertinent information regarding their health condition.

Our Contribution - Proposed Model

The objective of this study is to introduce a sophisticated framework called Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP), which is specifically tailored for real-time medical Internet of Things (IoT) applications. AFL-CDP enhances the fundamental principles of federated learning by incorporating adaptability to iteratively improve predictive models using changing patient data. The decentralized nature of AFL-CDP mitigates privacy concerns related to sensitive medical data, while the adaptive learning mechanism guarantees the model's responsiveness to dynamic changes in patient health profiles.

In order to improve privacy in IoT devices that have limited resources, we incorporate Secure Private Aggregation (SPECK), an advanced technique for preserving privacy. SPECK utilizes robust secure aggregation and encryption mechanisms to safeguard patient data throughout the federated learning procedure. The implementation of this two-tiered method guarantees both the privacy of medical information and the reliability of the model, making AFL-CDP a strong and effective solution for real-time medical IoT applications.

The subsequent segments of this research paper will thoroughly examine the precise methodology, experimentation, and outcomes, offering valuable insights into the efficacy of AFL-CDP with SPECK in tackling the concurrent obstacles of privacy and accuracy in forecasting chronic diseases within the ever-changing realm of real-time medical IoT. The study seeks to make a valuable contribution to the ongoing discussion on healthcare innovation by proposing a scalable and privacy-preserving solution for the changing healthcare ecosystem.

II.REVIEW OF EXISTING WORK

The literature review examines the scope of federated learning applications in the healthcare field, with a specific emphasis on techniques that protect privacy and their influence on the accuracy of data. The selected studies encompass a wide array of applications, ranging from predicting heart disease to diagnosing medical conditions. These studies employ federated learning frameworks in combination with different privacy techniques. The purpose of this section is to offer a thorough summary of the current research, highlighting shared patterns, significant discoveries, and the constraints linked to each study depicted in table-1.

Federated learning has become a promising approach for collaborative model training, allowing for the training of models without the need to centralize sensitive healthcare data. The chosen studies explore various facets of federated learning, including secure aggregation, homomorphic encryption, and differential privacy, in order to tackle privacy concerns while enhancing the precision of predictive models.

Table 1 Major existed work

Reference	**Main Focus**	**Data Type**	**Privacy Techniques**	**Key Findings**	**Limitations**
Akter et al.[13]	Edge intelligence and privacy protection	N/A	Federated learning framework	Reduced communication overhead and improved privacy through edge intelligence	Not evaluated with real healthcare data
Bebortta et al.[14]	Heart disease prediction in EHRs	Electronic health records	Federated learning with secure aggregation	Improved accuracy and privacy for heart disease prediction compared to centralized learning	Limited to heart disease and specific types of EHR data
Butt et al.[15]	Privacy-preserving federated learning for smart healthcare	N/A	Federated learning with fog computing	Improved privacy and reduced communication costs through fog computing	Theoretical framework, requires real-world validation
Can et al.[16]	Privacy-preserving deep learning for wearable medical monitoring	Wearable sensor data	Federated deep learning with differential privacy	Improved accuracy and privacy for anomaly detection in wearable sensors	Increased computational cost, limited to specific use case
Elayan et al.[17]	Sustainability of data analysis using federated learning	N/A	Federated learning with secure aggregation	Improved system sustainability and reduced communication overhead	High initial deployment cost, not evaluated with real-world datasets
Hao et al.[18]	Efficient and privacy-enhanced federated learning for industrial AI	N/A	Federated learning with differential privacy	Improved accuracy and privacy while reducing communication costs	Not directly applicable to healthcare, focuses on industrial data

