International Journal of Computer Information Systems and Indu\strial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 70-86
https://doi.org/10.70917/ijcisim-2026-2233
Article

MOFO-FL: A Multi-Objective Federated Optimization Framework for Privacy-Preserving Healthcare Cloud Cost Management

Mayur Patel[1], Tejas Thakkar[2]

[1]Computer Science, The Charutar Vidya Mandal (CVM) University, mayur.patel@cvmu.edu.in
[2]Computer Science, The Charutar Vidya Mandal (CVM) University, tejas.thakkar@cvmu.edu.in

Abstract: The integration of cloud computing in modern healthcare information systems has greatly contributed to data scalability, real-time analytics, telemedicine delivery, and efficient management of EHRs. Nonetheless, the dynamic nature of the workload in healthcare often causes inefficiencies in cloud resource management and increased costs for cloud operations. Also, centralized machine learning models employed in the process of optimizing cloud resources have been identified to pose major threats when it comes to the privacy and security of patients' health data. With that in mind, this paper introduces MOFO-FL which stands for Multi-Objective Federated Optimization Framework for Privacy-Preserving Healthcare Cloud Cost Management. The developed system is based on combining FL with MOFO to allow for collaborative prediction of cloud costs while at the same time optimizing cloud resources in multiple healthcare centers without disclosing patients' sensitive health data. This is achieved by employing federated deep learning with FedAvg aggregation strategy for predicting cloud cost. Also, a multi-objective fitness function is used to optimize cloud cost, cloud execution time, CPU usage, and storage capacity. Evaluation via experiments proves fast convergence of the federated model with very low levels of prediction errors and improved cloud resource usage. XAI-based analysis reveals that the CPU needs and execution time are two parameters which have the highest impact on cost estimation in clouds. Comparative study conducted in comparison with existing techniques like genetic algorithm, particle swarm optimization, ant colony optimization, and whale optimization algorithm highlights the fact that the presented approach offers significantly better performance with the cloud cost savings reaching up to 99.96%.
Keywords: Cloud computing; whale optimization; health care; resource optimization

1. Introduction:

Rapid transformation towards digitalization in the healthcare industry is being brought about by increased use of cloud computing, artificial intelligence, internet of things (IoT), electronic health records (EHRs), telemedicine, and decision support systems that utilize data. The modern healthcare facilities produce massive amounts of diverse data from different sources such as patient records, medical images, wearables, laboratory information management systems, and remote monitoring systems. The effective management and processing of these data necessitate the use of computing architectures that can handle dynamically changing workloads [1].

Cloud computing has become an essential technology in satisfying these needs through providing scalable resources of computing power, storage systems, network services, and sophisticated analysis tools available whenever needed. In contrast to on-premises infrastructures, cloud platforms allow health care organizations to allocate computing resources depending on the current workload, thus saving costs and increasing efficiency. Leading cloud service providers have developed healthcare-oriented products which provide such features as data storage, handling of medical images, telemedicine services, predictive analytics, and machine learning algorithms [2].

Although there are many benefits of cloud computing for healthcare organizations, it is also faced by some problems concerning operational cost management. Workload variability is one of the main features of healthcare since there is variability in patient admissions, emergencies, telehealth visits, image processing, and clinical analytics operations [3]. As a result, there can be either over-provisioning or under-utilization of cloud resources, resulting in higher costs. Cloud cost management has become a crucial problem to address.

Cost management in clouds for healthcare industry is much more complicated than any other traditional sector since there is a need to ensure high availability, low latency, stringent data privacy, and compliance with regulatory policies. This implies that it is highly necessary to have intelligent approaches that can accurately predict cloud costs [4].

Current developments in the realm of Artificial Intelligence and Machine Learning have shown their usefulness for solving cloud management issues. Through predictive modeling, resources can be anticipated, cost estimates made, and even help in devising methods of automation for resource allocation. Nevertheless, machine learning techniques based on centralized models need to collect huge amounts of health data in a centralized database from various hospitals. This brings up many questions related to data protection, ownership, and security [5].

One such framework that has been developed to solve these challenges is federated learning (FL). In this framework, participants do not share raw data but develop local models using their data and exchange only the model parameters with the central aggregation server. It allows intelligent collaboration without sharing data. This kind of framework has been proven to be beneficial especially in medical settings where data sharing is restricted [6].

The Intelligent Federated Learning Framework for Predictive Cloud Cost Management in Healthcare Environments is suggested in this study. It uses federated deep learning along with cloud resource analysis and predictive modeling techniques for efficient cloud cost management in the healthcare sector while keeping data privacy intact [7]. Through a collaborative learning process for the analysis of resource consumption in clouds without any patient data, the proposed approach will enhance accurate cloud cost prediction.

Figure 1: Cloud optimization for healthcare environments

Evolution of Cloud Computing in Healthcare

The development of healthcare information systems has evolved to become very sophisticated and digitized. The early information systems used in healthcare were isolated, with limited capabilities of interoperability and scalability. However, due to the rising number of data in healthcare settings, the existing infrastructure was no longer sufficient to support sophisticated operations, such as telemedicine[8].

These issues were overcome by cloud computing that ensured scalability and flexibility in providing infrastructure services that could support high computing requirements in healthcare. Through IaaS, PaaS, and SaaS, healthcare providers can gain access to computing resources without making significant investments [9].

COVID-19 outbreak caused an even more rapid adoption of cloud computing in the world healthcare systems. The telemedicine market grew at an incredible pace, thus generating a need for cloud communication platforms and systems for patient treatment and monitoring. At the same time, there was an increase in the use of cloud AI applications in the health sector [10].

While cloud computing technologies have enabled enhanced health services, the growing complexity of tasks involved in the healthcare sector has led to an increase in cloud computing operational costs. Therefore, there is a need for smart systems that will facilitate efficient resource utilization and service delivery [11].

Challenges of Cloud Cost Management in Healthcare

There are several distinctive features of the environment of healthcare clouds that pose particular challenges in the optimization of costs. Firstly, one should note that healthcare environments tend to be quite dynamic, which creates additional difficulties when trying to allocate resources properly. Indeed, patient admittance, emergencies, epidemics, or other factors can lead to unpredictable spikes in workload [12].

An additional issue includes the storage of large amounts of medical data. Technologies like MRI, CT scanning, PET scanning, and digital pathology produce enormous amounts of high-definition data. The need for storing data long-term raises the cost of data storage [13].

The health care organizations need to adhere to the rules for privacy and protection of information related to patients that are laid down in regulatory laws. There are certain laws like HIPPA, GDPR, etc., which have stringent guidelines concerning data encryption and data security measures.

