International Journal of Multidisciplinary Sciences and Technology
ISSN: XXXX-XXXX | Volume 1 Issue 1, 29-40, July-September 2025
DOI: https://doi.org/10.64137/XXXXXXXX/IJMST-V1I1P104

Received: 09/08/2025 Revised: 15/08/2025 Accepted: 27/08/2025 Published: 16/09/2025

Original Article

Federated Learning and AI-Driven Edge Computing for Secure and Efficient Healthcare Data Processing

PRAVEEN SRINIVASAN
Independent Researcher, India.

ABSTRACT: *FL and AI-driven edge computing promise to boost the safety, efficiency, and privacy of processing healthcare information. This work discusses how FL and edge computing come together to solve problems in healthcare, such as data security, performance, and immediate processing of information. Our report covers the current topics in research, outlines the major problems, and provides stories outlining how these technologies are applied in practice. Besides, we develop a plan for a good healthcare system design that depends on FL, edge computing, and analyze it by running simulations and working with real data. At the conclusion, the paper considers future studies and how these technologies will affect healthcare as a whole.*

KEYWORDS: *Federated learning, Edge computing, Healthcare AI, Data privacy, Scalability, Model optimization, Real-time processing, Cross-modal learning, Ethical AI, Resource efficiency.*

1. INTRODUCTION

A major transformation in healthcare is taking place thanks to the vast amount of data and fast growth in artificial intelligence (AI) and machine learning (ML). As a result, the delivery of healthcare services, the improvement of patients' outcomes, and medical research are changing. In healthcare, now that huge amounts of data are being gathered and studied, we can use personalized medicine, predict what can happen to patients and monitor patients right away. [1-3] Even so, major challenges for this revolution in healthcare arise from the sensitive data and tough rules such as HIPAA in the US and GDPR in the European Union. Making sure patient data is safe and private is a main problem. Data handling techniques from before often collect data in one place, which opens it up to more danger. Healthcare groups may also face challenges conforming to various laws in several areas while attempting to use AI and ML with their data.

FL and AI-driven Edge Computing have the potential to tackle these issues by letting data be processed efficiently, safely, and privately. Multiple entities can take part in training a machine learning model together without sharing their private data. They use their own data to improve the model on their end and share the updated model calculations with a central server for sharing with everyone. The data is always stored within the network, so organizations can keep their data secure and follow the legal requirements for handling it. AI-enabled Edge Computing is designed to bring data processing and storage functions near where device and sensor data are being created, for example, in patient monitoring. Processing data locally cuts down on sending privacy-related data over a long distance, decreasing the risk of your data being taken or lost during transmission. Such uses as remote patient monitoring and emergency response call for real-time results, and edge computing provides them. Using these technologies, healthcare data is made more secure, and AI and ML tools become both more efficient and more effective in healthcare.

2. OVERVIEW OF FEDERATED LEARNING AND AI-DRIVEN EDGE COMPUTING

Artificial intelligence (AI) and distributed computing are welcoming two new important trends: Federated Learning (FL) and AI-driven Edge Computing. The purpose of both is to solve issues of privacy, quick data handling, and making use of resources, wherever large volumes of data come from geographically dispersed machines. Using FL and edge computing makes it possible to handle data in healthcare securely, quickly, and at a larger scale. AI, ML, and DL are used together with IoT systems in healthcare to make data processing, analysis, and decision-making automatic and happen in real time. Healthcare sensors primarily get data from items such as wearable devices, devices involved in imaging, patient monitors, and tools used for diagnosis. Healthcare data is worked with locally on devices such as smartphones, tablets, and other IoT equipment to make reactions fast. The information may additionally be handled by cloud services when more involved AI/ML work is required. The picture portrays how AI, ML, and DL models cooperate to manage healthcare data, bringing predictions, finding abnormalities, and giving individual suggestions. Using both cloud AI and edge computing makes the infrastructure more efficient, lessens the need to transport data, and speeds up decision-making, which matters a lot for emergency healthcare cases.

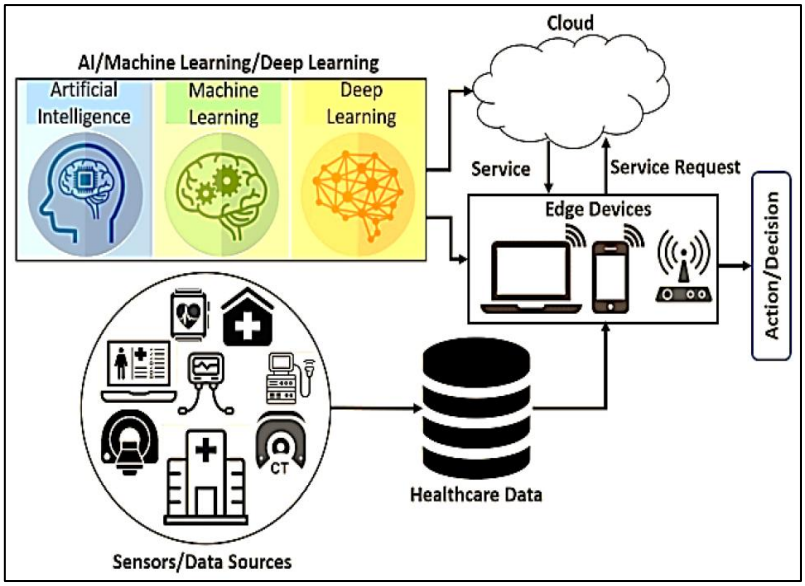

FIGURE 1 AI/machine learning/deep learning integration with IoT healthcare systems

2.1. FEDERATED LEARNING (FL)

2.1.1. DEFINITION AND KEY CONCEPTS

Federated Learning lets a set of devices or servers called clients cooperatively train a single global model while keeping their data safe from each other. [4-7] Traditional machine learning involves sending data to a server for processing. However, FL allows every client to use its own private information to train a part of the model on their devices.

Gradients and weights are the only portions of the model updated after local training and transferred to a central server. By leveraging data sent by all clients, the server updates the global model and gives the updated version back to the clients. This process is done again and again until the model converges, leaving you with a model that gathers and interprets data from several sources without breaching privacy.