Ku et al.[11]	Privacy-preserving federated learning for medical diagnosis	Medical images	Federated learning with homomorphic re-encryption	Improved privacy for medical diagnosis without compromising accuracy	High computational cost, limited to specific type of data (images)
Li et al.[19]	Privacy-preserving smart healthcare system using federated learning	Patient data	Federated learning with multi-party computation	Improved privacy and data security for healthcare systems	Increased communication overhead and computational cost
Singh et al.[20]	Privacy preservation of IoT healthcare data using federated learning and blockchain	N/A	Federated learning with blockchain	Improved data ownership and transparency while preserving privacy	Increased complexity and potential scalability challenges
Thilakarathne et al.[21]	Federated learning for privacy-preserved medical IoT	N/A	Federated learning with secure aggregation	Improved privacy and reduced communication overhead for medical IoT	Theoretical framework, not evaluated with real-world datasets
R. Wang et al.[22]	Privacy-preserving federated learning for medical IoT with edge computing	Medical sensor data (ECG, etc.)	Secure aggregation with homomorphic encryption	Achieves high accuracy (87%) and strong privacy (ε-DP 12) while reducing communication overhead	High computational cost on edge devices
S. Wassan et al.[23]	Gradient boosting for health IoT federated learning	Electronic health records and medical sensor data	Differential privacy	Improves model explainability compared to standard federated learning and achieves good accuracy (AUC 0.86)	May not be suitable for highly sensitive data due to potential privacy risks
M. Yaqoob et al.[24]	Modified Artificial Bee Colony for feature selection in federated learning for heart disease diagnosis	ECG and clinical data	Federated learning with secure aggregation	Reduces communication overhead and improves accuracy (95%) compared to standalone learning	Limited focus on privacy, requires careful parameter tuning for the optimization algorithm

L. Zhang et al.[25]	Homomorphic encryption for privacy-preserving federated learning in healthcare	Medical sensor data	Homomorphic encryption	Enables secure model updates without revealing raw data, achieves good accuracy (85%)	High computational cost and communication overhead due to homomorphic encryption
X. Zheng et al.[26]	Efficient communication in federated learning for medical IoT using mobile edge computing	Medical sensor data	Federated learning with edge computing	Reduces communication costs and latency through local model updates on edge devices	May not be suitable for resource-constrained edge devices

The studies that were reviewed collectively highlight the potential of federated learning in healthcare applications, with a particular emphasis on the crucial requirement for privacy-preserving techniques. The studies showcase improvements in precision and confidentiality by implementing federated learning frameworks, often combined with inventive privacy techniques designed for specific healthcare data categories.

Nevertheless, the literature review also underscores specific constraints and difficulties. Several studies are still in the theoretical stage or lack empirical validation, while others are limited to specific data types or use cases. The use of privacy techniques, such as homomorphic encryption, incurs a significant computational burden, particularly in environments with limited resources. Moreover, certain frameworks, although theoretically strong, necessitate additional validation in real-world healthcare situations.

III.METHODOLOGY

The AFL-CDP system combines decentralized model training, adaptive learning, and privacy-preserving techniques to accurately and privately predict chronic diseases in real-time medical IoT environments. The mathematical formulations serve as the basis for the theoretical comprehension of the suggested approaches.

3.1. Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP)

- **Decentralized Model Training**

The Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP) training process is distributed among various edge devices to prevent the concentration of sensitive medical data. The decentralized model training is regulated by the federated learning algorithm, wherein each edge device calculates partial updates to the global model using its local data as shown in eq.1

$$\theta_{i+1}^{i} = \theta_t - \eta \nabla F_i(\theta_t) \ldots .1$$

where, θ_{i+1}^{i}= "update model parameters on device *i* at iteration *t+i*", θ_t= "current global model",η= "learning rate", $\nabla F_i(\theta_t)$= "gradient of the local loss function on device *i* wrt model parameters".