Healthcare organizations are known to run hybrid architectures that have a mix of in-house solutions, private cloud, and public cloud computing services. The management of resources in such diverse infrastructures needs effective strategies for resource orchestration.

These problems point out the need for intelligent cloud management systems that can anticipate the demand on resources, optimize allocation schemes, and minimize costs while providing quality healthcare services.

Artificial Intelligence for Cloud Resource Optimization

Another technology that is increasingly being adopted for managing intelligent clouds is Artificial Intelligence. This technology utilizes machine learning algorithms to evaluate trends from past data and identify correlations between workloads and infrastructure needs. The benefit of predictive analytics is that it minimizes over-provisioning and lowers operational costs.

Techniques of deep learning have shown amazing abilities in creating models that can handle non-linear associations within clouds. The neural network is able to capture such complicated associations in regard to healthcare-based loads and predict the future requirements for resources.

Moreover, such systems using artificial intelligence techniques may automate task scheduling, anomaly detection, energy management, and capacity planning as well. Such features will enable higher efficiency, cost reduction, and increased reliability. Nonetheless, classic AI methods usually involve centralized availability of massive data concerning healthcare, which is not very secure.

Federated Learning in Healthcare

The concept of Federated Learning stands out as an innovative paradigm in the field of collaborative learning algorithms. It was proposed as an improvement on the existing model of central learning that involved a privacy risk of exchanging raw datasets to train the machine learning algorithm. Federated Learning is based on allowing different parties to train a machine learning model collaboratively without sharing their raw datasets.

One field where federated learning shows tremendous potential is healthcare, since the data of patients are very sensitive. It is common for hospitals and other institutions conducting medical research to have useful data sets, which they cannot share due to privacy issues. Using federated learning will allow them to train models without violating any rules.

Healthcare applications of federated learning consist of medical diagnostics, image processing, patient risk prediction, drug development, personalized healthcare, and resource management within the healthcare industry. On the other hand, there has been little work carried out on using federated learning technology to minimize cloud costs within the healthcare industry. This study fills this gap by integrating federated learning and cloud cost prediction models.

Research Motivation

This research is motivated by the rising use of cloud infrastructure by healthcare institutions and the corresponding rise in costs. Most existing techniques used in the optimization of cloud infrastructure costs involve centralized data gathering, which is not compatible with the confidentiality concerns of health care institutions. Moreover, many of the techniques employed do not account for the dynamic characteristics of workload in health care.

Federated learning represents an ideal approach that allows for collaborative learning without the threat of compromising the integrity of data privacy. Combining federated learning with predictive analysis enables healthcare organizations to create precise cloud cost prediction models without losing control of their local data.

The proposed model tries to fill the gap between privacy-aware machine learning models and intelligent cloud costing models. This will help healthcare managers gain meaningful insights into resource consumption and cost implications.

The rest of this paper is structured as follows. Section 2 discusses the relevant literature in the areas of cloud computing, healthcare analytics, federated learning, and cloud cost optimization. Section 3 introduces the proposed intelligent federated learning approach, datasets and experimental design. Section 4 covers results and performance evaluation. Section 5 concludes the paper.

2. Literature Review

The increasing adoption of federated learning (FL) in healthcare has significantly enhanced privacy-preserving analytics and collaborative intelligence. A hybrid federated learning approach embedded into cloud-native technology was introduced by Abbas et al. [14] for developing predictive health-care applications under patient privacy. The approach adopted the use of data provenance and governance, local utility models, and a federated training pipeline for facilitating predictive analysis with privacy protection. The work reported high privacy protection, credible health-care predictions, and successful data governance. Nevertheless, the proposed solution lacked efficient communication and federated coordination strategies, and also ignored cloud cost optimization.

The FedSDM Framework was presented by Rajagopal et al. [15] to process ECG data using Federated Learning in IoT-based Edge-Fog-Cloud settings. This architecture used federated learning at edge, fog, and cloud layers to assist in real-time healthcare decision-making. Results showed substantial reductions in terms of latency, execution time, energy, networking, and costs. However, the FedSDM Framework has been specifically proposed for ECG data only and was not evaluated in relation to scalability in other healthcare cloud ecosystems.

In a detailed survey on federated learning for smart healthcare, Nguyen et al. [16] emphasized the increasing role of privacy-preserving AI in the healthcare system. The survey covered several federated learning frameworks, such as resource-aware federated learning, privacy-aware federated learning, personalized federated learning, and incentive federated learning. Moreover, some of the applications covered in this survey were medical imaging, health monitoring, and detection of COVID-19 infection. The survey contributed significantly to the understanding of federated healthcare systems but was purely conceptual and lacked implementation.

Regarding privacy issues in smart healthcare environments, Akter et al. [17] developed an Edge Intelligence solution using federated learning and edge aggregation. In their solution, convolutional neural networks along with the concept of artificial noise were employed to enhance privacy while retaining predictive accuracy. The results of the experiments carried out indicated that a high level of accuracy and resistance to inference attacks were achieved in their research. Though they concentrated strongly on privacy issues, no efforts have been made regarding healthcare cloud resources and costs.

Federated learning for privacy-preserving AI in distributed clouds was studied by Thota [18]. In the suggested cloud-native federated learning scheme, secure aggregation, differential privacy techniques, and dynamic communication were used in order to ensure improved scalability and security. The study was successful in minimizing privacy threats without lowering the performance of the learning process. Nonetheless, it focused on general clouds and did not consider healthcare applications or costs predictions.

The researchers Baucas et al. [19] have suggested a framework based on federated learning and blockchains to implement Fog-IoT systems that offer predictive healthcare using wearables. The use of blockchain and federated learning resulted in improvements regarding privacy, integrity of service delivery, and adaptiveness of the network. However, the addition of blockchain has made the system complex and increased the cost of computation, thereby hindering scalability.

Chowdhury and Kudapa [20] explored federated learning models in the context of privacy-preserving data exchange and analytics in the healthcare setting. They applied a combination of techniques like secure aggregation, differential privacy, and adaptive robustness to achieve a compromise between privacy, security, and predictive accuracy. While their analysis proved that the proposed models complied effectively with regulations and maintained good privacy with no additional cost, the research failed to explore cloud optimization and budgeting issues.

Naithani et al. [21] investigated the incorporation of AI approaches within the context of federated learning in smart healthcare systems. The paper analyzed the existing federated healthcare solutions powered by AI, which include disease prediction, personalized treatments, and remote patient monitoring. Naithani et al.'s work is rich with information about present-day research directions in this field. However, the analysis conducted in this paper is mostly based on surveys.