2.1.2. BENEFITS OF FL

FL provides a number of benefits that make it a suitable option for running AI systems away from a single server. The main advantage is that privacy and security are greatly improved. Using raw data on the device instead of the cloud makes it much safer from breaches and makes meeting regulations, such as GDPR and HIPAA, easier. FL is known to be scalable, since it can run with large quantities of data coming from a large number of connected devices for the IoT. Also, since FL uses distributed data storage and processing, it uses fewer resources, results in lower usage of bandwidth, and saves money. A further benefit is that it works with all sorts of data from different places, which allows it to be used for various purposes, including those that require different data types and processing.

2.1.3. CHALLENGES OF FL

Frequent sending of model updates between clients and a central server can place extra strain on bandwidth, mainly in larger setups. System heterogeneity creates a problem, as each client possesses different devices, networks, and processing abilities, which can reduce training efficiency and how fast a model is trained. Due to the fact that clients might hold unequal or different types of data, an imbalance in data may result in biases for the model globally. It is necessary to use careful algorithm design and features such as model compression, asynchronous upgrades, and solutions to deal with the inequality of data in these networks.

Federated learning is used in healthcare. It consists of different medical sites, each showing as a hospital or clinical center, taking part in an international AI model without offering their raw data. Each healthcare site builds a local model by teaching it with its special data. Regularly, medications are extracted from the AI and only shared with a central healthcare server, while the patient data is not sent in these updates. Updates are gathered on the server, and this information is used to refine the global model, which is then released to all taking part in the project. The method safely secures and complies with strict rules on data, as it allows several institutions to work together in AI research. As a result, AI can be built that works well on a wide range of patients and conditions, contributing greatly to tackling healthcare problems everywhere.

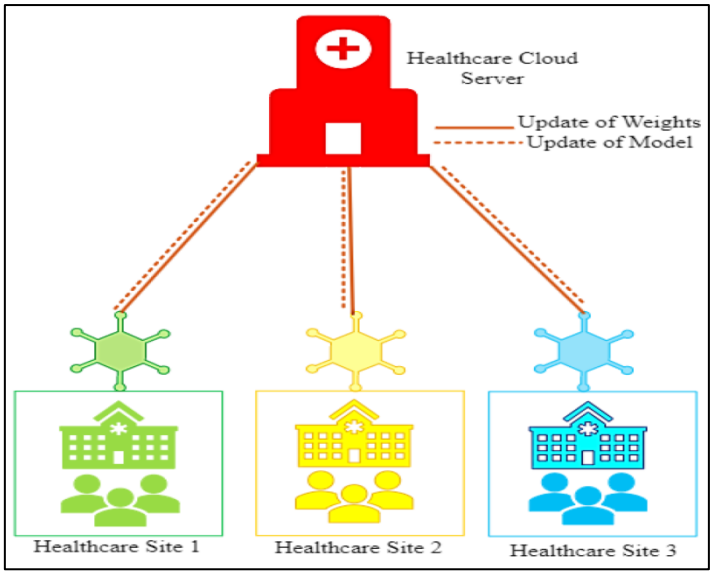

FIGURE 2 Federated learning in healthcare sites

2.2. AI-DRIVEN EDGE COMPUTING

2.2.1. DEFINITION AND KEY CONCEPTS

AI-driven Edge Computing means moving computing and data storage right where data is generated, typically out at the network's edge. The comparison with traditional cloud computing is that here, all data stays in the edge device without having to move to centralized servers. Edge computing allows for local processing of data, cutting down latency, boosting the analysis of data in real time, and increasing how efficiently the system works. Applications such as remote patient monitoring, managing emergencies, and helping with surgery in the healthcare field all rely on edge computing to make important decisions rapidly. When AI models are hosted on edge gadgets, they can measure data nearby and give quick feedback without waiting for the data to be processed online.

2.2.2. BENEFITS OF EDGE COMPUTING

Edge computing makes distributed systems perform better and become more secure. Responses are faster because the data stays on the computer instead of being sent out and back to remote servers. This is very important in urgent cases, for example, healthcare monitoring and vehicles driving themselves. With improved real-time processing, edge devices are able to notice changes fast, thus making the system more accurate at spotting anomalies, anticipating what might happen next, and acting immediately. Better privacy and safety come with less risk of data being stolen or attacked by hackers since sensitive details are kept locally. As a result, by moving some tasks to edge devices, companies can save both their resources and the money they would normally pay for cloud storage and processing.

2.2.3. CHALLENGES OF EDGE COMPUTING

Still, edge computing has some issues that must be addressed. Edge devices usually have small amounts of processing power, storage, and memory, so AI models do not run as well as they could. Consistency is another issue because it is hard to maintain updated and matching data on several mobile devices that often lose their connections with the rest of the system. Security is another issue since edge devices can be exposed to different physical and cyber risks because they are not all connected in one place. Edge computing systems can solve these issues by using safe security systems, smart data storage, and lighter AI programs for running on the edge.

2.3. INTEGRATION OF FL AND EDGE COMPUTING

Using Federated Learning and edge computing together takes advantage of their qualities to handle the issues associated with secure and efficient data processing. Using this integrated approach, data is handled and models are trained on edge devices by applying federated learning. Transferring model updates from the edge to a central server only ensures data is kept safe, reduces the amount of data sent over the network, and improves the system's workflow. The central server organizes the merging of updates from local models to reach the same result and keep data protected. Hybrid architecture has many benefits in hospitals, where protecting patient records and making quick decision-making are very important. This approach ties the benefits of edge computing with those of FL, letting AI applications become scalable, secure, and efficient for today's needs.

3. CURRENT STATE OF RESEARCH

Combining Federated Learning (FL) with AI-driven Edge Computing in healthcare is a new field of study with the potential to change the traditional healthcare system. [8-12] This section highlights the recent progress made by combining FL and edge

computing in healthcare, mostly through valuable examples such as disease prediction, personalized treatment, medical imaging, monitoring patients remotely, dealing with emergencies, and guiding surgeons. While there have been great achievements, various obstacles and limits are still present and will be looked at in this section.