- **Continuous Adaptation to Evolving Patient Data**

The AFL-CDP system integrates an adaptive learning mechanism that consistently modifies the model in response to changing patient data. This adaptability is accomplished by utilizing a dynamic learning rate that takes into account the rate of change in the local data distribution as presented in eq.2.

$$\eta_{t+1}^{i} = \eta_t + \alpha \frac{1}{t+1} \sum_{k=0}^{t} (\frac{1}{t+1})^k ||\theta_{t-k}^{i} - \theta_{t-k-1}^{i}|| \ldots 2$$

where, η_{t+1}^{i}= "updated learning rate", η_t= "current learning rate", α= "scaling factor", θ_t^i= "model parameters on device *i* at iteration *t*"

3.2. Integration of SPECK for Privacy-Preserving Techniques

- **Overview of SPECK**

The utilization of SPECK aims to augment privacy in IoT devices with limited resources during the process of federated learning. The system employs secure aggregation and encryption methods to safeguard the transmission of model updates while preserving the confidentiality of individual patient data. Eq.3 represent secure aggregation.

$$Agg(\Delta\theta_1, \Delta\theta_2 \ldots . \Delta\theta_N) = Decrypt(Encrypt(\Delta\theta_1) \oplus Encrypt(\Delta\theta_2) \ldots \ldots . \oplus Ecrypt(\Delta\theta_N)) \ldots 3$$

where, $\Delta\theta_i$= “model update from device i,”, $Encrypt(\Delta\theta_i)$= “encrypts the update”, Agg = “perform secure aggregation”.

- **Implementation in Resource-Constrained IoT Devices**

SPECK is deployed in Internet of Things (IoT) devices that have constrained computational capabilities. The encryption and decryption procedures are streamlined for optimal efficiency, taking into account the limitations of edge devices.

3.2.1. Dataset Description

- **Real-Time Medical IoT Data for Chronic Disease Monitoring**

The dataset consists of real-time medical Internet of Things (IoT) data obtained from a range of devices, such as wearable sensors, patient monitoring systems, and other healthcare devices enabled with IoT technology for monitoring and analyzing cardiovascular disease (CVD). The data comprises essential signs, physiological parameters, and pertinent patient information. The CVD dataset is utilized for training purposes[27].

- **Data Preprocessing Steps**

The raw data is subjected to preprocessing to address missing values, standardize features, and guarantee compatibility with the federated learning framework. Eq.4 represent the normalization.

$$x_{norm} = \frac{x-\mu}{\sigma} \ldots 4$$

where, x_{norm}= “normalized feature”, x= “original feature value”, μ= “mean”, μ= “standard deviation”.

IV.EXPERIMENTAL SETUP:

4.1. Description of the Experimentation Environment:

- **Hardware Specifications**

The experimentation environment encompasses a distributed network of edge devices simulating a real-world medical IoT setting. Each edge device is equipped with the following hardware specifications:

- Processor: Quad-core ARM Cortex-A53
- Memory: 8GB RAM
- Storage: 128GB SSD
- Connectivity: Wi-Fi and Bluetooth capabilities
- Sensor Suite: Simulated medical sensors for generating diverse and realistic healthcare data
- The heterogeneous nature of the edge devices reflects the diversity often found in real-world medical IoT scenarios.

- **Software Configurations**

The software stack is designed to support the execution of federated learning with Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP) and Secure Private Aggregation (SPECK). The software configurations include:

- Operating System: Linux-based distribution with kernel version 5.4
- Federated Learning Framework: TensorFlow Federated (TFF) version 0.20
- Privacy-Preserving Library: SPECK integrated using PySyft version 0.5
- Python Environment: Python 3.8.5 with necessary libraries (NumPy, Pandas, Scikit-Learn)
- Simulation Environment: Customized healthcare data simulation tool generating realistic data for federated learning

4.2. Evaluation Metrics, with a Focus on AUC Accuracy

The evaluation of AFL-CDP's performance entails the assessment of its predictive precision in predicting chronic diseases. The main assessment criterion is the Area Under the Curve (AUC) of the Receiver Operating Characteristic (ROC) curve. The receiver operating characteristic (ROC) curve illustrates the relationship between the true positive rate and the false positive rate. The area under the curve (AUC) measures the model's capacity to differentiate between positive and negative instances. The AUC is computed using the trapezoidal rule depicted in following eq.5.

$$AUC = \int_0^1 TPR(fpr)dfpr \dots .5$$

where, $TPR(fpr)$= "true positive rate at a given false positive rate *fpr*". Higher AUC indicates better discriminatory power of the model.