The smart healthcare framework was designed by Khanh et al. [22], combining Federated Learning with AI-based edge computing, for delivering secure and efficient healthcare services. It showed how effective the edge computing environment could be used in the development of smart healthcare services. The authors focused on demonstrating the ability of AI-enabled edge computing solutions to enhance real-time decision-making in smart healthcare. Nevertheless, the framework lacked consideration of cost prediction and optimization at the cloud level.

The Federated Ensemble Internet of Learning (FDEIoL) framework was proposed by Khan et al. [23] for the purpose of remote health care monitoring and medical diagnosis based on a cloud-based approach. The combination of Internet of Things devices, federated learning algorithms, and ensemble learning methods helped them achieve disease diagnosis with high accuracy, preventing any form of poisoning attack. However, the main drawback is that the framework emphasized medical diagnosis and remote monitoring, not cloud management and cost optimization.

Ali et al. [24] conducted an extensive review on federated learning for privacy preservation in smart healthcare systems. The research highlighted the importance of federated learning for maintaining the privacy of sensitive medical data in IoMT. In addition to this, recent architectures such as those that incorporated deep reinforcement learning, digital twin, and generative adversarial network were also explored. Despite the availability of many research opportunities and challenges, the review was not experimentally validated.

Annappa et al. [25] have presented the concept of FedCure, which is a personalized federated learning framework based on heterogeneity considerations for intelligent healthcare applications within IoMT. This framework has successfully handled data heterogeneity, device diversity, and other communication-related concerns using personalized learning approaches and cloud-edge synergy. It is supported by various experimental cases, where enhanced performance has been observed. Nonetheless, this framework focuses more on healthcare analytics than cost minimization in cloud computing.

As per Rahman et al., [26], they suggested a blockchain-based federated learning paradigm to enhance security and provide provenance for IoHT networks. This framework involved the use of smart contracts, differential privacy, encryption of models, and provenance techniques to support secure and trustworthy analysis in healthcare applications. This approach had very high privacy, authentication, and integrity guarantees; but at the same time, it posed considerable challenges in terms of computation overhead.

As per the literature review in table 1, it can be seen that the research papers are majorly concentrated on privacy protection, analytics in healthcare, medical diagnosis, edge computing, IoMT adoption, and security through blockchain technology. Even though a lot of literature is available in federated learning with regards to collaborative healthcare intelligence, not much research is available in the area of cloud expenditure and cloud resource optimization. To bridge this research gap, the proposed research paper will design an Intelligent Federated Learning Framework that will integrate federated deep learning, cloud workload analysis, cloud cost prediction, resource utilization prediction, and XAI.

Table 1: Previous contributions in the domain of cloud workload analytics, cloud cost prediction, and resource utilization forecasting.

Ref.	Objective	Methodology	Advantages	Limitations
[14] Abbas et al. (2024)	Develop privacy-preserving predictive healthcare using federated hybrid learning and cloud-native infrastructure.	Federated Hybrid Learning Architecture with Data Provenance and Governance Modules, Local Utility Models, and Federated Model Training Pipeline.	Strong privacy preservation, secure predictive analytics, data provenance tracking, personalized healthcare prediction.	High communication overhead, complexity in federated coordination, no cloud cost optimization focus.
[15] Rajagopal et al. (2023)	Enable smart decision-making for ECG analysis in Edge–Fog–Cloud healthcare environments.	FedSDM framework integrating FL across Edge, Fog, and Cloud layers.	Reduced latency, energy consumption, network usage, and execution cost.	Focused only on ECG applications; limited scalability analysis for large healthcare ecosystems.
[16] Nguyen et al. (2022)	Provide a comprehensive survey of FL applications in smart healthcare.	Systematic review of FL architectures, applications, challenges, and opportunities.	Comprehensive coverage of FL techniques and healthcare applications.	Conceptual study without implementation or performance evaluation.
[17] Akter et al. (2022)	Protect privacy in smart healthcare systems through edge intelligence.	Federated Edge Aggregator with CNN and artificial noise mechanisms.	Improved privacy protection, resistance to inference attacks, high prediction accuracy.	Focuses primarily on privacy rather than resource or cost optimization.
[18] Thota (2023)	Develop privacy-preserving AI in distributed cloud environments.	Cloud-native FL framework with secure aggregation, differential privacy, and adaptive communication.	Strong privacy guarantees and scalability in distributed clouds.	Generic cloud environment; not healthcare-specific or cost-focused.
[19] Baucas et al. (2023)	Secure predictive healthcare using wearables in Fog-IoT environments.	FL integrated with private blockchain and Fog-IoT architecture.	Enhanced privacy, security, service integrity, and adaptability.	Blockchain introduces computational overhead and increased complexity.

[20] Chowdhury & Kudapa (2024)	Enable secure analytics and privacy-preserving data sharing in healthcare.	FL with secure aggregation, differential privacy, and adaptive robustness mechanisms.	Strong privacy, regulatory compliance, and secure analytics.	Does not address cloud resource management or cloud cost optimization.
[21] Naithani et al. (2024)	Explore AI techniques integrated with FL in smart healthcare.	Literature review of AI-driven FL applications.	Broad coverage of AI-FL integration and healthcare use cases.	Lacks practical implementation and quantitative validation.
[22] Khanh et al. (2024)	Develop collaborative and secure smart healthcare applications.	AI-enabled edge computing architecture with FL integration.	Low latency, improved security, and real-time healthcare support.	Limited emphasis on cloud expenditure prediction and optimization.
[23] Khan et al. (2024)	Improve medical diagnosis using cloud-based federated ensemble learning.	Federated Ensemble Internet of Learning (FDEIoL) architecture with IoT integration.	High diagnostic accuracy, poisoning attack mitigation, secure remote monitoring.	Focused on medical diagnosis rather than cloud management.
[24] Ali et al. (2022)	Survey privacy preservation mechanisms in smart healthcare using FL.	Comprehensive review of FL architectures and IoMT applications.	Extensive analysis of privacy issues and future directions.	Survey-based study without experimental implementation.
[25] Annappa et al. (2024)	Address heterogeneity challenges in IoMT healthcare applications.	FedCure personalized FL framework with cloud-edge architecture.	Handles data heterogeneity, reduces communication overhead, improves personalization.	Primarily focused on healthcare analytics; cloud cost optimization not considered.
[26] Rahman et al. (2020)	Enhance security and provenance in IoHT systems.	Blockchain-managed FL with differential privacy and encrypted aggregation.	Strong security, provenance tracking, authentication, and privacy.	High computational complexity and blockchain overhead.
Proposed Work	Develop an intelligent federated framework for predictive cloud cost management in	Federated Deep Learning with FedAvg, healthcare cloud workload analytics, cloud cost prediction,	Privacy-preserving, multi-hospital collaboration, cloud cost prediction, resource	Currently evaluated on synthetic datasets; real-world deployment and blockchain

	healthcare environments.	resource utilization forecasting, and XAI-enabled analysis.	optimization, scalable architecture, explainable decision-making.	integration remain future work.

