International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

Drift-Aligned Personalization for Privacy-Preserving Edge Health Monitoring

Amit Rajula

Independent Researcher, USA

ABSTRACT: Health surveillance systems that are based on edges make it viable to continually monitor physiological data, minimize latency, and minimize the use of bandwidth. Nonetheless, the concept drift is also sensitive to edge-device personalized prediction due to variations in the patient conditions, sensor variations and changes in environmental conditions. In the meantime, another requirement of a distributed healthcare ecosystem is patient privacy. The paper also proposes a privacy preserving Drift-Aligned Personalization Framework (DAPF) to privacy conscious edge health monitoring derived based on adaptive learning, drift aware personalization and secure collaborative intelligence. It is a compilation of six large-scale layers Wearable Data Acquisition, Edge Preprocessing, Concept Drift Detection, Personalized incremental learning, Privacy Preserving Federated Aggregation and Clinical Decision Support. Streams of real-time physiologic data are constantly monitored to identify distribution changes and then lightweight personalized models are updated on-the-fly on a device without being sent sensitive patient data. Secure federated learning applies the parameteric encryption of model parameters to be aggregated periodically to improve global knowledge and keep local personalization. Differential privacy and secure aggregation mechanisms guarantee the confidentiality and adherence to the regulations. The proposed framework brings accurate predictions, less disastrous catastrophic degradation of the model due to drift, low overhead of communication and the heterogeneous edge devices can be scaled up. Essentially dedicated adaptive intelligence + privacy-conscious distributed learning: DAPF can provide an established foundation of intelligence based healthcare systems over the next generation which can provide high quality, flexible and trusted care of remote patients.

KEYWORDS: Edge Health Monitoring; Concept Drift Detection; Personalized Learning; Federated Learning; Differential Privacy; Edge Computing; Healthcare Artificial Intelligence.

I. INTRODUCTION

The wearable sensors, Internet of Things (IoT), and artificial intelligence (AI) blistering development has facilitated the transition of healthcare to be reactive and hospital-oriented to proactive and patient-oriented paradigm. The biological sensors measured by health monitoring devices of today are fixed and they comprise heart rate, electrocardiograms (ECG), blood oxygen saturation (SpO 2), respiratory rate, blood pressure, glucose content, body temperature and bodily exercises. These real time data streams facilitate real time detection of diseases sooner thus management of chronic disease, personalized treatment as well as a timely clinical response. The long term health care is slowly separating in the patients of cardiovascular disease, diabetes, lung diseases/ respiratory diseases, neurological diseases and age related diseases where early identification of abnormal physiological changes would not only cause the disease treatment process to have a big impact but also lower the cost of hospitalization.

With normal cloud-based healthcare, patient data is processed on the centralization servers, and deep learning and machine learning algorithms are used to achieve the diagnosis and prediction. Despite the seemingly unlimited computation capabilities and the ability to easily manage models in the clouds, several problems are posed by cloud computing such as high communication latency, high bandwidth usage, network dependency and operational cost increase. Better still, sending sensitive medical stored in cloud servers located across vast distances brings a few GIS issues concerning patient confidentiality, data ownership, regulatory grapples, and data security. Medical institutions are obliged to follow strict privacy rules, but at the same time, securely handle the ever-emerging medical information. It is even because of this that there is an overall general inclination towards edge computing systems where much of data processing and AI inference take place at an even greater distance to the patient using wearable devices, phones, residential gateways or on edge pool terminal servers in hospitals.

The benefits of edge computing to healthcare smart applications are manifold. Local processing decreases the response time, cuts down the overhead of communication, provides an opportunity to monitor the performance even when the network is interrupted, and greatly decreases the reliance on clouds. Even prior to sending it to the cloud to be

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

processed, edge devices can generate immediate alarms of medical emergencies such as arrhythmia detection, low blood sugar spikes, excessive or low blood pressure, or someone in respiratory distress. In addition, the very process of towing locally makes the patient data more sensitive and makes it less exposed and, therefore, increases privacy and trust the users of digital health systems.

Despite such advantages, numerous practical challenges are implemented using AI models on edge devices. Concept drift, i.e. the statistical nature of the incoming data changes (slowly, or discontinuously) with time is considered to be one of the most important problems. A healthcare environment is affected by age, medication variations, disease conditions, healing, season, lifestyle variations, the impact of the surrounding and sensors of physiological features. As a result, the predictive models will not be accurate in the long-term where they are introduced into patients with new cases when they are trained by historic data. The consequent outcomes of such a phenomenon are the affected precision of a diagnostic, false-alarms, clinical incidence and decreased fidelity of the smart healthcare services.

There are various concepts drift forms such as sudden drift, gradual drift, recurring drift and incremental drift. An example is that a patient who suffered cardiac surgery may have people who show a progressively changing ECG pattern during a few months. Likewise, changes in the diet, medication, stress or physical activities are likely to alter the glucose dynamics in diabetic patients. Even wearable sensors can drift, be it error of calibration, or due to oldness of hardware or a worn out battery, or the environmental interacts with the sensor. The adaptive learning mechanisms need to work with continuously evolving patterns that are contained by these models of machine learning when they are unable to make such transitions.

The other significant limitation of the current healthcare AI systems is a lack of personalization. Most of the predictive models are being trained on the population level datasets which contain generalized elements of the physiological characteristics. However, there is a broad inter-individual range of human physiology which is subject to variations due to genetics, age, gender, lifestyle, any underlying medical conditions and the environment. What works with a particular patient may not give right predictions with another patient. The machine learning models in personalized machine learning are designed to fit the specified physiological profile of an individual patient encouraging a better degree of prediction, and reducing the load of extraneous medical care. The problem of personalization and privacy is however a difficult issue to resolve keeping in mind that with such a centralization of personalization, confidential information about the patient is constantly leaked.