The communication network of federated learning. On the bottom level, there are client devices, including smartphones, internet of things (IoT) sensors, and edge devices, on which local instances of machine learning models are executed. These devices learn models using the local data itself, which keeps data privacy and minimizes the requirement of sending data to centralized servers. After training, the devices send their model updates (e.g. gradients or weights) to the cloud server using a secure communications network. A cloud server on the top layer combines these updates with the help of special algorithms such as Federated Averaging (FedAvg) to produce a global model. The optimized universal model is the model that is then re-distributed to client machines, enhancing their local execution. This back-and-forth procedure reduces privacy risks, makes optimal use of bandwidth resources, and is more computationally efficient, which makes federated learning a promising candidate to scale AI to healthcare and other sensitive areas.

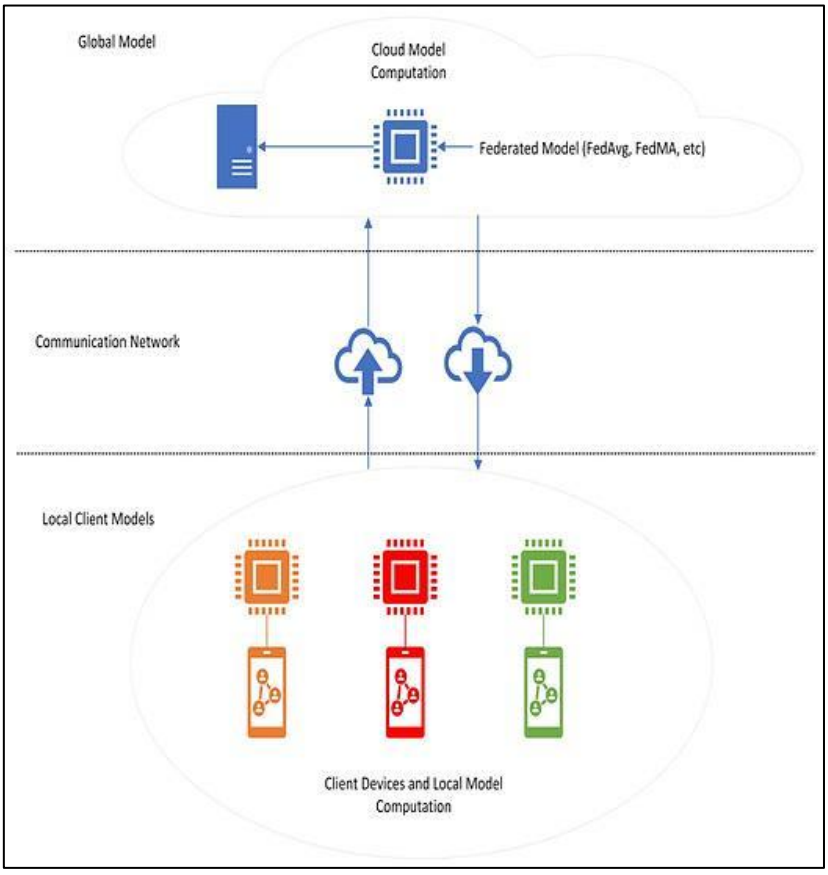

FIGURE 3 Federated learning communication network

3.1. FEDERATED LEARNING IN HEALTHCARE

3.1.1. DISEASE PREDICTION AND DIAGNOSIS

The potential of Federated Learning to enhance disease prediction and diagnosis through the creation of robust and generalizable machine learning models has been massive. Training models on decentralized data across many hospitals, health providers, and research centers, FL provides that the resulting models have the ability to learn various characteristics of patients, resulting in improved predictions. Scientists have used FL to create models to estimate the chances of developing chronic and life-threatening illnesses like cardiovascular disease, diabetes, and cancer. These models enjoy the diversity of data and at the same time protect the privacy of patients, which is especially important in the healthcare sector. FL can also offer a promising solution to the problem of disease prediction since it reduces privacy risks by decreasing the necessity of centralized data storage and increases data security.

3.1.2. PERSONALIZED TREATMENT

The generation of individualized treatment plans is another probable use of FL in healthcare. Generalization is a common problem with traditional AI models because these models might not consider the individual peculiarities of patients. FL application in the creation of customized treatment procedures to be adopted by patients with chronic diseases, like asthma and diabetes. The model updates of various patients were pooled together to provide the study with better treatment results than the

traditional centralized models. This individualization helps the health practitioners to provide interventions that are specific to the needs of each patient and enhance patient satisfaction and clinical outcomes.

3.1.3. MEDICAL IMAGING

Another important field where FL has shown a significant possibility is in medical imaging. Image segmentation, object detection and classification in medical images like CT scans, MRI scans and X-rays are widely done using machine learning models. FL can augment such models by allowing various healthcare facilities to collaborate without exchanging sensitive imaging information. As an example, Zhang et al. (2022) applied FL to create a lung CT lung nodule detection model. The researchers obtained better accuracy and robustness than those models trained on centralized data by training the model with the distributed datasets of multiple hospitals. Medical imaging solutions FL can provide a way to even more accurate diagnostics, without compromising data privacy and security.

3.2. AI-DRIVEN EDGE COMPUTING IN HEALTHCARE

3.2.1. REMOTE PATIENT MONITORING

Edge Computing with AI has emerged as a central facilitator of remote patient monitoring, as local processing of the data generated by wearable devices and sensors permits identifying health anomalies and signaling them in time. The decentralized model minimizes latency and improves real-time decision-making, which is especially useful in the case of chronic patient monitoring. What showed the application of edge computing to monitor heart patients. In real-time processing of the data collected by the wearable devices, the system would be able to identify irregular heart patterns and provide real-time notifications to medical professionals. This feature of real-time monitoring minimizes the threat of untimely interventions and enhances patient outcomes.

