Empowering Consumer Healthcare Through Sensor-Rich Devices using Federated Learning for Secure Resource Recommendation

Afifa Salsabil Fathima, Syed Muzamil Basha, Syed Thouheed Ahmed, Surbhi Bhatia Khan, Senior Member, IEEE, Fatima Asiri, Shakila Basheer, Madhu Shukla.

Abstract – When implementing zero-trust edge computing, offloading computational tasks and data access through traditional model training and usage approaches can lead to increased latency. Since the traditional methods often involve extensive communication with a central server, creating additional network hopping stations/nodes resulting in increased latency. The challenge is bound to allocate a befitting resource at a given consumer demand. In this proposed system, a federated learning model based data offloading and consumer medical resource recommendation of IoT is discussed and validated. The user/consumer group and local training models are aligned with edge servers for data preprocessing and customization with a series of resources demand creation and coordination. The consumer resource allocating priorities are fine-grained with the proposed blockchain based priority analyzer for recommendation and allocation. The computational parameter such as resource pool, average waiting time, energy consumption and transmission trust delays are observed and validated. The proposed framework fetches consumer resources logs and synchronizes the centralized training model for effective scheduling and allocation of resources with an accuracy of 94.92% under the 5G operating spectrum. The technique has demonstrated minimal latency in offloading the data request demand and resource allocation at the cloud servers.

Keywords – Healthcare, IoT, federated learning, medical edge cloud, blockchain, resource recommendation

Afifa Salsabil, Syed Muzamil Basha is associated with School of Computer Science and Engineering, REVA University, Bengaluru, Karnataka, India.
Syed Thouheed Ahmed is with School of Computing and Information Technology, REVA University, Bengaluru, Karnataka, India.
Surbhi Bhatia Khan is Department of Data Science, School of Science Engineering and Environment, University of Salford, Manchester United Kingdom; s.khan138@salford.ac.uk
Fatima Asiri is working with College of computer science , Informatics and computer systems department, King Khalid University, Saudi Arabia; Falmalye@kku.edu.sa
Shakila Basheer is working with Department of Information Systems, College of computer and Information science, Princess Nourah bint Abdulrahman University, P.O. BOX 84428, Riyadh 11671, Saudi Arabia, sbbasheer@pnu.edu.sa
Madhu Shukla is working with the Department of CSE - AI, ML & DS, Marwadi University, Rajkot - 360003, Gujarat, India, Madhu.shukla@marwadieducation.edu.in.

*Correspondence: Surbhi Bhatia Khan (s.khan138@salford.ac.uk) and Fatima Asiri (Falmalye@kku.edu.sa).

I. INTRODUCTION

Medical servers and resource allocation is a challenging task in edge and server computing. With reference to the smart cities and innovative communicating approaches, the edge computing plays a vital role. The edge-layer primarily controls and coordinates the data/information from edge-devices and provides reliable solutions. In the biomedical field, the edge layer computes the vital data processing and computing local training models if required to restrain and coordinate the resource recommendation process at the central server associated to the medical application. The central servers are either loaded with primary application tasks or are scheduled with upcoming tasks such as user queries and data analysis from the administrator. The servers/edges are continuously busy processing the request and demand of the users. The resources are bound to the servers and hence effective distribution and monitoring can provide reliable medical solutions.

The resource recommendation and modeling of healthcare sensors are based on the bandwidth allocated for sharing and implementation. The current challenge under 4G and previous generation based spectrum is the latency caused during the transmission process as the centralized computation was remote via cloud ecosystem and was defined under the paradigms of centralized model development. These models primarily caused delay in decision making and distributed pattern computation from the data generated via IoMT/IoT devices. The 5G based spectrum in this research work is developed under the private 5G simulation environment for IoMT devices validation and data pattern extraction. The scope of data collection, monitoring and coordination in wearable devices is a challenging task with respect to the Internet of Medical Things (IoMT). The biomedical sensory data collected via these devices are aligned with respect to the working and synchronization categories. Hence a recommendation system is required for the customization of information and the resources allocation to ensure a smoother transaction in data synchronization and computation. The zero-trust tolerance zone assure the operations are maximized in this relevance as further research gaps are discussed in the subsection as follows.

A. Research Gaps and Challenges

The zero trust tolerance of the information and data is a challenging task with reference to the centralized processing approach. The central servers and the authenticated distributed servers are bound to operate in the resource spectrum available on demand and hence causing an increased latency in the computation and access. The connected IoT/IoMT devices are driven by sensor data, classified as sensitive data with respect to the data source, data origin type and the structure of inclusive data mapping under the accessing range. Thus causing a relative delay in resource monitoring and management.