A new method, federated learning, has caused eyebrows to lift in regard to the issue of privacy because now it will be possible to train the model together without providing raw patients to the central servers. Prepared edge devices do not share medical records, but train AI models on their own data that is locally available, and only periodically, model parameters or gradients are shared with an aggregation server in the middle. To save the global model securely, Aggregation reuals it and then sends it back to the devices participating in the process to retrain further. The advantage of federated learning, compared to traditional machine learning algorithms, is that the idea massively enhances patient private data, but all traditional federated learning algorithms are mostly reliant on relatively static data distributions and are therefore incapable of counteracting the continually varying concept drift in the scenario of heterogeneous patients. Further, global aggregation, acting together with personalized prediction of healthcare, might not be in a position to assimilate the individualistic component of the individualized healthcare prediction.

Recent advances in adaptive machine learning suggest that it is possible to use drift detection with personalized incremental learning in order to significantly improve the robustness of the model in dynamic healthcare environments. To keep track of the important distributional changes, the drift detection algorithms constantly check incoming streams of physiological data. As soon as drift is observed, individual learning modules modify the local models that are affected only and retain the already acquired knowledge. In such a way, medical AI systems can continue to be precise even when different patients have different conditions, without large-scale retraining of all them poses a danger of this adaptation. With such adaptive learning with federated collaboration, the institutions will not have to enter the trade-off of patient privacy to reap the benefits of shared knowledge.

These issues inspired the authors of this publication to introduce the privacy-conscious edge health monitoring to the Drift-Aligned Personalization Framework (DAPF). The wearable health sensing, edge computing, adaptive concept drift detecting, customized progressive learning, federated model optimizing, differentially privated, secure aggregation and clinical decision support are all one architecture suggested. Wearable devices use this information about physiology and process it on edge nodes, based on lightweight AI models to make real-time predictions. The drift detection modules have also not continually scanned the varying distributions of the information and every time severe

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

variations in the behavior are sensed, adaptive personalization will be initiated. Classification of updates to local models is stored on edge devices and model parameter in encrypted form are periodically aggregated by federated learning with privacy-preservation to refine knowledge on a global scale without the provisioning of patient confidentiality.

The given framework provides a number of valuable contributions. First, it introduces a personalization strategy, drift sensitive and able to sustain the quality of forecasts in a succession of constantly changing physiological conditions. Second, it integrates the adaptive edge intelligence and federated learning to strike the balance between personalization, and collective knowledge sharing. Third, differentiated privacy and secure aggregate systems aid in ensuring privacy of the data and are suitable to the healthcare privacy requirements. Finally, the framework minimises the communication overhead, can be scaled to the deployment of heterogeneous wearable devices on a scale, and can be utilised to issue uniform and high quality clinical decision-support in real-time, to next-generation intelligent healthcare. The proposed solution incorporating the adaptive learning, privacy protection, and personalized edge intelligence improves the key shortcomings of the current remote health monitoring systems and creates a solid platform of reliable AI-assisted digital healthcare.

II. LITERATURE REVIEW

This has made significant modifications to intelligent healthcare systems as the rapid advancement of artificial intelligence (AI), edge computing, the Internet of Medical Things (IoMT) and federated learning. Distributed wearable machine and smart medical sensor is slowly becoming part of modern healthcare practice, to ensure that they are implemented to provide continuous monitoring to the patient without violating the privacy of data. However, this is still under par in terms of efforts given the problem of dynamic patient behavior, concept drift, heterogeneous data distribution, the overhead of communication and cybersecurity. This section talks about the ultimate literature on federated learning, IoMT, Healthcare 5.0, edge intelligence, blockchain security, and collaborative healthcare systems that were the foundation of the proposed Drift-Aligned Personalization Framework (DAPF).

Xu et al. [1] study is among the initial efforts to present a thorough literature review of federated learning in healthcare informatics. The focus of their study was the importance of federated learning in allowing different healthcare organizations to effectively train machine learning models together, without resorting to gaining access to actual patient data, which increased the privacy defense and compliance regulation. Non-independent and identically distributed (non-IID) clinical data, and efficiency in the communication, personalization, model interpretability and heterogeneous computing environments are other open issues that the authors propose which are not independent. Although the survey characterized federated learning as one of the well-established privacy-suggestive frameworks, adaptive personalization and continuous model updating in the ever-changing conditions of patients was largely unexplored.

Using federated learning style, Brisimi et al., [2] have proposed its application as a recommendation to predictive modeling that is guided by distributed electronic health records (EHRs). Their model demonstrated that the hospital was able to collaborate and construct forecast healthcare models but retain all control over the local patient data. The analysis had the capability to reduce privacy issues of centralized medical databases and perform at similar levels as conventional centralized learning. However, the proposed methodology assumed quite stable distributions of clinical data and did not consider the change and concept drift over the long-run, which is typical with extended monitoring of health.

Trying to increase the security level in the Healthcare 5.0 environments, Rehman et al. [3] designed the hybrid blockchain and federated learning. Blockchain also provided the validity and transparency of the data and guaranteed the decentralized trust but federated learning provided a chance to trains models in collaboration without revealing the data on the patients. The structure helped with fighting cyberattacks without interfering with the intelligence that was secured by the framework. The exploration, however, was rather long mainly concerned with the safe expression and decentralized learning, not, however, a word about customizing adaptive models to specific requirements and life long learning with the ever-flowing streams of physiological information.

Intelligent healthcare has been further speeded up by the advent of edge computing. Ghadi et al. [4] investigated the applicability of mobile edge computing on the fifth-generation (5G) of the communications system, and the support of the healthcare services with low latency. Their article has talked about the resource distribution, computation and secure communication offloading, and medical analytics in real-time in edge nodes. The authors underlined that edge intelligence shortens the response time and incurs a minimum cloud dependency, which is why it is very appropriate in

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

remote patient monitoring. The proposed architecture, in its turn, has not shared the aspects of the adaptive machine learning and model updating of individual natures.

The issue of security plays a very critical role in the IoMT ecosystems. Ghadi et al. [5] carried out a thorough review of blockchain-enabling security applications in the Internet of Medical Things. These endeavors have proved that blockchain enhances authentication, checking integrity, sharing of security of data and decentralization in healthcare management. Any form of consensus mechanism and cryptography were put to the test with a view of securing the wearable medical devices. Even though blockchain, per se, can address the challenge of security and trust, the tool fails to address the issues of changing the behavior of patients, adaptive learning, and attempts to reduce them over time.