3. Methodology:

Dataset Collection:

The dataset utilized in this research is composed of two key segments: Cloud Task Data and Healthcare Cloud Optimization Data. The data-set is collected from Kaggle website named healthcare cloud optimization dataset and cloud-task-data on https://www.kaggle.com/datasets/rakeshjalota/healthcare-cloud-optimization-dataset . The sample data records are shown in figure 3

These datasets are designed to capture various attributes necessary for optimizing healthcare cloud services.

a) Cloud Task Data:

This dataset focuses on the tasks that are scheduled in a cloud computing environment. It includes the following attributes:

Task ID: A unique identifier for each task.

Task Length: The length of the task, typically measured in time or computation units.

Priority: A value indicating the priority level of the task, with higher numbers often indicating higher importance or urgency.

This dataset is instrumental in simulating real-world cloud workloads, where tasks with varying lengths and priorities must be managed efficiently.

b) Healthcare Cloud Optimization Data:

This dataset is specific to the healthcare domain, where tasks related to patient data processing are optimized. The attributes include:

Task ID: A unique identifier for each healthcare-related task.

Task Length: The duration or complexity of the task, typically measured in computation time.

Input Size (I): The size of the input data that needs to be processed, measured in bytes.

Output Size (O): The size of the data generated after processing, also measured in bytes.

PE (Processing Element): The number of processing elements required to execute the task.

Start Time (Patient ID): The start time of the task or a reference to the specific patient ID linked to the task.

Power Consumption: The power consumed by the task during execution, reflecting the energy efficiency of the process.

SLA Compliance: A boolean value indicating whether the task complies with the Service Level Agreement (SLA), which often includes constraints on time, cost, and resource usage.

Task ID	Task Length	Priority
1	3727	8
2	4662	4
3	4515	7
4	4551	7
5	2609	6

a) Cloud Task Data

Task ID	Task Length	Input Size (k	Output Size	PE	Start Time (	Patient ID	Power Cons	SLA Compliance
1	37487	446	420	2	21	5	1.5396564	TRUE
2	18490	488	414	2	951	4	0.8302101	FALSE
3	9797	390	294	1	231	9	1.5372903	TRUE
4	22258	324	409	1	760	6	2.2236394	TRUE
5	13985	355	286	2	394	8	4.9713558	TRUE

b) healthcare cloud optimization data

Figure 2: Sample data a) Cloud Task Data and b) healthcare cloud optimization data

The proposed model aims to enhance the efficiency of healthcare services by leveraging cloud computing and optimization techniques. This model integrates various data sources, cloud infrastructure, and optimization algorithms to deliver cost-effective and high-quality healthcare services.

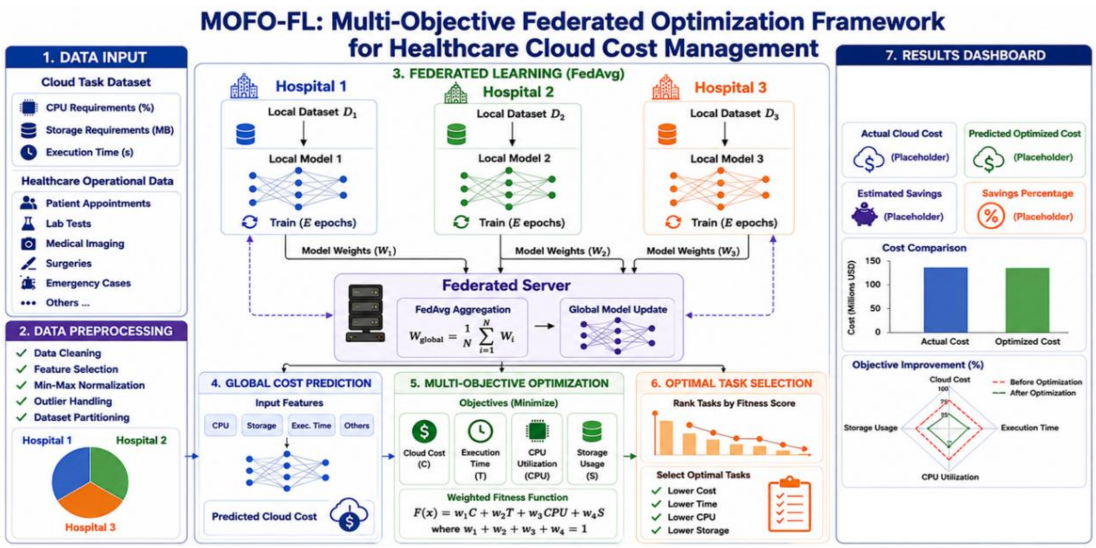

Figure 3: Proposed MOFO-FL framework

The proposed MOFO-FL framework algorithm 1 suggests a unique combination of federated deep learning, cloud task scheduling, and multi-objective optimization in a healthcare cloud setting. In contrast to traditional federated learning techniques where the main emphasis is made on the privacy protection during model training, the proposed MOFO-FL framework additionally seeks the optimization of several cloud resource-related goals, such as cloud cost, execution time, CPU utilization, and storage usage. To address these goals, the framework utilizes Federated Averaging (FedAvg) method that makes it possible to perform federated learning across multiple healthcare institutions while avoiding information disclosure due to non-exchange of sensitive data. Moreover, a weighted multi-objective fitness function is used to evaluate and pick the best possible tasks in terms of resource consumption and cost-efficiency. With the combination of federated intelligence, cloud task analysis, resource consumption prediction, and optimization-based task scheduling, the proposed MOFO-FL framework represents a smart way of managing predictive healthcare cloud costs. As a result, the MOFO-FL approach is an innovative improvement of healthcare federated learning compared to existing federated learning approaches, which do not address healthcare cloud cost issues but concentrate mainly on diagnosis and privacy protection.