In this research, the focus is aimed to provide a sustainable solution for medical resource sharing and scheduling in the area of telemedicine and telehealth and further building an ecosystem for effective cyber-physical systems (CPS) in eHealth environment. In the current times, the resources shared by the medical infrastructure such as hospitals, government and private research centers and data archives are limited and are bound to face task/job overloading for the demand generated by the users such as patients, medical experts, medical researchers, engineers and others. Many innovative and novel techniques are proposed and developed to provide effective task scheduling and offloading. In the past, the edge-cloud computing approaches [1] define the need and purpose of an effective task scheduler for improvising the peak performance of the servers.

B. Contributions

The contributions of the research are given below:

- The research article addresses the need of task processing and task scheduling via a federated learning and blockchain approach. The federated learning (FL) model is derived from the de-centralizing the computational capabilities.
- The FL model is trained via independent local federated models at the edge layer, such that each local model is associated within the network via the block chain operation.
- The blockchain coordination and local FL models are controlled via the a centralized or global server. The resource recommendation process is alignment in coordination with the resource distribution agent (RDA) and resource monitor (RM) defined in the framework.

The outcome of this technique is to secure a relatively lower processing time delays and latencies during the resource recommendation and offloading process. The technique is inclusive of Zero-Trust Management (ZTM) for secure operations in the edge-server and edge-device layers' in coordination with the local and global federated learning models. The CPS exchanges include the third party servers and service providers and hence the ZTM assurance is inclusive in the proposed system.

This manuscript is organized with an introduction and literature reviews in section I and II focused on setting the theme of the research, followed by section III with methods and materials used and proposed in the manuscript. The section IV and V discusses on the Resource Distribution Agent (RDA) based mathematical modeling and section VI is dedicated for the blockchain activation and resource alignment with section VII concluding the proposed models via task offloading and providing the recommendation of the resources. The Section VIII discusses the results and research finding and section IX concludes the manuscripts.

II. LITERATURE REVIEWS

The edge computational research on task/job offloading and scheduling is a wide researched domain. The process includes primary scheduling algorithms in a centralized servers and cloud computing environments. [2] The technological platforms include fog computing [3], cloud computing and edge computing [4]. These approaches include traditional surveys and observation reports from various algorithms and frameworks to provide effective selection of task offloading approaches in centralized servers. With multi-access edge-computing also termed as mobile-edge computing, [5] the standard offloading of tasks and scheduling to the computational zone was streamlined and pushed towards the users and thus causing a delay in synchronizing the user-devices and the computational servers. The overall process includes recent techniques such as [6] Fruit-Fly based optimization of task offloading (FOTO), Cooperative Multi-task scheduling based Ant Colony Optimization (CMS-ACO) and [7] has a novel approach discussed with the Fog assisted IoMT monitoring system design for healthcare applications. The approach as integrated reverse path and multiple subjective data aggregation approach for decision making. whereas in [8] an adaptive offloading algorithm dedicated for remote healthcare application. These approaches include performance parameters such as improved demand ratio management, improvising the operating cost, effective scheduling and minimal latency on offloading process.

The complexity of task offloading medical applications in Zero-Trust (ZT) scenarios is to provide secure and reliable channel of CPS operations. The machine learning based techniques such as [8] Computation Offloading using Reinforcement Learning (CORL), [9] Optimizing Mobility-Aware task offloading in IoMT devices [10] using Distributed partial Markov Model (Dec-POMDP) and IoT-Fog Cloud environment based techniques [11] for improvising the latency and reduce the operating cost or the energy consumption during the operations. These approaches are based on centralized computation and requires active communication and coordination with the servers which intern results in providing a secure ZTM based operations.