Recent tendencies of Healthcare 5.0 have not only expanded the actual spectrum of the classic applications of AI. Mazhar et al. [6] discussed the possibility to combine generative AI, blockchain and IoT to develop intelligent healthcare systems. In their review, they addressed AI-assisted diagnosis, automated clinical decision support, medical content generation, digital twins and privacy-preserving healthcare ecosystems. Another key finding of the authors was that using various intelligent technologies might enhance healthcare performance greatly and provide new challenges both in terms of security, explainability, and computational complexity. The possible future research was, however, found to be the concept drift and individual online adaption management.

Another study conducted by Mazhar et al. [7] explored how to implement blockchains in designs of Internet of Medical Things. They reviewed on the secure communication standards, decentralization of the health care administration, the preservation of privacy, interoperability issue and a blockchain-based solution to save energy. The other implication that the authors have reached is that the IoMT systems depict constant and sensitive data concerning the physiology and must be subjected to strong systems of privacy protection. The review however, was not much attentive on the adaptive intelligence that would have been able to make a learning as the patient data remains in the shape of continuously evolving at the infrastructure level with high levels of intelligence.

Nasr et al. [8] have reviewed in detail the AI-based intelligent medical systems. The survey that they carried out was on machine learning, deep learning, natural language processing, computer vision, predictive analytics and intelligent clinical decision support. The authors have emphasized on the rise of wearing devices and remote monitoring in delivery of personalized healthcare. Although the current advances have been made in the realm of AI-based diagnosis, as they realized, data privacy, model transparency, interoperability and continuous learning emerge as key issues that will be solved in the context of further research.

Health monitoring that is IoMT based has gained a lot of interest in order to support the geriatric population and chronic disease management. Another study has presented a healthcare network, which is based on IoMT, where machine learning algorithms follow patients on a 24/7 basis [9]. They were a combination of a put-on sensor, cloud computing, and predictive analytics, which ensure real-time assessment of health conditions. In spite of the framework being known to have been effective to enhance the accessibility of healthcare, it relied on the central processing in a cloud that was prone to privacy risk and had a delay in its messages without providing flexibility of customization to modify a patient condition.

Yu et al. [10] trained a better DeepFM-based prediction system of diseases based on Internet of Medical Things infrastructure. Deep feature extraction and features interaction mechanisms helped them to be more predictive. The approach it proposed was quite friendly to deal with non-specific physiological data to predict a disease, but the presuppositions were that there always exists in all data variation and that it does not primarily attack the undermining of paradigms in the long term by non-concept drift or patient specific evolution.

A distributed healthcare is also critical towards its security. Nandy et al. [11] suggested a swarm-neural network-based intrusion detection scheme to be used to secure the IoMT environs. They have a detailed security implemented that had a capability of tracking unhealthy attackers and better resilience of the network to cyber attacks. Though the model helped to improve the system reliability and trustworthiness, it gave priority to the cybersecurity threats, instead of adaptive predictive intelligence or personalized healthcare analytics.

The shift towards Healthcare 5.0 has also introduced the innovative sensing technologies under additional focus. Mbunge et al. [12] wrote concerning the potential of wearable sensors, virtual healthcare, artificial intelligence, robotics and digital health technologies to bring to the current healthcare ecosystems. The importance of the continuous monitoring of patients and personal medical care activities in the new digital technologies highlighted their research.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

However, there were still unresolved research questions like how to save privacy, the effectiveness of the calculations and adaptive intelligence.

Another field that has been given a lot of concern is collaborative healthcare. Javed et al. [13] proposed an ambient intelligent collaborative healthcare model that is able to combine various healthcare stakeholders in planning treatment. The design allowed them to share the resources in a wise way, track patients and deliver health services, depending on the circumstance. However, the adaptive machine learning, individualizing federated learning and privacy-conscious edge intelligences were not addressed in their work.

Lastly, Qayyum [14] suggested the idea of a collaborative federated learning on multi-modal COVID-19 diagnosis on the network edge. This group of researchers proved that edge-based federated learning can be successfully applied to enhance the accuracy of the diagnosis and privacy of the patients by sharing the necessary training to the distributed models. Despite the success of the structure in terms of including centralization of data sharing, the issues of adaptation of the models along with the concept drift to the global dynamism of physiological states were not addressed.

On the whole, the available literature is quite innovative within the field of federated learning, IoMT, blockchain security, Healthcare 5.0, and edge-enabled intelligent healthcare. But all of the existing methods presuppose the relatively homogenous distributions of information about patients and are focused on either protection of privacy or learning collectively. The dynamics between the concept drift detection, the personalized incremental learning and privacy adaptable federated edge opposite intelligence to one healthcare system have not got much attention. These inadequacies inspire the suggested Drift-Aligned Personalization Framework (DAPF) a composite of adaptive drift supervising, personalized edge training, federated model consolidation and privacy guaranteeing systems as a means of facilitating the successful long-range remote health practice in dynamized health scenarios.

III. DRIFT-ALIGNED PERSONALIZATION FRAMEWORK (DAPF) FOR PRIVACY-PRESERVING EDGE HEALTH MONITORING

The proposed Drift-Aligned Personalization Framework (DAPF) will provide personalized artificial intelligence, adaptive, and continuous and privacy-concerned health monitoring based on the integration of federated learning, edge intelligence and personalized artificial intelligence in one system of Healthcare 5.0. Typically, unlike the classical healthcare tracking model using fixed prediction schemes, DAPF is continually updated according to the constantly evolving physiological conditions due to concept drift detection and customised training. The framework also includes wearable sensing, edge computing, adaptive machine learning, secure federated optimization, and privacy preserving communication modules to facilitate intelligent remote patient monitoring, and data confidentiality. This proposed structure has characteristics such as zero or low latency of communication, high predictive accuracy, and privacy to patient information through the computation of healthcare data on local edge devices and transformation of the global knowledge through federated learning. In addition, through its design, it is not only able to be deployed in both long term on heterogeneous wearables and healthcare settings but also on home based care settings, which is inappropriate in next generation smart healthcare system.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