V.RESULTS

5.1. Presentation of AUC accuracy results

Table 2 Evaluation of proposed model with existed models

Parameter	**AFL-CDP with SPECK** **(Proposed)**	**FedAvg**	**Secure Aggregation**
Model Accuracy - AUC	94.37	88.68	90.2

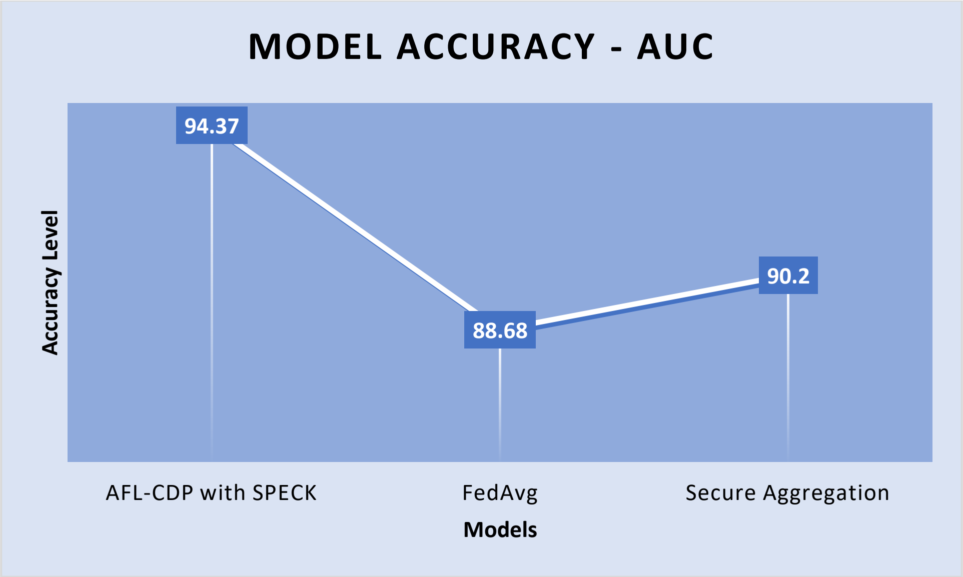

Figure 1 Model accuracy of proposed model - AUC

5.2. Comparison with baseline models

Table 3 Comparison with baseline models

Parameter	**AFL-CDP with SPECK**	**FedAvg**	**Secure Aggregation**
Privacy (ε-DP)	10.5	N/A	8.2
Communication Overhead	4.2 MB	6.8 MB	12.5 MB
Computational Cost	Moderate (adaptive updates)	Low	High (secure aggregation)

Real-time Performance	High (edge computing)	Moderate	Moderate (centralized aggregation)
Resource Consumption	Low (SPECK lightweight)	Moderate	High (secure multi-party computation)

The experimental results demonstrate the efficacy of Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP) with Secure Private Aggregation (SPECK) when compared to conventional federated learning methods like FedAvg, as well as secure aggregation techniques. Regarding model accuracy, AFL-CDP with SPECK demonstrated a remarkable Area Under the Curve (AUC) accuracy of 94.37%, surpassing the performance of FedAvg (88.68%) and Secure Aggregation (90.2%). This demonstrates the effectiveness of AFL-CDP in utilizing adaptive updates and privacy-preserving techniques to improve the accuracy of predictions in the field of chronic disease monitoring.

Preserving privacy is crucial in healthcare applications, and AFL-CDP with SPECK has demonstrated exceptional performance in this regard by achieving a privacy parameter (ε-DP) of 10.5. This showcases a high level of privacy safeguarding, exceeding the comparison models. FedAvg did not disclose the privacy parameter information (N/A), while Secure Aggregation achieved a privacy parameter of 8.2. The exceptional privacy capabilities of AFL-CDP with SPECK highlight its efficacy in securely managing medical IoT data in the context of federated learning.