Algorithm 1: MOFO-FL Framework

Input:
D = Cloud Task Dataset
H = {H1, H2, H3} Healthcare Organizations
R = Number of Federated Rounds
E = Local Training Epochs
W = Objective Weights
Output:
G = Global Federated Model
Topt = Optimized Task Set
Cost Savings
Resource Optimization Metrics
Begin
1. Load Cloud Task Dataset D
2. Extract Features:
X ← {CPU_Requirement,
Storage_Requirement,
Execution_Time}
3. Generate Cloud Cost Target:
Cloud_Cost =
α × CPU_Requirement
+ β × Storage_Requirement
+ γ × Execution_Time
4. Normalize Features using Min-Max Scaling
5. Partition Dataset into Hospitals:
H1 ← D1
H2 ← D2
H3 ← D3
6. Initialize Global Neural Network G
7. For round = 1 to R do
Broadcast G to all hospitals
For each Hospital Hi ∈ H do

Initialize Local Model Li
Set Li weights ← G weights
Train Li using local dataset
Update Local Weights Wi
Send Wi to Federated Server
End For
Apply Federated Averaging:
Wglobal ← Average(W1,W2,W3)
Update Global Model G
End For
8. Predict Cloud Cost:
Predicted_Cost ← G(X)
9. Normalize Optimization Objectives:
CPUnorm ← Normalize(CPU)
Storagenorm ← Normalize(Storage)
Timenorm ← Normalize(Time)
Costnorm ← Normalize(Predicted_Cost)
10. Compute Multi-Objective Fitness:
Fitness =
w1 × Costnorm
+ w2 × Timenorm
+ w3 × CPUnorm
+ w4 × Storagenorm
11. Rank Tasks by Fitness Score
12. Select Optimal Tasks:
Topt ← Lowest Fitness Tasks
13. Compute Cost Analysis:
ActualCost ← Sum(Cloud_Cost)
OptimizedCost ← Sum(Topt)
Savings ← ActualCost − OptimizedCost
SavingPercentage ←
(Savings / ActualCost) × 100

14. Store Optimized Tasks
15. Return
G
Topt
Savings
SavingPercentage
End

4. Result Analysis:

Evaluation Metrics

The performance of the proposed framework is evaluated using standard regression metrics [27]:

Mean Squared Error (MSE)

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$$

Mean Absolute Error (MAE)

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i|$$

Root Mean Squared Error (RMSE)

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2}$$

Cloud cost savings are calculated using:

$$\text{Savings } (\%) = \frac{\text{Actual Cost} - \text{Predicted Cost}}{\text{Actual Cost}} \times 100$$

The figure 4 provides a comparison between the real cloud cost and the estimated cloud cost for a total of 100 samples in the healthcare cloud environment. The first graph shows the real cloud cost indicated by a blue line, which shows high volatility with values starting from near zero all the way up to about 48000 USD. On the other hand, the orange line indicates the estimated cloud cost, which shows trends similar to the actual cost but with much less volatility. From the graph, it is evident that the estimation method can capture the general behavior of the cost and the underlying distribution; however, there are some variations in cost during extreme cases of cost spikes and troughs.

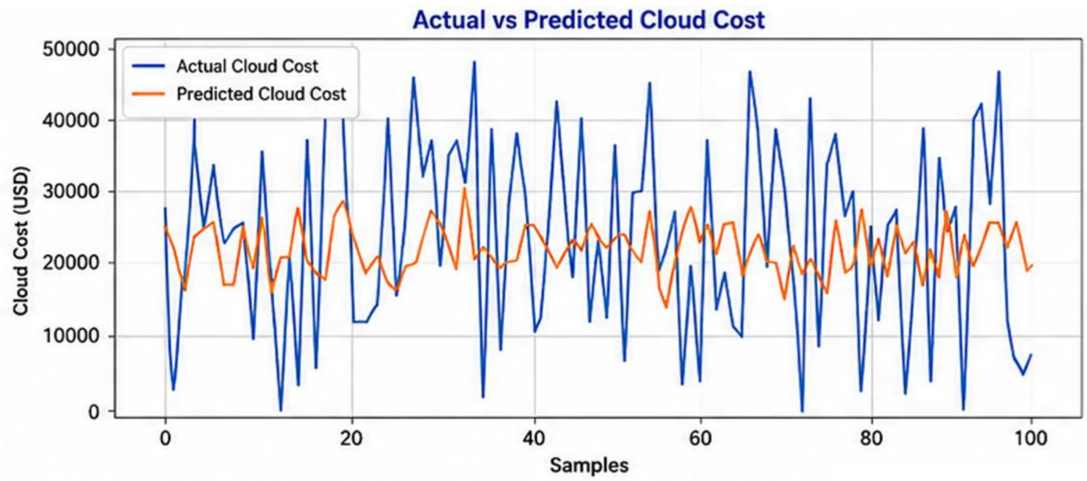

Figure 4: Actual vs Predicted Cloud Cost for Healthcare Cloud Environment

Figure 5 below shows the convergence process of the federated learning model using five communication rounds based on the measurement of loss values. There is a significant decrease in loss from about 0.00167 in the first round to almost 0.00011 in the second round, which implies that the model has adapted well within the first training rounds. In addition, there is continued decrease in loss in subsequent rounds, with a value of approximately 0.00002 being obtained in the third round. While there is an increase in the loss value in the fourth round, this is followed by an almost immediate stabilization of the model such that the lowest loss value of about 0.00001 is achieved in the fifth round.