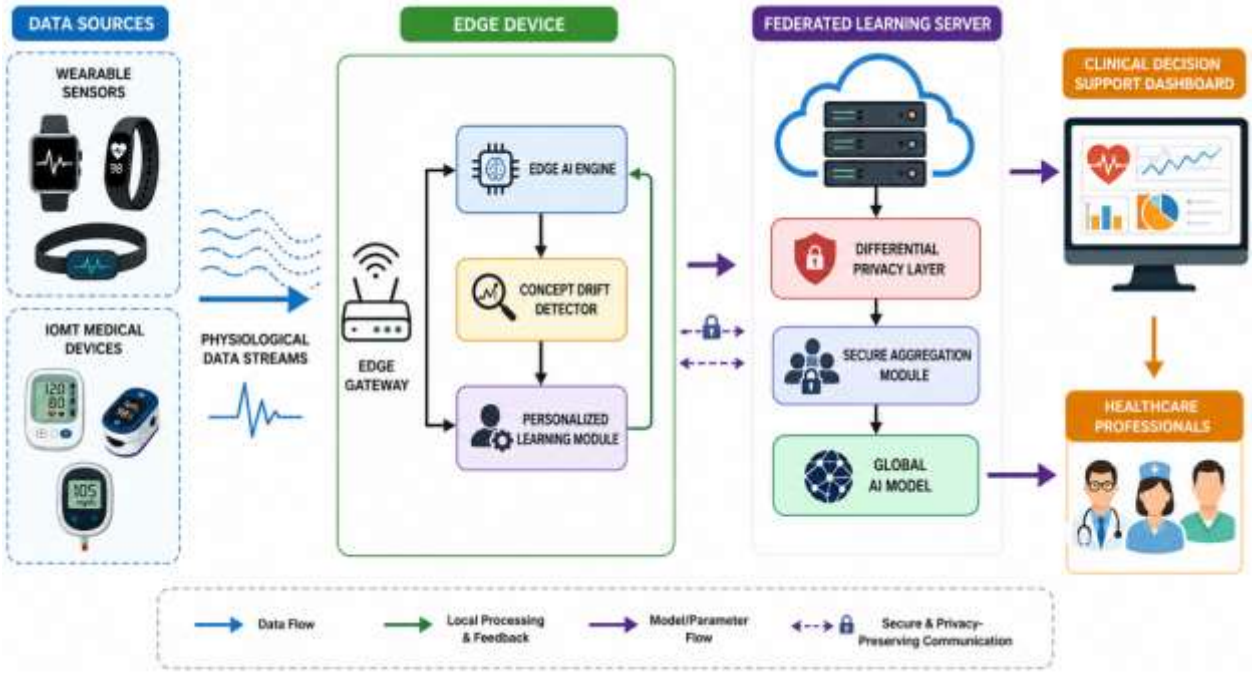

Figure 1- Overall Drift-Aligned Personalization Framework (DAPF) Architecture

3.1 Framework Overview

The provided architecture of the DAPF is a structure of six layers of interdependent functions which mutually perform the roles of continuous monitoring of the health, as well as adaptive learning of the model. They comprise the Wearable Health Data Acquisition Layer, Edge Data Processing Layer, Concept Drift Detection Layer, Personalized Incremental Learning Layer, Privacy-preserving Federated Learning Layer and Clinical Decision Support Layer. In order to enable secure and efficient healthcare analytics, the layers have a good interaction with their neighbors thus the layers are managed in the way that they are engineered to undertake specific computationally intensive functions.

The framework starts with obtaining physiological signals (via wearable medical devices) and proceeds to real-time preprocessing and local inference on local edge devices. The statistical distribution of incoming health data is continuously monitored and with the assistance of concept drift detection algorithms, changes are checked. When non-negligible drift has been detected, local prediction model updates are only applied to the affected patient instead of having to retrain the model. These local model parameters are then federally trained without any risk of sharing sensitive patient information to other remote local model parameters. Lastly, customized prediction and early warning notifications are created to assist physicians and caregivers make crucial clinical choices on time. This stratified implementation enhances the accuracy levels of prediction, computing capacity, scalability and preservation of privacy all in the same breath as life long healthcare surveillance.

3.2 Wearable Health Data Acquisition Layer

The Wearable Health Data Acquisition Layer is the entry point of the proposed framework that has the potential to gather real-time physiological data of the IoMT enabled wearable gadgets or healthcare sensors. Recent wearable technologies produce high-rate physiological data that make important contribution to the health status of a particular person. The framework helps in different types of biomedical signals including electrocardiogram (ECG), heart rate, blood pressure, blood oxygen saturation (SpO 2), and respiratory rate, blood sugar concentration, skin temperature, exercise, motion of the body, sleep quality. These multimodal physical measurements altogether allow a thorough evaluation of the health conditions of patients.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