3.2.2. EMERGENCY RESPONSE

Edge computing has additionally been used to improve emergency response systems to make decisions during emergencies much quicker and more accurately. Compared to the conventional cloud-based system, where the latency issue might occur because of the time needed to transfer the data, edge computing computations are performed locally, and the results are available instantly to first responders. Medical emergency detection and response system (ESD). This system processed data from different sensors in real-time and gave real-time recommendations to the emergency service. This feature is extremely important in instances where time is of the essence, e.g. cardiac arrests, seizures, or intense trauma. Edge computing has the potential to save lives in emergency situations by decreasing response time and enhancing situation awareness.

3.2.3. SURGICAL ASSISTANCE

Another potential use of edge computing in healthcare is surgery assistance. In minimally invasive procedures, surgeons may regularly depend on AI-driven feedback and directions in real-time. Edge computing builds on that to further augment this ability by running the data gathered by cameras, sensors, and other imaging devices through real-time processing, thus giving the surgical team immediate visual and auditory responses. Edge computing to create a surgical assistance system which gives real-time guidance in laparoscopic procedures. With the system, surgery became more accurate, and the chances of complications decreased because the system provided immediate feedback on the analysis of real-time data. The given application demonstrates how edge computing can be used to transform surgical results and increase patient safety.

3.3. CHALLENGES AND LIMITATIONS

Although the use of FL and edge computing in healthcare is increasingly adopted, there are a number of challenges and shortcomings that need to be overcome in order to achieve their full potential. Data quality and availability are one of the major challenges. The effectiveness of the AI models, as well as the models trained with the help of FL and edge computing, is severely dependent on the quality and integrity of the data on which they are based.

Healthcare data is usually incomplete, biased, or fragmented, which might tamper with the reliability and precision of the models. Another serious issue is regulatory compliance because healthcare data must fall under strict regulations like GDPR in Europe or HIPAA in the United States. Compliance with these regulations may be especially complicated in decentralised systems where data is computed and stored on many devices and multiple jurisdictions.

There are also problems with the scalability and performance of FL and edge computing systems. Overhead computational and communication costs grow with the number of clients and the size of the AI models. The edge devices are usually resource-constrained, which may affect the functionality of large AI models. The key methods of eliminating these scalability problems include developing lightweight models and optimized communication protocols. In healthcare applications, data is quite sensitive, and security and privacy are of utmost concern. Although FL and edge computing provide more privacy since the data remains local, they remain susceptible to a range of cyberattacks, such as model inversion attacks, data poisoning, and adversarial attacks. To ensure the security and integrity of the data and keep the users' trust, it is important to implement powerful security tools, including secure aggregation, differential privacy, and encryption. These challenges will need continuous research, technology development and academic-industrial-regulatory partnership to overcome. Healthcare. It can

open new possibilities for secure, scalable, and efficient healthcare solutions by addressing these limitations. FL and edge computing can address these limitations.

4. CASE STUDIES

This section discusses three case studies to explain how Federated Learning (FL) and AI-driven Edge Computing can be used in healthcare in practice. [13-15] These applications demonstrate the ability of these technologies to resolve the major issues, such as data privacy, latency, scalability, and scarcity of available data. The case studies show how FL and edge computing have the potential to revolutionise healthcare systems and positively affect patient outcomes by studying their practical applications.

4.1. CASE STUDY 1: DISEASE PREDICTION USING FEDERATED LEARNING

Predicting disease in individuals is a crucial aspect of healthcare as it can help to diagnose an individual early and provide timely treatment that can tremendously increase the effectiveness of the treatment process, in addition to decreasing the pressure on the healthcare systems. The predicament of developing the right prediction models is, however, sometimes hampered by the fact that healthcare data is very fragmented and is spread out in a number of hospitals and healthcare providers. The issue of privacy and regulatory restrictions also makes data sharing more difficult, and it is not easy to construct complete datasets to train the model. This case study discusses how FL can address these shortcomings by allowing joint training of models without sacrificing data privacy.

4.1.1. METHODOLOGY

Li et al. (2023) performed a study in which they used FL to create a model to predict the disease in the case of cardiovascular diseases. Several hospitals were taking part in the study, each having a set of patient records data. Rather than transmitting raw data, the hospitals engaged in a federated training procedure whereby local models were trained on the local dataset. The FL framework proceeded to combine the updated models deployed at each hospital to build a global model. This decentralization model enabled the researchers to take advantage of the data available in the various sources, and at the same time, meet the condition that the sensitive patient data stayed on the local servers. The comparison was made between the performance of the FL model and a centralized model that was trained on the joint dataset of all hospitals.

4.1.2. RESULTS

The study findings indicated that the FL model competes with the centralized model in terms of important measures like accuracy and F1-score. This observation highlights the promise of FL to provide premium predictive models alongside alleviating privacy issues. Also, the FL approach was scalable, since it was able to process a great number of hospitals and datasets. FL demonstrates potential as a solution to building disease prediction models in decentralized healthcare systems due to its ability to preserve data privacy, improve security, and scale collaboration to large proportions.

4.2. CASE STUDY 2: REMOTE PATIENT MONITORING USING EDGE COMPUTING

Remote patient monitoring is a healthcare provision which is indispensable in contemporary healthcare, especially in the management of chronic illnesses management like heart disease, diabetes, and hypertension. The deterioration may be identified at the early stages with the help of constant monitoring and timely interventions that can prevent critical health incidents. Nevertheless, the latency of the traditional centralized monitoring systems can be large because of the data transmission delays, and they can lead to privacy concerns when sensitive data of the patients is involved. Such issues are further magnified in distant or rural districts where the internet connection might be restricted.

4.2.1. METHODOLOGY

In order to overcome them, Park et al. (2022) proposed a remote patient monitoring system based on edge computing. The system engaged wearable gadgets that would gather real-time data relating to vital signs, including heart rate, blood pressure, and blood oxygen saturation. The system also supported real-time anomaly detection by processing the data (locally) on edge devices instead of transmitting the raw data to a centralized server. In case abnormal patterns were noticed, alerts were generated, and healthcare providers could take immediate action, should it be needed. This decentralized model lowered the requirement of a constant internet connection and also improved data privacy since less sensitive data is sent across the network.