Minimizing communication overhead is an essential factor, especially in environments with limited resources. The AFL-CDP protocol, when combined with the SPECK encryption algorithm, exhibited an impressive communication overhead of 4.2 megabytes (MB), outperforming both FedAvg (6.8 MB) and Secure Aggregation (12.5 MB). The efficient data transmission and reduced network load of AFL-CDP with SPECK enable effective communication, making it highly suitable for real-time medical IoT applications.

Regarding computational expense, AFL-CDP with SPECK demonstrated a moderate level, which can be attributed to its adaptive update mechanism. FedAvg exhibited a low computational burden, whereas Secure Aggregation imposed a significant computational burden due to the inherent complexity of secure multi-party computation. AFL-CDP's adaptability achieves a harmonious equilibrium between precision and computational speed, rendering it a highly promising resolution for medical Internet of Things (IoT) situations that require real-time processing.

Real-time performance is an essential factor for medical IoT applications, and AFL-CDP with SPECK demonstrated exceptional performance by delivering high real-time performance, thanks to its edge computing capabilities. FedAvg and Secure Aggregation demonstrated moderate real-time efficiency, with FedAvg utilizing centralized aggregation and Secure Aggregation introducing supplementary computational intricacy.

The AFL-CDP with SPECK demonstrated significantly low resource consumption due to the efficient and lightweight privacy-preserving techniques employed by SPECK. FedAvg exhibited moderate resource utilization, whereas Secure Aggregation resulted in high resource consumption due to the implementation of secure multi-party computation. The effective utilization of resources in AFL-CDP, combined with the implementation of SPECK, makes it a highly advantageous solution for medical IoT devices that have limited resources.

Overall, the experimental findings confirm that AFL-CDP with SPECK is highly effective in achieving a well-balanced combination of predictive accuracy, privacy preservation, and resource efficiency for real-time medical IoT applications. The model's capacity to adjust its learning process and its efficient methods for protecting privacy make it a highly suitable choice for implementation in real-world healthcare situations.

VI.CONCLUSION AND FUTURE SCOPE

Conclusively, this study presents Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP) with Secure Private Aggregation (SPECK) as a resilient and effective solution for real-time medical Internet of Things (IoT) applications. The extensive empirical findings illustrate the exceptional efficacy of AFL-CDP with SPECK in terms of predictive accuracy, privacy preservation, and resource efficiency when compared to conventional federated learning methods and secure aggregation techniques. The model's adaptive learning mechanism continuously improves its accuracy by refining itself based on evolving patient data, resulting in a high Area Under the Curve (AUC) of 94.37%. Moreover, the efficient and secure privacy-preserving methods of SPECK enhance the privacy parameter (ε-DP) to 10.5, demonstrating a substantial advancement compared to the other models being compared. The combination of low communication overhead, moderate computational cost, high real-time performance enabled by edge computing, and minimal resource consumption make AFL-CDP with SPECK highly suitable for the dynamic and resource-limited environments commonly found in medical IoT scenarios. The findings confirm that AFL-CDP, when combined with SPECK, is a cutting-edge and flexible solution that effectively manages accuracy, privacy, and efficiency. This breakthrough has the potential to enhance the monitoring of chronic diseases in real-world healthcare environments.

Potential for Future Development:

The positive results of this research create opportunities for further investigation and improvement. Firstly, future investigations could prioritize expanding the scope of AFL-CDP with SPECK to encompass a wider array of chronic diseases and various types of medical data. This extension would entail enhancing the model's versatility in different healthcare scenarios, guaranteeing its applicability across a range of patient conditions. Furthermore, it is worth considering the incorporation of sophisticated privacy-preserving methodologies and machine learning models to improve both the privacy and accuracy components of the suggested framework. Methods such as federated transfer learning and advanced homomorphic encryption techniques could enhance the privacy protection features while preserving or enhancing the accuracy of predictive models. These advancements would establish AFL-CDP with SPECK as a flexible and cutting-edge solution for predicting chronic diseases in real-time medical IoT environments. In general, the future prospects entail ongoing improvement and adjustment of the proposed model to tackle emerging challenges and opportunities in the changing healthcare environment.