The techniques of including blockchains and federated learning is primarily discussed in [12] the Blockchain based Reliable Task Offloading (BRTO) framework for IoMT and Software Define Networks (SDN) applications, this approach includes the ant based optimization for improvising the data security and robustness of the SDN. The report in [12] is subjected on the recent challenges and upgrading provided in the IoT and consumer space for the relevance development of the model at the ZT phase and operations, A state of art next generation consumer electronics is discussed in [13] followed with a purpose and design requirements of the users. In [14] the Mobile Edge Computing (MEC) and Mobile Cloud Computing (MCC) is discussed for effective offloading, response time and energy consumption. With reference to the Zero-Trust operations, the architecture is well-defined and monitored in [14] for cloud-edge-terminal in 5G bandwidth and further in [15] a matured security framework for MEC is discussed. For the federated learning models, a heterogeneous resource recommendation model for healthcare applications is proposed and a detailed study is reported in [16], whereas in [17] a revolution of Health 5.0 prospective and consumer based implementation challenges are discussed with respect to IoT applications and towards the future prospects and guidelines of including the FL models for effective resource recommendation and modeling. The informative analysis on energy driven IoT systems is the demand centric requirement for the durable consumers. The study in [18] provides an Optimal Cooperative offloading scheme for effective energy management in IoT framework. The potential requirement is to provide effective and secure operation framework.

The descriptive comparison is computed from [19 – 21] is reported with a fuzzy based zero tolerance detection and mapping. In [22] a detailed and latest review on the challenges of zero-tolerance via multiple sensory data is reported with an analysis and relevance for scenario validation. The validation is further justified with a federated learning model of ZT verification in [23] for intrusion detection under an active network for effective classification. The IoMT data-verification and channel mapping under 6G is reported in [24] padded with federated learning model for IoMT resource recommendation under dynamic ecosystem. The mobile based architecture [25] is justified for computing and validating the ZT scenario for effective resource mapping and process monitoring.

III. METHOD AND MATERIALS

Medical cloud and connected edge devices are coordinated via services of communicating instructions towards resource sharing and resource allocation. The improvising cloud-edge configuration is updated via interval of time by the cloud-administrator towards the resources peak availability and scheduling pattern to avoid load-overloading on the cloud servers. The communication and computing data crunch is further streamlined by parallel computing cum instruction handling buffers. In this methodology the edge-servers/edge-cloud resource recommendation scenario is validated under zero trust zone of edge-cloud operation. Typically, the computing server allocates primary resources to the incoming server computation demand and further on “Zero Trust” scenario activation, the centralized archives of federated learning based cloud load distribution is activated.

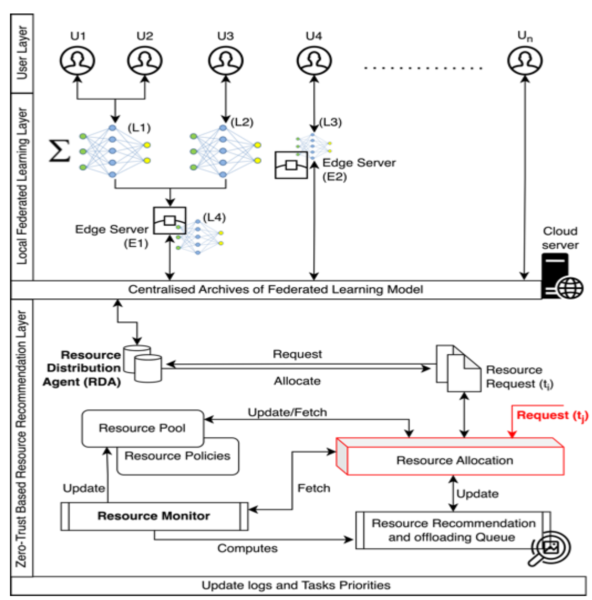

Fig. 1: Arcitecture representation of proposed system

The role of federated learning (FL) model in the proposed system is to enhance the quality of learning models involved in the training and validation phase for ZT scenario identification. The privacy of the medical users and the devices are at most concern in the open communication channel and hence the federated model assures the users privacy is preserved and index's are computed based on the reliability of the data and the accessing privileges of the users. As represented in Fig. 1, the individual learning models (L1) is a combination on two users (U1 and U2) whereas (L2) is derived from (U3) and further the (L4) is extracted from the learning of (L1) and (L2) accordingly. This multi-layer learning model extracts information and customizes the data via user authentication and permissions granted. The FL model assure the learning is computed and the process of privacy is secured via ZT scenario.