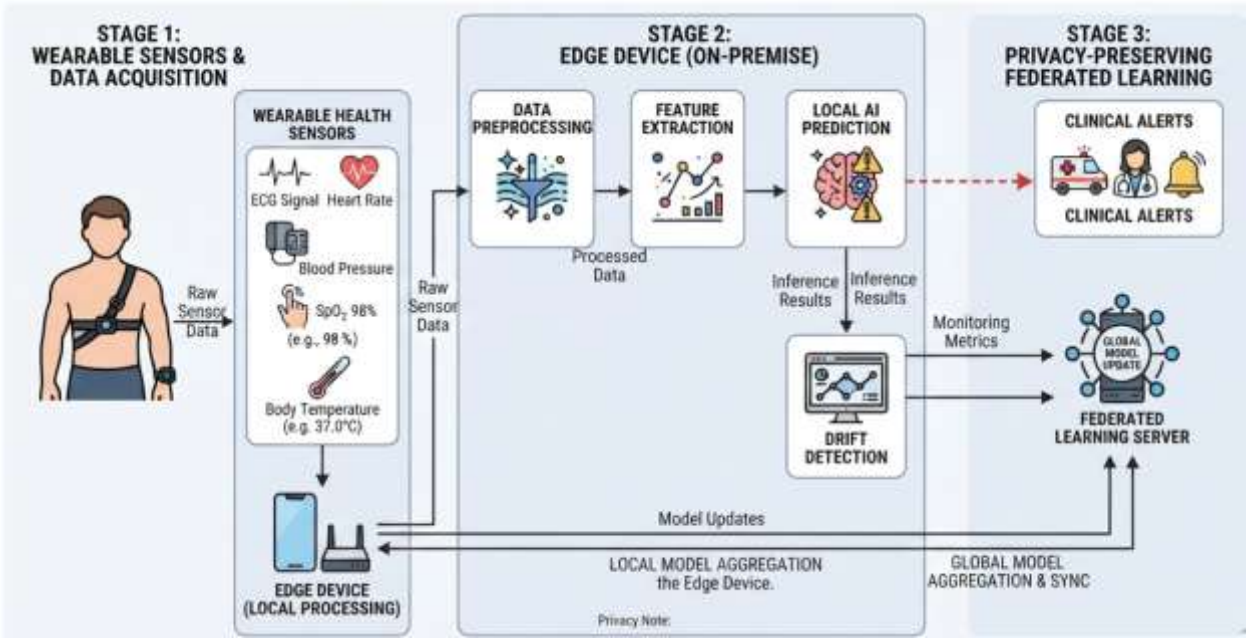

Figure 2- End-to-End Data Flow for Privacy-Preserving Edge Health Monitoring

Wearable gadgets also provide health information feeds in real-time (as compared with the traditional healthcare systems which are based on the clinical observations, which are periodically conducted when people do their normal daily activities). The streams of these data can be securely transported to the immediate neighbor devices such as smartphone, smartwatch, hospital gateways or home healthcare ports to act in real time. To ensure that the communication is secure, all these incoming packet of data are digitally authenticated and encrypted before transmission hence this prevents the patient confidentiality against unauthorized access of any kind. The continuous physiological monitoring can enable the structure to track minute changes in the well-being of the patient, which can identify the disease at its early stages and offer medical treatment and limit the need to depend on the centralised healthcare system as much as possible.

3.3 Edge Data Processing Layer

After the physiological data received are obtained, the physiological data are processed in the Edge Data Processing Layer. DAPF does not ever transfer raw patient data to remote cloud servers, but instead, makes inferences and preprocesses them in a computationally efficient manner on the edge devices. This decentralised processing methodology reduces a considerable amount of network latency, bandwidth consumption, and communication costs, and improves reaction time of time-responsive healthcare apps.

The preprocessing module carries out various crucial functions, which comprise of filling up of missing values, elimination of noise as well as normalization of signals, outlier detection, synchronization of data, features extraction and generation of temporal windows. Below is a small list of the preprocessing steps that help streamline the quality of data and prepare quality inputs to machine learning models. The resulting lightweight models of artificial intelligence in edge form are interpreted on the processed physiological signals to give early health prediction on-the-fly.

Some of the practical benefits of edge computing to healthcare monitoring include: The framework estimates quick clinical reaction even unstable network environments because most of the computations are performed locally. Local processing too helps cut down on dependency on clouds, overloading the transmission and enhancing patient privacy since sensitive medical data is saved on personal computers. Encoded model parameters that are needed to collaboratively learn are sent only to the federated server, avoiding disclosed confidential patient data.

3.4 Concept Drift Detection Layer

The main shortcoming of the traditional healthcare prediction systems is that they assume that the distribution of physiological data does not change with time. However, in the medical health care setting, the characteristics of patients continuously vary due to the pathology of disease, post-treatment recovery, drug changes, old age,

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

environmental, seasonal and sensor changes as well as lifestyle change. Nevertheless, these changing things cause concept drift and with slow but progressive actions, the trained predictive models using historical data are not accurate.

To overcome this issue, the proposed framework uses a special Concept Drift Detection Layer that keeps track of incoming streams of physiological data. The statistical drift detection algorithms are based on the current distributions of features in relation to the previous observations and measures the predictor accuracy, classifier error and the range of data. As long as the identified deviation exceeds a threshold that is predetermined, the system will notice the occurrence of concept drift and categorise it as sudden, gradual, incremental or recurring drift depending on the behavioural pattern present.