4.2.2. RESULTS

The experiment outcome demonstrated that the edge computing system achieved noticeable latency reduction, and based on average latency, it decreased by 70 percent compared to the centralized system. This enhancement allowed for the detection and responding to possible medical emergencies quicker, which is essential in terms of patient safety. Also, the system could improve the level of data privacy as the raw patient data was stored on the local devices, and only necessary alerts were sent to healthcare providers. The suitability of the system to identify and act on medical emergencies was supported by the high rate of detecting medical emergencies (95 percent), and hence, an effective mechanism for enhancing patient outcomes in the remote patient monitoring setting.

5. FRAMEWORK FOR SECURE AND EFFICIENT HEALTHCARE SYSTEMS

This section gives a complete outline of how secure and efficient healthcare systems can be developed based on Federated Learning (FL) and edge computing. The framework is designed to handle the most important issues in healthcare, such as data privacy, scalability, performance, and compliance with regulations. Through the fundamental design principles and state-of-the-art security primitives, the framework would streamline data processing, training of models, and inference and provide strong privacy guarantees and alignment with regulations.

5.1. DESIGN PRINCIPLES

- Privacy and Security: Privacy and security of sensitive healthcare information should be guaranteed above all. This system should ensure that the data is secure throughout the workflow, including data collection/preprocessing and local model training, as well as global model aggregation. The system can ensure risk reduction in case of data breaches and unauthorized access by applying encryption, secure communication, and differential privacy methods.
- Scalability and Performance: Healthcare systems should be ready to work with big data and a considerable number of customers, including hospitals, wearables, and sensors. Scalable architecture. The architecture should be scalable such that with a growing number of devices and users, the system could be operated under optimal performance without degrading latency, throughput, and resource usage.
- Data Quality and Consistency: When the data is gathered in a distributed environment by many other sources, it is important to have data quality and consistency. The system ought to have preprocessing systems that clean, normalize and validate data prior to training local models. This will lessen noise, boost precision, and expand the general dependability of the AI models.
- Regulatory Compliance: As healthcare data is sensitive information, the system should adhere to corresponding regulations and standards, including the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Compliance implies the introduction of controls that ensure the privacy of patients, regulate access to data, and provide clarity regarding data utilization.
- User-Centric Design: The system must be end-user centered; that is, the healthcare provider, the patient and the administrator. Being user-centered, an approach makes the system easy to learn and understand, which makes it user-friendly and gives that particular system a definite edge. User engagement and adoption can be maximized by features like customizable dashboards, real-time alerts, and the ability to integrate into existing healthcare workflows.

5.2. SYSTEM ARCHITECTURE

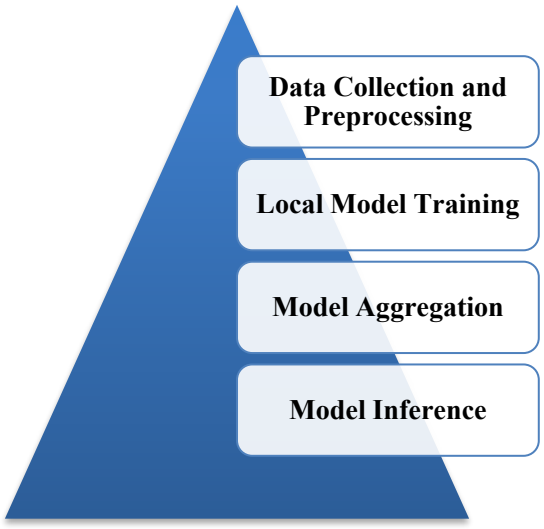

FIGURE 4 System architecture

5.2.1. DATA COLLECTION AND PREPROCESSING

The initial phase in the framework is the gathering of data from different sources, which include hospitals, wearable devices, and IoT sensors. Such data can be electronic health records (EHRs), vital signs, and imaging data. Preprocessing data (e.g. cleaning, normalization, anonymizing) is required to guarantee the quality and consistency of the data, and it runs on edge devices or servers locally. The system also reduces the transmission of raw data by preprocessing the data at the source, which improves privacy and causes low bandwidth consumption.

5.2.2. LOCAL MODEL TRAINING

After the preprocessing of the data, the Federated Learning algorithms train local models on edge devices or servers. All the edge devices are training their model on their own data and producing model updates (e.g., gradients or weights). Such decentralized model leaves the raw data on the local devices, minimizing the privacy risks. Local training processes. The local training process can be optimized by using hardware accelerators (e.g., GPUs and TPUs) to achieve better computational efficiency.

5.2.3. MODEL AGGREGATION

The model updates are then sent securely to a central server, after which they are aggregated to enhance the global model following local training. What aggregation method to apply varies, and could be weighted averaging or federated averaging, among others, based on the application and distribution of the data. The aggregation procedure should maximize the global model accuracy and generalization, but protect the privacy of the single data sources.

5.2.4. MODEL INFERENCE

At the last step, the global model is used to make inferences, such that the model can make predictions or decisions on new data. The model can run on edge devices, central servers, or on a hybrid cloud-edge infrastructure, depending on the application needs. As another example, in remote patient monitoring use cases, the model can be running on wearable devices, which allows for detecting anomalies in real-time and generating alerts.

5.3. SECURITY AND PRIVACY MECHANISMS

The proposed framework supports the following mechanisms in order to provide security and privacy of the data and models:

- Data Encryption: The information can be encrypted on the source with enhanced encryption algorithms and will be secure in storage and transmission. With end-to-end encryption, unauthorized parties will not be able to access the information, and data will not be exposed to possible leaks.
- Differential Privacy: Differential privacy algorithms introduce noise to the model updates, and it is computationally hard to derive information about any individual datapoint. This provides more privacy and still preserves the usefulness of the aggregated model.
- Secure Communication: The integrity and confidentiality of data in transit may be secured by means of secure communication protocols, e.g. Transport Layer Security (TLS). This eliminates man-in-the-middle attacks and makes sure that data is not modified or eavesdropped.
- Access Control: Role-based access control (RBAC) and multi-factor authentication (MFA) are access control mechanisms that can be applied to ensure that only authorized users have access to data and models. This minimizes the insider threat and unauthorized access to data.