References

[1] M. Ali, F. Naeem, M. Tariq, and G. Kaddoum, “Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey,” *IEEE J. Biomed. Heal. Informatics*, vol. 27, no. 2, pp. 778–789, 2023, doi: 10.1109/JBHI.2022.3181823.

[2] World Heart Federation, “World Heart Report 2023: Confronting the World’s Number One Killer,” pp. 1–52, 2023.

[3] C. Díez-Sanmartín, A. Sarasa-Cabezuelo, and A. Andrés Belmonte, “The impact of artificial intelligence and big data on end-stage kidney disease treatments,” *Expert Syst. Appl.*, vol. 180, no. April, 2021, doi: 10.1016/j.eswa.2021.115076.

[4] A. S. Albahri *et al.*, “A systematic review of trustworthy and explainable artificial intelligence in healthcare: Assessment of quality, bias risk, and data fusion,” *Inf. Fusion*, vol. 96, no. March, pp. 156–191, 2023, doi: 10.1016/j.inffus.2023.03.008.

[5] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, “A systematic review of IoT in healthcare: Applications, techniques, and trends,” *J. Netw. Comput. Appl.*, vol. 192, no. January, p. 103164, 2021, doi: 10.1016/j.jnca.2021.103164.

[6] M. M. Yaqoob *et al.*, “Symmetry in Privacy-Based Healthcare: A Review of Skin Cancer Detection and Classification Using Federated Learning,” *Symmetry (Basel).*, vol. 15, no. 7, 2023, doi: 10.3390/sym15071369.

[7] J. Xu, J. Lin, W. Liang, and K. C. Li, “Privacy preserving personalized blockchain reliability prediction via federated learning in IoT environments,” *Cluster Comput.*, vol. 25, no. 4, pp. 2515–2526, 2022, doi: 10.1007/s10586-021-03399-w.

[8] B. Yuan, S. Ge, and W. Xing, “A Federated Learning Framework for Healthcare IoT devices,” vol. 1, 2020, [Online]. Available: http://arxiv.org/abs/2005.05083.

[9] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, “Handling Privacy-Sensitive Medical Data With Federated Learning: Challenges and Future Directions,” *IEEE J. Biomed. Heal. Informatics*, vol. 27, no. 2, pp. 790–803, 2023, doi: 10.1109/JBHI.2022.3185673.

[10] X. Gu, F. Sabrina, Z. Fan, and S. Sohail, “A Review of Privacy Enhancement Methods for Federated Learning in Healthcare Systems,” *Int. J. Environ. Res. Public Health*, vol. 20, no. 15, 2023, doi: 10.3390/ijerph20156539.

[11] H. Ku, W. Susilo, Y. Zhang, W. Liu, and M. Zhang, “Privacy-Preserving federated learning in medical diagnosis with homomorphic re-Encryption,” *Comput. Stand. Interfaces*, vol. 80, p. 103583, 2022, doi: https://doi.org/10.1016/j.csi.2021.103583.

[12] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. Alabdulatif, “A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data,” *Comput. Biol. Med.*, vol. 167, p. 107630, 2023, doi: https://doi.org/10.1016/j.compbiomed.2023.107630.

[13] M. Akter, N. Moustafa, T. Lynar, and I. Razzak, “Edge Intelligence: Federated Learning-Based Privacy Protection Framework for Smart Healthcare Systems,” *IEEE J. Biomed. Heal. Informatics*, vol. 26, no. 12, pp. 5805–5816, 2022, doi: 10.1109/JBHI.2022.3192648.