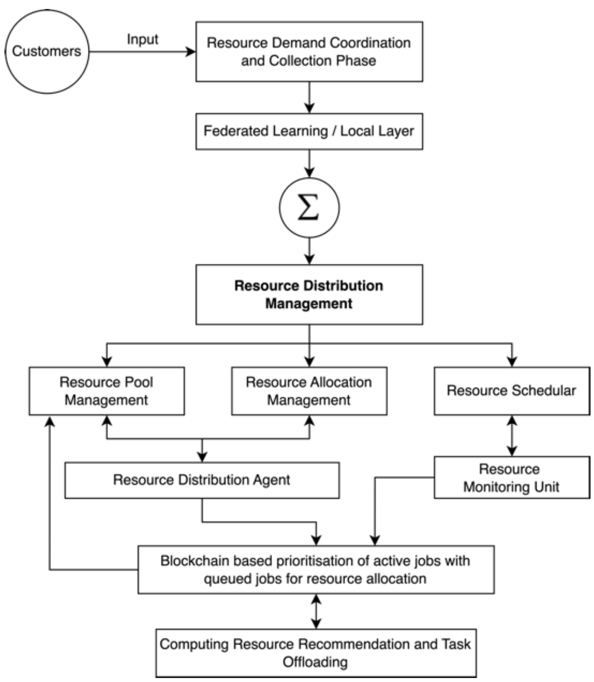

Fig. 2: Data/Control flow representation of proposed system

The activation of "Zero-Trust" scenario raises the auto activation of streamlining resource recommendation via Resource Distribution Agent (RDA). The agent contacts resource pool and resource allocation stack to monitor the current resource allocated and fabricated under the given time interval and thus extracts the relevant resource information with expected releasing in the thersholding time bond. This primary inclusion reflects on the resource catalog and hence most relevant medical resources are prioritized. At the Zero-trust scenario the trivial approach of resource allocation and resource scheduling is governed by the resource distribution agent (RDA). The process further streamlines the jobs/tasks associated to the expected resource availability and maps for ease in execution and thus on-hold jobs free from resource unavailability is executed. The Resource Monitor (RM) raises a trigger to control and coordinate the overall recommendation process and allocation process. The RM further assures the synchronization of resources pool at regular interval of time and thus over-due on the resources are released from the jobs. The priority fixing and policy governances are updated on regular intervals until the waiting time and resource pools are bounded above the threshold value. Typically, the governed policies are further updated and resource allocation in the section is primarily governed and monitored by the cloud distribution agent or RDA and resource monitor (RM). The federated learning approach is synchronized with each local federated layers configured to fetch a centralized federated learning model. The interdependency of resources requirements and resource allocation is justified and tracked using the block chain based informative system.

Table. 1: Mathematical model variables and description

Symbol	Description
(R)	Resource Recommendation
(ZT)	Zero Trust
(RDA)	Resource Distribution Agent
(U)	Users
(ω)	Weighted matrix variable
(FL_{local})	Federated learning model
(ES_i)	Edge Server
(R_M)	Resource Monitoring
(R_P)	Resource Pool
(R_S)	Resource Scheduling
(D)	Demand ratio
(B)	Block chain variables
(P)	Priority parameter

IV. RDA PREREQUISITES AND ZERO TRUST SCENARIO

The process of distributing resources in the trivial approach is considered as $\left(f(x) \Rightarrow f(R)/R \in R_1, R_2, R_3 \ldots\right)$ where (R) is the basic/existing resources allocation algorithm and the appended resource allocated under Zero-Trust (ZT) is redefined as $(f(R_{ZT})/\forall R_{ZT} \in R)$ and $(\forall R_{ZT} \rightarrow \sum(RDA))$ where (RDA) is the generalized term for resource distribution agent. The fundamental aspects of this approach are to define and customize the RDA such that $[\forall RDA \Rightarrow (f(R) \cup f(R_{ZT}))]$ where each allocation function is operated independently in the given zone. The customized representation further evaluates the process function from user (U) demand collection and thus represented as shown in Eq. 1.

$$f(R_{ZT}) = \lim_{n\to\infty}\left(\sum_{i=1}^{n}\sum_{j=i+1}^{n-1}\left\{\frac{\delta(U_i)\oplus\delta(R_{ZT})_j}{\delta t}\right\}\oplus\omega(R_{ZT})_j\right) \tag{1}$$

Where, User (U_i) extracts the zero trust ratio propositions at $(R_{ZT})_j$ with a correlated weight matrix (ω) for customizing the resource allocation patterns. In general, the fundamental parameters of $(\forall(R_{ZT})_j \notin \forall(R_{ZT})_{j+1})$ then the value of corelationship mapping are disconnected. This causes a large volume of data loss during the transmission phase. Technically, the zero-trust is accounted via RDA and thus $(ZT \Rightarrow RDA)$ and $\forall(R_{ZT} \subseteq R_{RDA})$ at given time (t).