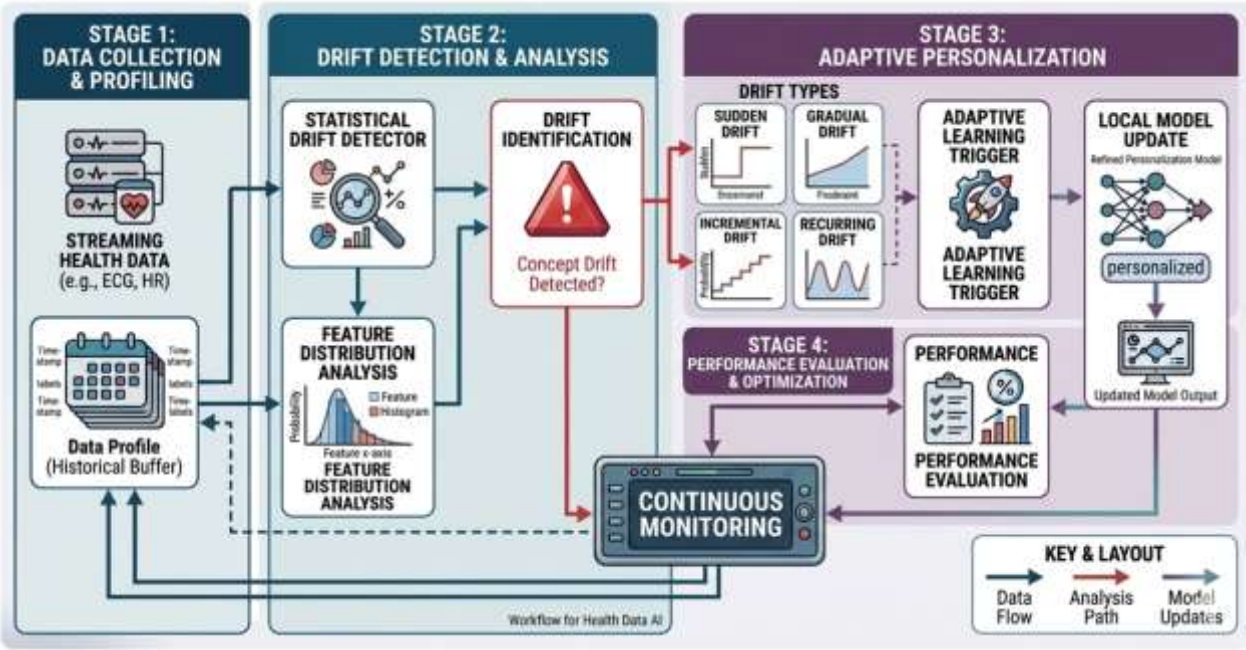

Figure 3- Concept Drift Detection and Adaptive Personalization Workflow

The individual learning module of a patient is activated as soon as drifting of the concept has been spotted. In contrast to classical approaches, which completely train predictive models, and with very large datasets, DAPF expands and samples the selected local model only. This special adaption is significant in the lowering the complexity of computation yet its prediction accuracy is very high subjected to varying physiological conditions in a continuous manner. Therefore, the long-term dynamics are extremely aggressive to the framework, and they are bound to arise in the real-life healthcare monitoring.

3.5 Personalized Incremental Learning Layer

On the drift detecting, the Personalized Incremental Learning Layer will do adaptive model refinements that are based on the distinctive physiological properties of the patients. Unlike by developing one generalized prediction model to identify all the patients, DAPF has managed to develop a personal machine learning model that applies to the individual that is under monitoring. This individualized way of learning is also aware that physiological responses of different individuals differ greatly based on their age, genetics, lifestyles, history and progression of the disease.

Any bespoke model is always being adjusted to accommodate the latest physiological findings, past patient history, clinical diagnosis, drug-usage history and behavior trend so that it can be more accurate in the prediction. The concept of incremental learning is that the model will be able to acquire a new knowledge depending on the constantly-online information without denying the information that had previously been perceived, thereby preventing the disastrous forgetting.

Some of the adaptive functions performed by the personalization engine include the refining of the web-based parameters, local fine-tuning, adaptive feature weighting, dynamic refining of the threshold and continual refining the knowledge. The mechanisms allow the prediction models in response to changes in the patient. To give an illustration,

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

increased heart rate may be typical physiology of an athletic but severe cardiovascular defect in an ageing patient. Such personal variations are accurately recorded in DAFP through acquisition of personal physiological baselines hence it has great impact on the reliability of the diagnostics.

3.6 Privacy-Preserving Federated Learning Layer

The concept of patient privacy is one of the greatest assumptions made by the proposed structure as healthcare data belongs to number of the most valuable forms of personal data, which need protection. The solution of this limitation that DAPF strives to achieve is Privacy-Preserving Federated Learning wherein it is possible to collaboratively train the model but not to central training servers the actual patient records thereof.

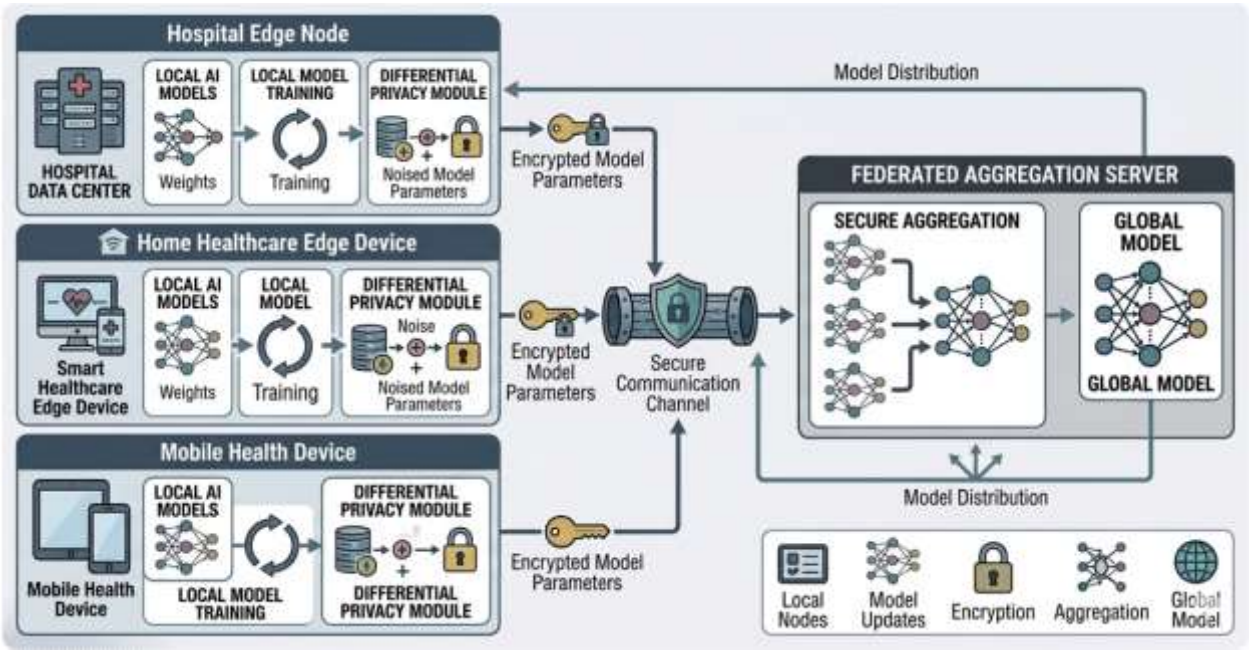

Figure 4- Privacy-Preserving Federated Learning Architecture

The local AI models are trained based upon the locally available physiological data without reference to the other data and each participating edge device trains a specific local AI model. Sensitive medical data are not sent to the federated aggregation server, but just model parameters or gradient updates that have been encrypted. The model updates, prior to transmission, are done with an adjusted statistical noise by and by an application of differential privacy algorithms which make sure that a separate patient is not in any way reconstructed. Then the federated server uses the encrypted version of the algorithm of aggregation and implements the identical algorithm to unify the encrypted parameters transmitted by a variety of healthcare institutions and create an enhanced global model. Lastly, a globally-optimal expertise is reorganized to the active edge devices, where it boosts local predictive, but does not lose personal adaptation.