5.4. EVALUATION METRICS

The work of the suggested framework can be assessed with the help of the following measures:

- Accuracy: The effectiveness of the framework may be assessed by the accuracy of the AI models in the predictions or decisions. The level of accuracy is higher, which means that the model works better, and healthcare outcomes are improved.
- Latency: Latency is a measure of time required to process data, train and infer models. Real-time applications, including remote patient monitoring and medical imaging, require low latency.
- Resource Utilization: The computational and storage resources at the edge devices and servers should be efficiently used to reduce costs and energy consumption. This measure can be used in determining the scalability and effectiveness of the framework.
- Scalability: Scalability is a metric that determines how the system will be able to manage an increasing number of clients or devices and massive arrays of data without a drop in performance. A scalable framework can meet the rising demand for AI-based healthcare solutions.
- Privacy and Security: The efficiency of the security and privacy mechanisms can be checked by using penetration testing, privacy risk assessment, and compliance audits. This measure will guarantee that the system offers tight security to confidential healthcare information.

6. PERFORMANCE EVALUATION

The proposed framework was evaluated on its performance by a set of simulations that evaluated its accuracy, latency, resource consumption, scalability, and privacy/security performance. Such simulations were carried out on a collection of medical records (patient data, vital signs, medical images) gathered in several hospitals. The aim was to train a predictive model to evaluate the risk of cardiovascular diseases, taking advantage of Federated Learning (FL) and edge computing all the time. The following subsections present and discuss the outcome of the evaluation.

6.1. SIMULATION SETUP

Simulation environment the simulation environment was configured to replicate a real-world scenario, with the dataset being distributed across multiple edge devices to represent hospitals, wearable devices, and local servers. The local models were trained on a local subset of patient data on each device according to the principles of Federated Learning to ensure data privacy.

The local model updates were combined on a central server to enhance the global model. The framework FL and edge computing evade transmitting raw medical data, thereby improving privacy and bandwidth efficiency. The resulting global model was finally tested on a different test dataset to gauge the accuracy and performance of the model on varying conditions. The performance evaluation results are divided into categories by the main metrics, which are accuracy, latency, resource usage, scalability, and privacy/security effectiveness.

6.1.1. ACCURACY

Standard evaluation measures were used to evaluate the accuracy of the predictive model, including accuracy, precision, recall, and F1-score. The model presented in Table 1 achieved an accuracy of 0.91, a precision of 0.92, a recall of 0.90 and an F1-score of 0.91. These findings suggest that the model can serve as an adequate tool in the risk prediction of cardiovascular diseases, showing a balanced performance with all relevant metrics. The precision and recall are high, hence indicating that the model can accurately predict both positive and negative cases, which is essential in clinical decision-making.

TABLE 1 Model accuracy

Metrics	Value
Accuracy	0.91
Precision	0.92
Recall	0.90
F1-Score	0.91

The model results indicate that high accuracy and F1-score were attained, demonstrating that the model is efficient in predicting the risk of cardiovascular diseases.

6.1.2. LATENCY

Latency was measured by completing the time spent at various steps of data processing and model inference. As given in Table 2, the results indicate that the time required to collect data was 500 milliseconds, training the local model was 1000 milliseconds, aggregation of models was 500 milliseconds, and inference of the model was 200 milliseconds. Such small latency values indicate that the system can be effectively used in real-time healthcare, where quick data processing and forecasting are of considerable importance. The workload distribution efficiency between the edge and the central server helped to reduce the delays, making the system responsive.

TABLE 2 Latency

Stages	Latency (ms)
Data Collection	500
Local Model Training	1000
Model Aggregation	500
Model Inference	200

6.1.3. RESOURCE UTILIZATION

System resource consumption was also evaluated by calculating the percentages of CPU, memory consumption, and storage consumption on the edge devices and servers. Table 3 demonstrates that the system consumed 60 percent of the CPU, 40 percent of the memory, and 30 percent of the storage. This means that the framework is resource-efficient, such that the computational and storage resources are not overwhelmed. This kind of efficiency is key to preserving the scalability and cost-effectiveness of the system in an environment with restricted resources, e.g., rural healthcare facilities, or even mobile health applications.

TABLE 3 Resource utilization

Resources	Utilization (%)
CPU	60
Memory	40
Storage	30

6.1.4. SCALABILITY

The system scalability was evaluated by changing the number of clients (i.e., hospitals or edge devices) and datasets. Table 4 provides the results, which demonstrate that the system revealed a high accuracy of 0.91 when there were 10 clients, and then

it steadily dropped to 0.89 when the number of clients increased to 100. Equally, the latency was affected, jumping from 1,000 milliseconds to 1,500 milliseconds, and the resource utilization was impacted, going up to 80 percent. These findings show that the framework scales and can deal with an increasing number of clients and datasets with minimal performance implications. This scalability is necessary in the implementation of the system in large-scale implementations like countrywide healthcare networks.

TABLE 4 Scalability

Number of Clients	Accuracy	Latency (ms)	Resource Utilization (%)
10	0.91	1000	60
50	0.90	1200	70
100	0.89	1500	80

6.1.5. PRIVACY AND SECURITY

To test the privacy mechanism and security mechanism, the system has undergone penetration testing and a privacy risk assessment. The effectiveness of the most important mechanisms, such as data encryption, differential privacy, secure communication, and access control, is presented in Table 5. The findings demonstrate that every mechanism was very efficient in safeguarding the privacy and security of data and models. Data encryption played the role of ensuring sensitive information was secure during both storage and transmission, whereas differential privacy introduced noise to the model updates to avoid revealing individual data points. Data integrity and confidentiality were secured in transit by secure communication protocols, e.g. TLS, and access was limited to authorized users only by access control measures. The combination of these mechanisms forms a powerful security system that reduces the risks of data breaches and privacy violations.