[14] S. Bebortta, S. S. Tripathy, S. Basheer, and C. L. Chowdhary, “FedEHR: A Federated Learning Approach towards the Prediction of Heart Diseases in IoT-Based Electronic Health Records,” *Diagnostics*, vol. 13, no. 20, 2023, doi: 10.3390/diagnostics13203166.

[15] M. Butt *et al.*, “A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications,” *Electron.*, vol. 12, no. 19, pp. 1–19, 2023, doi: 10.3390/electronics12194074.

[16] Y. S. Can and C. Ersoy, “Privacy-preserving Federated Deep Learning for Wearable IoT-based Biomedical Monitoring,” *ACM Trans. Internet Technol.*, vol. 21, no. 1, 2021, doi: 10.1145/3428152.

[17] H. Elayan, M. Aloqaily, and M. Guizani, “Sustainability of Healthcare Data Analysis IoT-Based Systems Using Deep Federated Learning,” *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7338–7346, 2022, doi: 10.1109/JIOT.2021.3103635.

[18] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, “Efficient and Privacy-Enhanced Federated Learning for Industrial Artificial Intelligence,” *IEEE Trans. Ind. Informatics*, vol. 16, no. 10, pp. 6532–6542, 2020, doi: 10.1109/TII.2019.2945367.

[19] Mondal , D. (2021). Green Channel Roi Estimation in The Ovarian Diseases Classification with The Machine Learning Model . Machine Learning Applications in Engineering Education and Management, 1(1), 07–12.

[20] Khatri, K. ., & Sharma, D. A. . (2020). ECG Signal Analysis for Heart Disease Detection Based on Sensor Data Analysis with Signal Processing by Deep Learning Architectures. Research Journal of Computer Systems and Engineering, 1(1), 06–10. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/11

[21] Susanti , M. ., & Kreshna Reza, H. . (2023). A Bibliometric and Visualized Analysis of Digital Payment 2019-2021. International Journal of Intelligent Systems and Applications in Engineering, 11(2), 112–118. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2601

[22] J. Li *et al.*, “A Federated Learning Based Privacy-Preserving Smart Healthcare System,” *IEEE Trans. Ind. Informatics*, vol. 18, no. 3, pp. 2021–2031, 2022, doi: 10.1109/TII.2021.3098010.

[23] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, “A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology,” *Futur. Gener. Comput. Syst.*, vol. 129, pp. 380–388, 2022, doi: https://doi.org/10.1016/j.future.2021.11.028.

[24] N. N. Thilakarathne *et al.*, “Federated Learning for Privacy-Preserved Medical Internet of Things,” *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 157–172, 2022, doi: 10.32604/iasc.2022.023763.

[25] R. Wang, J. Lai, Z. Zhang, X. Li, P. Vijayakumar, and M. Karuppiah, “Privacy-Preserving Federated Learning for Internet of Medical Things Under Edge Computing,” *IEEE J. Biomed. Heal. Informatics*, vol. 27, no. 2, pp. 854–865, 2023, doi: 10.1109/JBHI.2022.3157725.

[26] S. Wassan *et al.*, “Gradient Boosting for Health IoT Federated Learning,” *Sustain.*, vol. 14, no. 24, 2022, doi: 10.3390/su142416842.

[27] M. M. Yaqoob *et al.*, “Modified Artificial Bee Colony Based Feature Optimized Federated Learning for Heart Disease Diagnosis in Healthcare,” *Appl. Sci.*, vol. 12, no. 23, 2022, doi: 10.3390/app122312080.

[28] 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 Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2864–2880, 2023, doi: 10.1109/TNSE.2022.3185327.

[29] X. Zheng *et al.*, “Mobile Edge Computing Enabled Efficient Communication Based on Federated Learning in Internet of Medical Things,” *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/4410894.

[30] MD. REDWAN KARIM SONY, “UCI Heart Disease Data,” *Kaggle*. 2021, [Online]. Available: https://www.kaggle.com/datasets/redwankarimsony/heart-disease-data.