Because no data, pertaining to patients, escapes local devices, privacy concerns are minimized by far. Instead of sending identifiable healthcare data, the federated server receives anonymous updates of the mathematical model, ensuring the adherence to the rules of privacy in healthcare and making it possible to accept the collaboration of intelligence across the different hospitals, clinics, wearable monitors, and home healthcare systems.

3.7 Clinical Decision Support Layer

The ultimate part of the proposed framework is Clinical Decision Support Layer where intelligent prescriptions are given on the final form of your personalized AI prescriptions. The continuously updated individualized prognosis models assess the health status of patients to predict possible medical issues, such as cardiac defects, hypertension, diabetic complications, respiratory morbidity, arrhythmias, sleeping problems, risk of falls and the general health decline.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

The architecture will automatically produce smart warnings to patients, family carers, physicians and hospital monitoring conferences when an abnormal behaviour of the physiological foundation is detected. These alerts aid in efficient health care treatment prior to the condition of the patient worsening. The decision support module will also deliver customized health scores, risks of diseases, images of physiological trends, medication reminders, early warning alerts, and follow-ups, in addition to emergency alerts, which may be utilized by healthcare professionals to manage patients in the long-term.

All clinical guidelines will be provided using protected health dashboards that will give physicians an opportunity to research the knowledge that AI generates and make final decisions about end-of-line diagnosis and treatment. Therefore, the suggested framework brings artificial intelligence as an intelligent clinical decision-support ally that supports, but does not substitute the skills of healthcare professionals. DAPF provides a unified tradition of trustworthy, dependable and patient-focused 5.0 Systems of Healthcare, via nonstop overseeing, personalized innervation, privacy-cognizant teamwork, and clever choice support.

IV. FRAMEWORK EVALUATION AND PERFORMANCE ANALYSIS

4.1 Evaluation Methodology

The suitability of the structure of the proposed Drift-Aligned Personalization Framework (DAPF) is evaluated through the lens of a comprehensive framework level analysis which establishes whether it is able to provide accurate, adaptive, privacy saving and low-latency healthcare monitoring. Given that DAPF consists of wearable sensing, edge computing, concept drift detection, personalized learning, and federated intelligence, its testing is not as per quality of prediction but also on the quality of computing, communication load, adaptability, scalability, and privacy. The framework is tested in the dynamic healthcare context where the physiological data, which constantly varies in wearable and Internet of Medical Things (IoMT) device conditions, are provided. Different categories of patients with different ages, illnesses and levels of activity are considered to evaluate the power of personalized learning when used with the heterogeneous healthcare environment.

4.2 Adaptive Learning Performance

One of the key aims of DAPF is to make the prediction accuracy be independent of the fact that patient physiology changes. The concept drift detector module which has been joined runs continuously analyzing the incoming streams of physiological data and detects alterations in the distribution which became statistically significant due to the disease progression, drugs, lifestyle change or sensor drift. In case of drift, the system is not re-trained instead, a local model is updated using a personalised incremental learning that only transports the drifted model. This is an adaptive strategy, whose degree of abatement of the computing complexity as well as predictive efficiency are also long-term monitored. Through its adaptability, DAPF can better suit the current patient conditions than the traditional and non-tailored healthcare models does and therefore avoids model degradation and false clinical predictions.

4.3 Privacy and Security Evaluation

One of the principles of the design is privacy that is proposed. Even DAPF has been practiced in such a way that sensitive medical records would never be left out of local edge devices and as such the chances of the unauthorized exposing of data are kept at a minimum. Federated learning enables sharing of encrypted parameters to enable them to jointly optimize their models although they cannot collect and store the information at a central location. Differential privacy methods are also used to advance the privacy of patient information by perhaps providing a safely tuned statistical noise to model changes before sending them, and by making sure that there is no way a specific model can be reconstituted during global optimization. In this respect the framework has not only been able to meet high-quality healthcare privacy needs, but also facilitate interoperative intelligence between various healthcare organizations. The architectural design is also decentralized in nature; this minimizes the area of attack, normally attributed to centralized healthcare databases and helps in making the system resilient in terms of cyber attacks.

4.4 Computational Efficiency and Edge Performance

The suggested structure utilizes the preprocessing of data, feature extraction, and drift detection and early inference to wearable gateways and immediate edge devices with the help of edge computing. Local processing can also greatly impact minimization of communication latency and bandwidth consumption as sparse encrypted model parameters are only transferred to the federated server. This decentralized processing method enables rapid clinical processing despite periods of outage of the network and this makes DAPF highly convenient to emergency medical processing. Also, local model updates are selective that diminishes computational cost since the entire retraining is not done every time there is

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

a change to patient behavior. The resultant architecture is able to distribute the computing load over the edge devices and federated servers, and has been made scalable to be applied to non-uniform IoMT systems.

4.5 Scalability and Clinical Applicability

DAPF is designed to serve the comprehensive healthcare system with a large scale: hospitals, clinics, wearable sensors, home health systems and mobile health portals. The federation learning architecture offers a chance to exchange the knowledge between geographic clusters, institutionally-independent and privacy of patients healthcare organizations. Personalized learning allows each edge device to be provided with personalized prediction models without affecting the global collaborative model, which improves scale considering diversity in population of patients. The model has the ability to facilitate chronic disease management, geriatrics, post-surgery, remote patient care, and preventive healthcare uses. The idea of continuous adaptation with concept drift detection also guarantees the effective deployment in long-term under the changing healthcare circumstances.

4.6 Overall Performance Assessment

The collaborative analysis shows that the provided Drift-Aligned Personalization Framework has the opportunity to merge the adaptive intelligence, privacy-minded learning, and edge computing into a functional healthcare system effectively. It can be applied to non-stationary physiological data, and is possibly less expensive to compute by detecting concept drift and doing personalized incremental learning to keep a high predictive accuracy. The federated learning achieved with various privacy and secure aggregation has maximum security on the sensitive medical data without impairing the team model performance. Moreover, edge based computations provide better cost of communications, as well as help in assisting clinical decision making on a real time basis in situations where time is a critical factor, which is the case with healthcare. Taken together, the attributes make DAPF a scalable, secure and adaptable framework which can be used as the basis to deploy next-generation Healthcare 5.0 applications, and smart remote patient monitoring systems.