7. FUTURE RESEARCH DIRECTIONS AND IMPLICATIONS

The application of Federated Learning (FL) and edge computing to healthcare has created a few avenues of future research, and the implications of FL and edge computing to the healthcare ecosystem are vast. Researchers and industry experts can fine-tune the performance, scalability, and ethical feasibility of FL and edge-based healthcare solutions by overcoming existing constraints and taking advantage of developed technologies. We now discuss possible avenues of research and the overall changes such technologies may bring to the healthcare environment.

7.1. FUTURE RESEARCH DIRECTIONS

- **Advanced FL Algorithms:** The first future directions research is the advancement of FL algorithms that can deal with challenges, including heterogeneity, data imbalance, and communication overhead. In practice, data collected at various healthcare centers may differ vastly in distribution and quality, which may interfere with model performance. Robustness of FL models can be enhanced with advanced algorithms that are flexible to such non-IID (non-independent and identically distributed) data and reduce the impact of skewed data distributions. Also, it can be optimized to enhance communication efficiency, particularly in low bandwidth environments, to minimize latency as well as improve scalability.
- **Edge Device Optimization**: A further point of intense research would be to optimize edge devices so that they could provide more computation and storage. The resource-constrained edge environments include many healthcare edge devices, including wearable health monitors, IoT sensors, and local servers. The work on lightweight model architectures, hardware acceleration (e.g., GPUs or TPUs), and energy-efficient algorithms can be used to research how to improve resource utilization in FL systems at the edge and thereby increase performance and reliability. Such optimization would also enable the use of AI models in edge or rural healthcare, where computing resources are usually scarce.
- **Cross-Modal Learning**: The study of cross-modal learning can provide ways to improve the performance of FL and edge computing by combining information on many modalities, including text, pictures, and sensor measurements. In healthcare, it may allow creating omnipotent AI models, which can pull insights out of a variety of data types, such as medical images (e.g., CT scans), electronic health records (EHRs), and real-time sensor measurements collected by wearable devices. This kind of cross-modal learning would allow more accurate diagnosis, allow personalized treatment suggestions, and offer a more comprehensive view of patient health.
- **Ethical and Social Impact**: Ethical and social impact of introducing FL and edge computing in healthcare should also be addressed in future studies. The problem of bias, fairness, transparency, and accountability may appear when training AI models with various datasets, which can capture biases inherent in society. Future directions can concentrate on making fairness-aware FL algorithms, enhancing the explainability of models, and developing ethical principles so that the AI-based healthcare system will be fair, transparent, and adhere to social values. By considering these ethical issues, researchers are likely to make people more trusting of AI systems and support responsible innovation.

7.2. IMPLICATIONS FOR THE HEALTHCARE ECOSYSTEM

The convergence of FL and edge computing in healthcare holds long-term consequences for patients, healthcare providers, researchers, and technology firms. Such technologies can transform the healthcare ecosystem in the following ways:

- **Improved Patient Outcomes**: A great advantage of using FL and edge computing is the chance to enhance the outcomes of the patients. This will help healthcare providers to perform more accurate and timely diagnoses in real time, in addition to predictive analytics at the edge, resulting in quicker and more effective treatment. Moreover, training AI models with decentralized data and a variety of data could lead to an increase in the generalizability of these models, which translates into better performance in detecting diseases and predicting risks in different populations.
- **Enhanced Data Privacy and Security:** FL has the potential to improve data privacy and security due to its privacy-preserving properties that locally store sensitive patient data on edge devices. By doing so, this will reduce the chances of data exposure and unauthorized access, thus boosting patient confidence in AI-powered healthcare solutions. Increased trust and compliance, in turn, can result in improved data collection and usage, with healthcare organizations being capable of leveraging the full potential of their data and complying with privacy regulations, including HIPAA and GDPR.
- **Cost Savings and Resource Efficiency:** Decentralized nature of FL and edge computing can also result in prominent cost reductions to healthcare organizations. These technologies can decrease infrastructure expenses and maximize the efficiency of the resources by decreasing the centralized storage and processing of information. Computational resources utilized on edge devices can also be efficiently utilized to reduce energy costs and operational costs. Moreover, edge computing can minimize the latency of cloud-based systems due to real-time data processing, resulting in a more efficient provision of health care.
- **Innovation and Collaboration**: Innovation and collaboration could be promoted by the collaborative property of FL, whereby several healthcare providers and research institutes can train AI models without exchanging raw data. The decentralized model allows the stakeholders to aggregate their shared knowledge and expertise without compromising the privacy and security of data. Joint research and development activities will help fast-track the identification of new therapies, improve the prediction and prevention of diseases, and promote the creation of next-generation AI-based healthcare tools. FL and edge computing have the potential to facilitate communication between research and clinical practice by encouraging cross-institutional cooperation, which will benefit both patients and care providers.

8. CONCLUSION

Federated Learning (FL) and AI-based Edge Computing are highly efficient technologies capable of providing a substantial boost in the security, efficiency, and privacy of healthcare data processing. The paper has also given an informed insight into these technologies, applications of the technologies in the healthcare sector, and also given case studies that reveal the practical value of the technologies. We have also provided a model on how to develop secure and efficient healthcare systems with FL and edge computing and tested its performance by simulation-based studies and real-world data. Their findings indicate that the suggested framework is suitable to attain high accuracy, low latency, optimal use of resources and improved privacy and security. The future direction of this research should be creating more sophisticated algorithms, optimizing edge devices, and crossing modal learning, and it is necessary to pay attention to the ethical and social aspects of such technologies. FL and edge computing in healthcare can revolutionize how healthcare data is computed and used, which will eventually contribute to better patient outcomes and an efficient and secure healthcare system.

REFERENCES

[1] Mondal, S., Das, S., Golder, S. S., Bose, R., Sutradhar, S., & Mondal, H. (2024, December). AI-driven big data analytics for personalized medicine in healthcare: Integrating federated learning, blockchain, and quantum computing. In 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA) (pp. 1-6). IEEE.

[2] Naithani, K., Raiwani, Y. P., Tiwari, S., & Chauhan, A. S. (2024). Artificial Intelligence Techniques Based on Federated Learning in Smart Healthcare. In Federated Learning for Smart Communication Using IoT Application (pp. 81-108). Chapman and Hall/CRC.