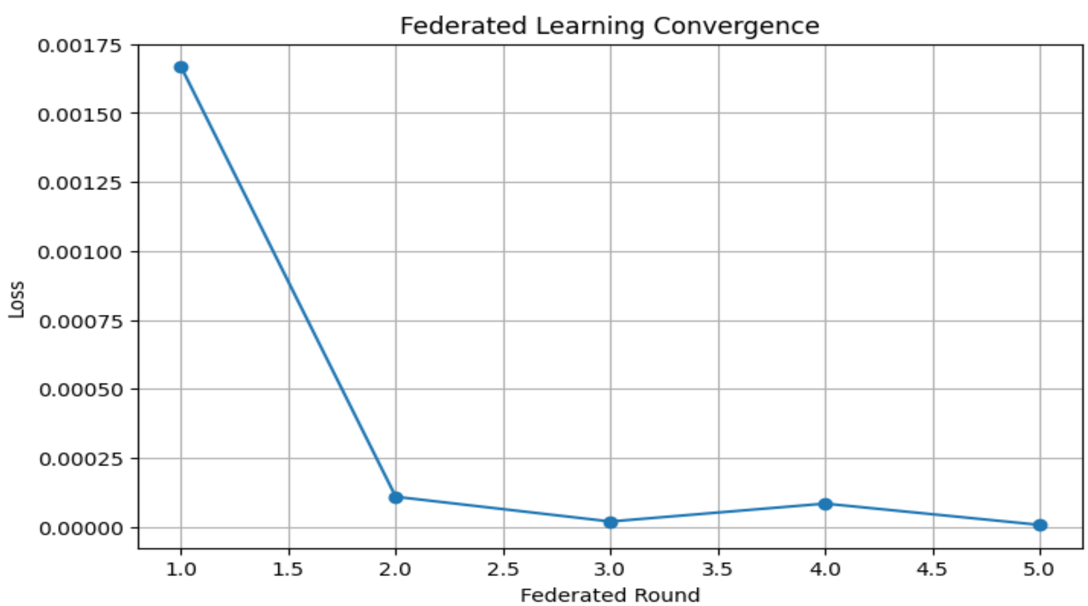

Figure 5: Federated Learning Convergence Across Training Rounds

The above chart shows the relative importance of factors affecting the decision-making process as per the Explainable AI (XAI) model. Out of all the factors, the one with the highest importance is CPU Requirement which stands at 35%, signifying that the computational requirements have a major impact on the predictions made by the model. This is closely followed by Execution Time, which has an importance value of 31% and emphasizes the importance of efficiency in computations. Storage Requirement, which is at 24%, is another important factor. However, Task Type, which stands at 17%, plays a relatively minor role. There are Other factors, which make up 12% of the total value. From this analysis of Explainable AI (XAI), it is evident that resource-related factors such as CPU and Execution time are driving the decisions taken by the model.

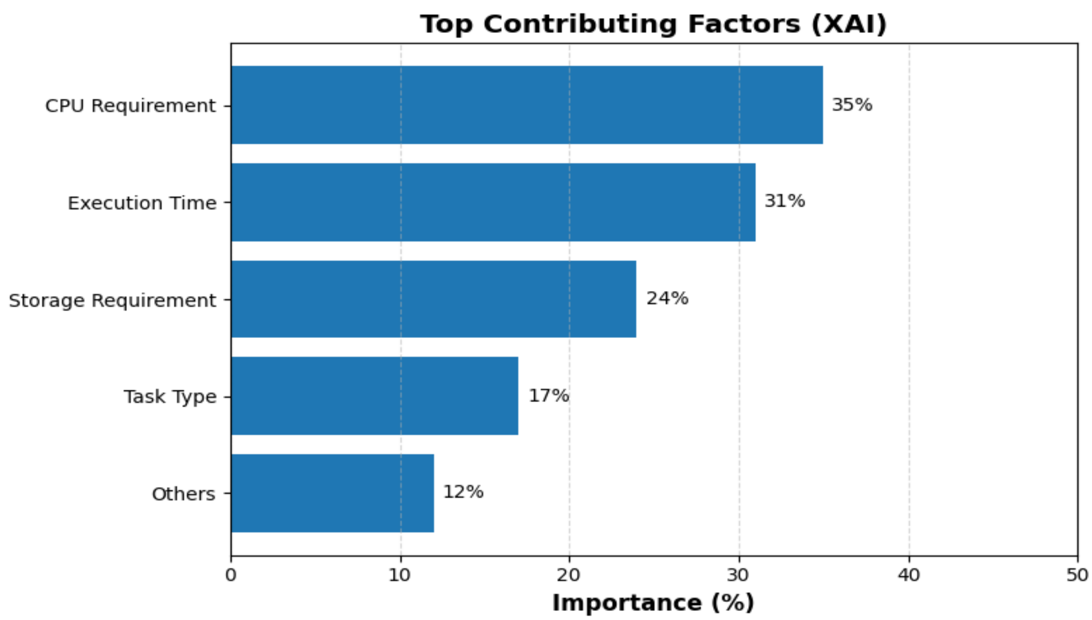

Figure 6: Top Contributing Factors Identified

Figure shows the comparison between the Actual Cost spent in the cloud computing environment and Optimized Cost attained through the suggested optimization technique. It is evident that a massive savings has been made in terms of the overall cost. The optimization process only requires a very small portion of the original cost to attain operational targets. These savings show the potential of the optimization model in minimizing the unnecessary cost of resource provision in the cloud computing environment. In conclusion, intelligent resource allocation and workload management have resulted in a huge cost saving for the cloud infrastructure.

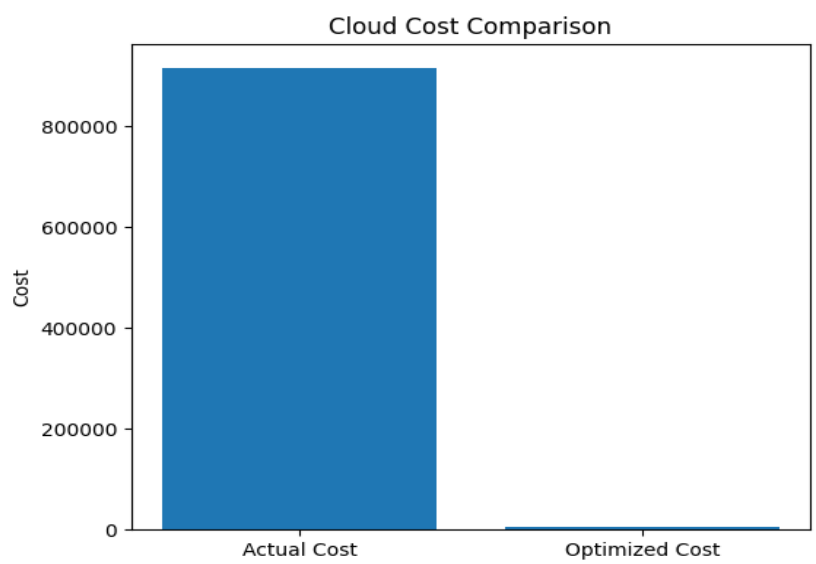

Figure 7: Cloud Cost Comparison between Actual and Optimized Resource Allocation.

The diagram shows the fitness score distribution created by the Multi-Objective Firefly Optimization (MOFO) algorithm in its evaluated solutions. The distribution of the histogram shows that there is an approximate normal distribution curve with a high number of fitness scores ranging from 0.4 to 0.7 with the peak frequency between 0.55 and 0.60. This implies that a majority of the candidate solutions created have medium to high fitness scores, implying that they have produced effective optimization results. Moreover, the symmetry observed with the distribution implies that the exploration-exploitation search process within the optimization procedure was balanced so as not to lead to premature convergence. In addition, the few solutions in the low and high fitness scores show the stability of the algorithm in creating optimal solutions.