The assigned learning patterns on the users (U) and the distributed resources (R) can be validated with the local federated learning model. The local FL models (FL_{local}) are a bi-product of integrating secondary learning patterns with the local edge users and devices. Typically defined as $(\forall R \Rightarrow f(FL_{local} \oplus FL_{Central}))$ where $(FL_{Central})$ is customized and functional into the operations of federated ecosystem for deriving patterns such as demand, resource allocation time, average waiting time, response time and the frequently requested devices/resources. Consider the user (U_i) are demanding the resources (R_i) in the time interval (t_i) such that $(\forall f(R_i) \Rightarrow U_1, U_2, U_3 \ldots U_i)$ and $(\forall f(R_i) \in f(R)/R \Rightarrow FL_{local})$ and (FL_{local}) is the local model learning associated with an edge-server (ES_i). The coordination results in data co-mapping and demand (D) validation such that $(\forall D \Rightarrow \exists ES_i \cup R_i)_t$ and learning function (FL_{local}) evaluates the RDA allocation as shown in Eq. 2.

$$RDA \Rightarrow \lim_{n\to\infty}\left\{\frac{\delta(R_i)}{\delta t_i} \cup \frac{\delta(FL_{local})_{ES_j}}{\delta t_j}\right\}_{(i,j)} \tag{2}$$

Where (FL_{local}) is bound with (ES_i) and thus, the learning weights (ω) of two entities are different at (t_i) and (t_j) and $(i \neq j \neq 0)$ for any given instances. Then the RDA allocation of (R_i) is validated with time (t_i) and (FL_{local}) with time (t_j) accordingly. The overall customization is further evaluated in federated learning based RDA model.

V. RESOURCE DISTRIBUTION AGENT (RDA)

The functional allocation of resources in generalized manner is represented as $f(R)$ whereas less than Zero-trust (ZT) is correlated with RDA as shown in Eq. 2. In further expansion, the RDA also monitors the front-end unit (i.e) the user-demand correlation and mapping and extends with back-end unit as the resource monitoring (R_M), resource pool management (R_P) and resource scheduler management (R_S) as shown in Fig. 2. The overall mapping can be represented as in Eq. 3. and Eq. 4 accordingly.

$$RDA = \sum(R_M \oplus R_P \oplus R_S)_n^{\infty} \tag{3}$$

$$\therefore f(RDA) \Rightarrow \left[\int_{n}^{\infty}\int_{n+1}^{k}\left\{\frac{\delta(R_M)_n \oplus \delta(R_S)_k}{\delta(R_P)_{n,k}}\right\} \oplus \Delta t_k\right] \tag{4}$$

Thus according to Eq. 4, the customization values of $f(RDA)$ are directly dependent on the (R_M) and (R_S) activation, whereas the time bound (t_k) is dependent on the resource availability and scheduled resources priority for further demand based allocation. The overall customization according to Eq. 4 is the resultant of RDA priority validation. Technically, the occurrence ratios of device allocated with resources are inter-dependent on the demand ratio (D) such that if $(D \Rightarrow f(R))$ and $(\forall f(R) < f(RDA))$ then (D) is executed with regular allocation process else $f(RDA)$ is activated, the Eq. 4 can be further represented as in Eq. 5 with $(t_j > t_i)$.

$$f(RDA) = \lim_{n\to\infty}\left\{\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left(\frac{\delta(R_M)_i \oplus \delta(R_S)_j}{\delta t_j}\right) \cup \Delta R_{P(i,j)}\right\} \quad (5)$$

According to Eq. 5, customization a variable of resource pool (R_P) becomes a decision making parameter as $(\forall R_{P(i,j)} \neq R_{Pi}, R_{Pj})$ i.e. $(\forall R_{Pi})$ there exists a demand (D_i) within time interval (t_i) and similarly (R_{Pj}) there exists demand (D_j). Thus according to $(\forall R_{Pi} \neq \forall R_{Pj})$ at (t_i, t_j) where a common resource pool is extracted in the interval as (R_{Pi}, R_{Pj}) as shown in Eq. 5. Thus the RDA allocates optimized resource to the demanded users with respect to zero-trust policies.