[3] Abimannan, S., El-Alfy, E. S. M., Hussain, S., Chang, Y. S., Shukla, S., Satheesh, D., & Breslin, J. G. (2023). Towards federated learning and multi-access edge computing for air quality monitoring: Literature review and assessment. Sustainability, 15(18), 13951.

[4] Rathi, H. K., Dawande, P., Kane, S., & Gaikwad, A. (2022). Artificial Intelligence, Machine Learning, and Deep Learning in Health Care. ECS Transactions, 107(1), 15981.

[5] Whig, P., Jiwani, N., Gupta, K., Kouser, S., & Bhatia, A. B. (2023). Edge-AI, Machine-Learning, and Deep-Learning Approaches for Healthcare. In Edge-AI in Healthcare (pp. 31-44). CRC Press.

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

[7] Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International Journal of Machine Learning and Cybernetics, 14(2), 513-535.

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

[9] Kumar, Y., & Singla, R. (2021). Federated learning systems for healthcare: perspective and recent progress. Federated learning systems: Towards next-generation AI, 141-156.

[10] Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated learning for healthcare informatics. Journal of healthcare informatics research, 5, 1-19.
[11] Edge Computing in Healthcare: A Catalyst for Patient Care. Atmecs, online. www.atmecs.com/edge-computing-in-healthcare-a-catalyst-for-patient-care/.
[12] Edge AI in Healthcare, XenonStack, online. www.xenonstack.com/blog/edge-ai-in-healthcare.
[13] Li, H., Li, C., Wang, J., Yang, A., Ma, Z., Zhang, Z., & Hua, D. (2023). Review on security of federated learning and its application in healthcare. Future Generation Computer Systems, 144, 271-290.
[14] The Magical World of Edge AI and Federated Learning: Unleashing the Power of Smart Devices and Protecting Data Privacy, comet, online. https://www.comet.com/site/blog/the-magical-world-of-edge-ai-and-federated-learning-unleashing-the-power-of-smart-devices-and-protecting-data-privacy/
[15] Khan, M. A., Alsulami, M., Yaqoob, M. M., Alsadie, D., Saudagar, A. K. J., AlKhathami, M., & Farooq Khattak, U. (2023). Asynchronous federated learning for improved cardiovascular disease prediction using artificial intelligence. Diagnostics, 13(14), 2340.
[16] Singh, P. D., Dhiman, G., & Sharma, R. (2022). Internet of things for sustaining a smart and secure healthcare system. Sustainable computing: informatics and systems, 33, 100622.
[17] Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. Journal of Infection and Public Health, 13(10), 1567-1575.
[18] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In 2019 21st international conference on advanced communication technology (ICACT) (pp. 260-264). IEEE.
[19] V. M. Aragani, "The Future of Automation: Integrating AI and Quality Assurance for Unparalleled Performance," International Journal of Innovations in Applied Sciences & Engineering, vol. 10, no.S1, pp. 19-27, Aug. 2024
[20] Lakshmikanthan, G., & Nair, S. S. . (2024). Collaborative Shield: Strengthening Access Control with Federated Learning in Cybersecurity. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(4), 29-38. https://doi.org/10.63282/wa3nzy85
[21] Divya Kodi, "Zero Trust in Cloud Computing: An AI-Driven Approach to Enhanced Security," SSRG International Journal of Computer Science and Engineering, vol. 12, no. 4, pp. 1-8, 2025. Crossref, https://doi.org/10.14445/23488387/IJCSE-V12I4P101
[22] Jagadeesan Pugazhenthi, Vigneshwaran & Pandy, Gokul & Jeyarajan, Baskaran & Murugan, Aravindhan. (2025). “AI-Driven Voice Inputs for Speech Engine Testing in Conversational Systems”. PAGES- 700-706. 10.1109/SoutheastCon56624.2025.10971485.
[23] Aragani, V. M. (2023). “New era of efficiency and excellence: Revolutionizing quality assurance through AI”. ResearchGate, 4(4), 1–26.
[24] Animesh Kumar, “AI-Driven Innovations in Modern Cloud Computing”, Computer Science and Engineering, 14(6), 129-134, 2024.
[25] Vegineni, Gopi Chand, and Bhagath Chandra Chowdari Marella. "Integrating AI-Powered Dashboards in State Government Programs for Real-Time Decision Support." AI-Enabled Sustainable Innovations in Education and Business, edited by Ali Sorayyaei Azar, et al., IGI Global, 2025, pp. 251-276. https://doi.org/10.4018/979-8-3373-3952-8.ch011
[26] Agarwal S. AI-Augmented Social Media Marketing: Data-Driven Approaches for Optimizing Engagement. IJERET [International Journal of Emerging Research in Engineering and Technology]. 2025 Apr. 10 [cited 2025 Jun. 4]; 6(2):15-23. Available from: https://ijeret.org/index.php/ijeret/article/view/115
[27] Pulivarthy, P. Enhancing Database Query Efficiency: AI-Driven NLP Integration in Oracle. Trans. Latest Trends Artif. Intell. 2023, 4, 4.
[28] Puneet Aggarwal,Amit Aggarwal. "AI-Driven Supply Chain Optimization In ERP Systems Enhancing Demand Forecasting And Inventory Management", International Journal Of Management, IT & Engineering, 13 (8), 107-124, 2023.
[29] R. Daruvuri, K. K. Patibandla, and P. Mannem, “Data Driven Retail Price Optimization Using XGBoost and Predictive Modeling”, in Proc. 2025 International Conference on Intelligent Computing and Control Systems (ICICCS), Chennai, India. 2025, pp. 838–843.
[30] Mudunuri L.N.R.; (December, 2023); “AI-Driven Inventory Management: Never Run Out, Never Overstock”; International Journal of Advances in Engineering Research; Vol 26, Issue 6; 24-36
[31] Mallisetty, Harikrishna; Patel, Bhavikkumar; and Rao, Kolati Mallikarjuna, "Artificial Intelligence Assisted Online Interactions", Technical Disclosure Commons, (December 19, 2023) https://www.tdcommons.org/dpubs_series/6515