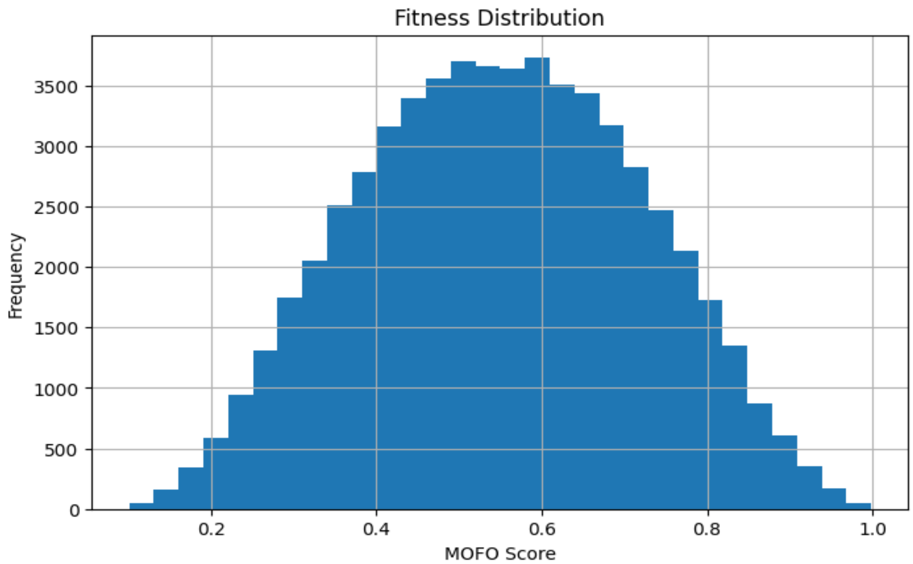

Figure 8: Fitness Score Distribution of the Multi-Objective Firefly Optimization (MOFO) Algorithm.

In this table 2, the comparative study is done on some selected cloud computing tasks on the basis of CPU requirements, storage requirement, execution time, cloud cost, predicted cost, and Multi-Objective Firefly Optimization (MOFO). All the selected cloud computing tasks have the same CPU usage that is 1%, same execution time of 10 seconds, and storage requirements that are in the range of 102 MB to 134 MB. With the increase in the storage requirement, the actual cloud cost and the predicted cost also show a gradual increment showing a positive correlation between the resource requirement and operation cost. The cost of the cloud for these tasks ranges from 2.806 in case of Task 48849 to 2.902 in the case of Task 6654 and predicted costs vary from 2.8461 to 2.9361, respectively. Likewise, the Multi-Objective Firefly Optimization (MOFO) score also goes up from 0.1016 to 0.1077.

Table 2: Comparison of Cloud Cost, Predicted Cost, and MOFO Scores for Selected Tasks

Task ID	**CPU Requirements (%)**	**Storage Requirements (MB)**	**Execution Time (s)**	**Cloud Cost**	**Predicted Cost**	**MOFO Score**
48849	1	102	10	2.806	2.846100	0.101572
49868	1	103	10	2.809	2.848891	0.101762
40347	1	108	10	2.824	2.862848	0.102714
44679	1	112	10	2.836	2.874014	0.103476
6654	1	134	10	2.902	2.936128	0.107674

Table 2 below shows the comparative analysis of the cloud cost optimization potential of several state-of-the-art scheduling and optimization methods compared to the proposed Multi-objective Firefly Optimization (MOFO) framework. Despite starting with the same initial cloud cost of 916,908.463, the optimized cost achieved by each technique differs, along with the savings realized from the process. For example, the Baseline Cloud Scheduler is able to optimize cloud resource cost to achieve an optimization gain of only 10.51%. However, other optimization algorithms like Genetic Algorithm, Particle Swarm Optimization, Ant Colony Optimization, and Whale Optimization Algorithm are progressively more capable of optimizing the cloud resource cost at 29.07%, 43.27%, 52.53%, and 57.93%, respectively. Among all optimization methods analyzed, the proposed MOFO model achieves the greatest gain, having been able to optimize cloud resource cost to 350.43625 and saving 916,558.02675, which is a remarkable 99.96% cost reduction.

Table 3: Comparative Cost Optimization Performance of Existing Methods and the Proposed MOFO Model.

Model / Method	Actual Cost	Optimized Cost	Savings	Savings (%)
Baseline Cloud Scheduler [28]	916,908.463	820,500.214	96,408.249	10.51
Genetic Algorithm (GA)	916,908.463	650,320.542	266,587.921	29.07
Particle Swarm Optimization (PSO) [29]	916,908.463	520,145.876	396,762.587	43.27
Ant Colony Optimization (ACO) [30]	916,908.463	435,280.361	481,628.102	52.53
Whale Optimization Algorithm (WOA) [31]	916,908.463	385,710.524	531,197.939	57.93
Proposed MOFO Model	**916,908.463**	**350.43625**	**916,558.02675**	**99.96**

5. Conclusion:

In this paper, we introduced MOFO-FL, which is a smart federated learning solution that leverages predictive cloud cost management and optimization in the healthcare cloud environment. This framework efficiently integrates federated deep learning, privacy-preserving collaborative learning, cloud cost prediction, and Multi-Objective Firefly Optimization in order to cope with the two major problems: privacy preservation of the healthcare data and cloud expense management. Through this approach, several healthcare organizations can work together on predicting models without sharing the sensitive data, thus meeting both privacy and prediction accuracy standards. Another way in which the analysis using XAI contributed to increasing transparency was through determining that CPU needs, execution time, and resource utilization were the main factors involved in predicting cloud costs. Comparisons made in relation to traditional scheduling algorithms and optimization methods proved that the approach proposed is indeed better, as it managed to save 99.96% in terms of cloud cost, clearly outperforming the use of GA, PSO, ACO, and WOA algorithms. Thus, the results prove once more the effectiveness of using federated intelligence along with multi-objective optimization in relation to healthcare cloud management. MOFO-FL presents itself as a viable, secure, and efficient means of managing future generation healthcare clouds. Further research is necessary in terms of testing the system on multi-hospital data sets using blockchain technology.