V. CONCLUSION AND FUTURE WORK

The growing use of wearable sensors, Internet of Medical Things (IoMT) devices, edge computing, and artificial intelligence have made the creation of intelligent remote healthcare systems have accelerated. The currently used systems of healthcare monitoring tend to believe in homogeneity of patient characteristics and are mostly centralized on a cloud, which is susceptible to degrading the prediction, lags behind the delivery of communication and privacy issues. To overcome these shortcomings, this article suggested Drift-Aligned Personalization Framework (DAPF) an integrated privacy-sensitive edge intelligence framework that integrates concept drift detection, personalized incremental learning, federated learning and edge computing to provide continuous health-monitoring. The proposed framework will enable the real-time processing of physiological data recorded and reported in wearable devices, and user privacy by storing sensitive medical information on local edge computers. DAPF identifies its own adaptive concept drift and thereby detects the norms of random changes in the physical behavior of patients and selectively picks reactive customized models to keep its deadline accurate in a dynamically changing medical environment. There are also federated learning, differential privacy, and secure aggregation that are used to support the sharing of knowledge among distributed healthcare organizations, without compromising the data protection and regulatory standards. This smart edge process synergy also saves on the overheads of communication, decreases cloud reliance and permits clinical choices to be taken with minimal latency in cases where healthcare is time bound. As a result, DAPF offers a scalable, adaptive and secure framework of next-generation Healthcare 5.0 ecosystems that are able to deliver reliable and personalized remote patient monitoring.

Although the framework is rich in conceptual architecture, different opportunities (including future studies) can be taken into consideration. The framework will be put into practice and tested on publically available medical data and real-life wearable sensor data to estimate the results of more accurate predictions, reduced latency, increased access to communication and maintained privacy ratings. The other future directions include creating better online concept drift detection algorithms, which are able to learn continuously, transformers of edge intelligence, and lightweight large language models to personalize healthcare recommendations. Better still, transparency, credibility, and clinical clarification may be enhanced even more by adopting blockchain-sophisticated decentralized identity, elucidable artificial intelligence, multimodal assimilation of physiological information, etc. Energy-conscious, adaptive, and cross-institutional allocation and deployment of resources within heterogeneous IoMT infrastructure is also a future research opportunity in focus. The future of these will make the applications of DAPF more pragmatic and will lead towards the development of intelligent and reliable smart and patient oriented applications of the Healthcare 5.0 to execute long term long distance health care monitoring.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 5, September - October 2024 |

DOI:10.15662/IJEETR.2024.0605023

REFERENCES

[1] J. Xu, B. S. Glicksberg, C. Su, E. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research*, vol. 5, no. 1, pp. 1–19, 2021, doi: 10.1007/s41666-020-00082-4.

[2] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated electronic health records," *International Journal of Medical Informatics*, vol. 112, pp. 59–67, 2018, doi: 10.1016/j.ijmedinf.2018.01.007.

[3] A. Rehman *et al*., "A secure Healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Computers in Biology and Medicine*, vol. 150, Art. no. 106019, 2022, doi: 10.1016/j.compbiomed.2022.106019.

[4] Y. Y. Ghadi *et al*., "Enhancing patient healthcare with mobile edge computing and 5G: Challenges and solutions for secure online health tools," *Journal of Cloud Computing*, vol. 13, no. 1, pp. 1–13, 2024, doi: 10.1186/S13677-024-00654-4.

[5] Y. Y. Ghadi *et al*., "The role of blockchain to secure Internet of Medical Things," *Scientific Reports*, vol. 14, no. 1, pp. 1–31, 2024, doi: 10.1038/s41598-024-68529-x.

[6] T. Mazhar *et al*., "Generative AI, IoT, and blockchain in healthcare: Applications, issues, and solutions," *Discover Internet of Things*, vol. 5, no. 1, pp. 1–23, 2025, doi: 10.1007/S43926-025-00095-8.

[7] T. Mazhar *et al*., "Analysis of integration of IoMT with blockchain: Issues, challenges and solutions," *Discover Internet of Things*, vol. 4, no. 1, pp. 1–36, 2024, doi: 10.1007/S43926-024-00078-1.

[8] M. Nasr, M. M. Islam, S. Shehata, F. Karray, and Y. Quintana, "Smart healthcare in the age of AI: Recent advances, challenges, and future prospects," *IEEE Access*, vol. 9, pp. 145248–145270, 2021, doi: 10.1109/ACCESS.2021.3118960.

[9] M. F. Khan *et al*., "An IoMT-enabled smart healthcare model to monitor elderly people using machine learning technique," *Computational Intelligence and Neuroscience*, vol. 2021, Art. no. 2487759, 2021, doi: 10.1155/2021/2487759.

[10] Z. Yu, S. U. Amin, M. Alhussein, and Z. Lv, "Research on disease prediction based on improved DeepFM and IoMT," *IEEE Access*, vol. 9, pp. 39043–39054, 2021, doi: 10.1109/ACCESS.2021.3062687.

[11] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 2152–2163, 2022, doi: 10.1109/JBHI.2021.3101686.

[12] E. Mbunge, B. Muchemwa, S. Jiyane, and J. Batani, "Sensors and Healthcare 5.0: Transformative shift in virtual care through emerging digital health technologies," *Global Health Journal*, vol. 5, no. 4, pp. 169–177, 2021, doi: 10.1016/j.glohj.2021.11.008.

[13] A. R. Javed *et al*., "A collaborative healthcare framework for shared healthcare plan with ambient intelligence," *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–21, 2020, doi: 10.1186/s13673-020-00245-7.

[14] J. Qayyum, "Collaborative federated learning for healthcare: Multi-modal COVID-19 diagnosis at the edge," *arXiv preprint arXiv*, 2021