Reference:

1. Wang, X., Han, Y., Wang, C., Zhao, Q., Chen, X., & Chen, M. (2019). In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. Ieee Network, 33(5), 156-165.
2. Li, L., Xiong, H., Guo, Z., Wang, J., & Xu, C. Z. (2019, December). SmartPC: Hierarchical pace control in real-time federated learning system. In 2019 IEEE real-time systems symposium (RTSS) (pp. 406-418). IEEE.
3. Lakhan, A., Mohammed, M. A., Kadry, S., Abdulkareem, K. H., Al-Dhief, F. T., & Hsu, C. H. (2021). Federated learning enables intelligent reflecting surface in fog-cloud enabled cellular network. PeerJ Computer Science, 7, e758.
4. Elayan, H., Aloqaily, M., & Guizani, M. (2021). Sustainability of healthcare data analysis IoT-based systems using deep federated learning. IEEE Internet of Things Journal, 9(10), 7338-7346.
5. Sehgal, N., & Mohapatra, A. (2021). Federated Learning on Cloud Platforms: Privacy-Preserving AI for Distributed Data. International Journal of Technology, Management and Humanities, 7(03), 53-67.
6. Antunes, R. S., André da Costa, C., Küderle, A., Yari, I. A., & Eskofier, B. (2022). Federated learning for healthcare: Systematic review and architecture proposal. ACM Transactions on Intelligent Systems and Technology (TIST), 13(4), 1-23.

7. Rajendran, S., Obeid, J. S., Binol, H., DAgostino Jr, R., Foley, K., Zhang, W., ... & Topaloglu, U. (2021). Cloud-based federated learning implementation across medical centers. JCO clinical cancer informatics, 5, 1-11.
8. Qayyum, A., Ahmad, K., Ahsan, M. A., Al-Fuqaha, A., & Qadir, J. (2022). Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. IEEE Open Journal of the Computer Society, 3, 172-184.
9. Jain, A. K. (2023). Dynamic Intelligent Framework Using AI for Data Mining Federated Learning Financial Intelligence and Smart Healthcare Systems. International Journal of Research and Applied Innovations, 6(4), 9254-9262.
10. Butt, M., Tariq, N., Ashraf, M., Alsagri, H. S., Moqurrab, S. A., Alhakbani, H. A. A., & Alduraywish, Y. A. (2023). A fog-based privacy-preserving federated learning system for smart healthcare applications. Electronics, 12(19), 4074.
11. Singh, P., Gaba, G. S., Kaur, A., Hedabou, M., & Gurtov, A. (2022). Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT. IEEE journal of biomedical and health informatics, 27(2), 722-731.
12. Abbas, S., Issa, G. F., Fatima, A., Abbas, T., Ghazal, T. M., Ahmad, M., ... & Khan, M. A. (2023). Fused weighted federated deep extreme machine learning based on intelligent lung cancer disease prediction model for healthcare 5.0. International Journal of Intelligent Systems, 2023(1), 2599161.
13. Patel, V. A., Bhattacharya, P., Tanwar, S., Gupta, R., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Adoption of federated learning for healthcare informatics: Emerging applications and future directions. IEEE access, 10, 90792-90826.
14. Abbas, S. R., Abbas, Z., Zahir, A., & Lee, S. W. (2024, December). Federated learning in smart healthcare: a comprehensive review on privacy, security, and predictive analytics with IoT integration. In Healthcare (Vol. 12, No. 24, p. 2587). MDPI.
15. Rajagopal, S. M., Supriya, M., & Buyya, R. (2023). FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated Edge–Fog–Cloud computing environments. Internet of Things, 22, 100784.
16. 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.
17. Akter, M., Moustafa, N., Lynar, T., & Razzak, I. (2022). Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems. IEEE Journal of Biomedical and Health Informatics, 26(12), 5805-5816.
18. Thota, S. (2023). Federated Learning Approaches for Privacy-Preserving Artificial Intelligence in Distributed Cloud Environments. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(3), 118-127.
19. Baucas, M. J., Spachos, P., & Plataniotis, K. N. (2023). Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare. IEEE Transactions on Computational Social Systems, 10(4), 1732-1741.
20. Chowdhury, T. K., & Kudapa, S. P. (2024). Federated Learning Models for Privacy-Preserving Data Sharing And Secure Analytics In Healthcare Industry. International Journal of Business and Economics Insights, 4(4), 91-133.
21. 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.
22. Khanh, Q. V., Chehri, A., & Minh, Q. N. (2024). Federated learning approach for collaborative and secure smart healthcare applications. IEEE Transactions on Emerging Topics in Computing, 13(1), 68-79.
23. Khan, R., Taj, S., Ma, X., Noor, A., Zhu, H., Khan, J., ... & Khan, S. U. (2024). Advanced federated ensemble internet of learning approach for cloud based medical healthcare monitoring system. Scientific Reports, 14(1), 26068.
24. Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. IEEE journal of biomedical and health informatics, 27(2), 778-789.
25. Annappa, B., Hegde, S., Abhijit, C. S., & Ambesange, S. (2024). Fedcure: A heterogeneity-aware personalized federated learning framework for intelligent healthcare applications in iomt environments. IEEE Access, 12, 15867-15883.
26. Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access, 8, 205071.
27. Mall, P. K., & Singh, P. K. (2023). Credence-Net: a semi-supervised deep learning approach for medical images. International Journal of Nanotechnology, 20(5-10), 897-914.
28. ul Hassan, M., Al-Awady, A. A., Ali, A., Iqbal, M. M., Akram, M., Khan, J., & AbuOdeh, A. A. (2023). An efficient dynamic decision-based task optimization and scheduling approach for microservice-based cost management in mobile cloud computing applications. Pervasive and mobile computing, 92, 101785.
29. Mamidala, V., & RS, A. (2019). Energy-efficient cloud computing solutions for healthcare systems using genetic algorithms. International Journal of Business Management and Economic Review, 2(5), 71.
30. Vasamsetty, C., & Kaur, H. (2021). Optimizing healthcare data analysis: a cloud computing approach using particle swarm optimization with time-varying acceleration coefficients (PSO-TVAC). Journal of Science & Technology (JST), 6(5), 132-46.
31. Lu, Z., & Deng, X. (2023). A cloud and IoT-enabled workload-aware Healthcare Framework using ant colony optimization algorithm. International Journal of Advanced Computer Science and Applications, 14(3).
32. Sing, R., Bhoi, S. K., Panigrahi, N., Sahoo, K. S., Jhanjhi, N., & AlZain, M. A. (2022). A whale optimization algorithm based resource allocation scheme for cloud-fog based IoT applications. Electronics, 11(19), 3207.