ALGORITHM - 1: RDA

Input: $f(R)$, $f(RDA)$

Step 1: Compute resource monitoring (R_M), resource pool management (R_P) and resource scheduler management (R_S)

Step 2: if $f(RDA)$

Then $RDA = \sum(R_M \oplus R_P \oplus R_S)_n^\infty$

Else

$$f(RDA) = \lim_{n\to\infty}\left\{\sum_{i=1}^{n}\sum_{j=i+1}^{n}\left(\frac{\delta(R_M)_i \oplus \delta(R_S)_j}{\delta t_j}\right) \cup \Delta R_{P(i,j)}\right\}$$

Step 3: on $(t_j > t_i)$

Assign $(\forall R_{P(i,j)} \neq R_{Pi}, R_{Pj})$

Step 4: validate condition $(\forall R_{Pi} \neq \forall R_{Pj})$ at (t_i, t_j)

Step 5: Generate blockchain $(B = B_1, B_2, B_3 ...)$

VI. BLOCKCHAIN BASED PRIORITIZATION OF ACTIVE RESOURCES AND ALLOCATION

The activated resource pool (R_P) synchronizes with the corresponding values of resource demand and scheduler indexing to retrieve block value data from the hashing blockchain structure. The incoming values of resource request is collected and stored within the block-array as shown in Fig. 03. The functional values of each blockchain component are associated with the parent hash and the successive block hashing address. Typically there are two types of blocks associated in proposed system. The primary is the demand requesting blocks and second is demand allocated blocks. The two blocks are correlated within the line of operation with respect to the servicing parameter. The basic blockchain (B) is collected as $(B = B_1, B_2, B_3 ...)$ such that $(\forall B_i \in f(R) \in f(RDA))$ at given instance of time (t). The interdependent block values are further associated with blocks requesting (B_Q) and block allocated (B_A).

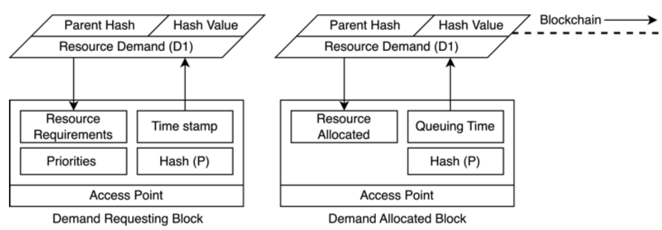

Fig.3: Block diagram of active blockchain model

The blockchain is thus constructed to assure the interconnected recommendations and resource allocations are connected and access point is evaluated. The process of blockchain is described in Fig. 3, with a demand allocation block supplied with a demand requesting block. The functional value of (B_Q) and (B_A) are bounded with a relationship matrix $(\Delta\mathrm{T})$, where $(\Delta\mathrm{T})$ assures the operations of two multi-units blocks associated with a given resource parameter as shown in Eq. 6.

$$\Sigma(B) \Rightarrow \int_0^n \frac{Gen(B_Q) \oplus \delta f(R)}{\delta t_i} \cup \int_n^\infty \frac{Gen(B_A) \oplus \delta f(RDA)}{\delta t_j} \tag{6}$$

$$\therefore \Sigma(B) \Rightarrow \lim_{n\to\infty}\left[\sum_{i=1}^{n}\sum_{j=n}^{\infty}\left(\frac{Gen(B_{Qi})}{\Delta\mathrm{T}} \oplus f(RDA)\right) \cup \left(\frac{\delta Gen(B_{Aj})}{\delta t_j}\right)\right] \tag{7}$$

$$\therefore \Sigma(B) \Rightarrow \lim_{n\to\infty}\left[\sum_{i=1}^{n}\sum_{j=n}^{\infty}\left(\log_n\left[Gen(B_{Qi})\right]\right) \cup \left(\frac{\delta Gen(B_{Aj})}{\delta t_j}\right)\right] \tag{8}$$

$$\therefore \Sigma(B) \Rightarrow \lim_{n\to\infty}\left[\frac{1}{t}\sum_{i,j}\left(\frac{\left(\log_n\left[Gen(B_{Qi})\right]\right) \cup \delta Gen(B_{Aj})}{\Delta\mathrm{T}}\right)\right] \tag{9}$$

Thus according to Eq. 6 the, $\left(f(R) \Rightarrow f(RDA)\right)$ such that if $f(RDA)$ is activated, the block structure is designed to generate (B_Q) block with regular $f(R)$ resource allocation patterns whereas (B_A) is done using $f(RDA)$ algorithm. Technically, the generation of (B_Q) block activates the collection of datasets and further activates (B_A) on resource allocation paradigm. The consolidated representation is demonstrated with Eq. 9 on the block generation.

VII. TASK OFFLOADING AND RESOURCE RECOMMENDATION MODEL

The blockchain computation as shown in Eq. 9, the $\Sigma(B)$ further expands to extract the thersholding parameter on priorities (P) where $(\forall B_i \Rightarrow P_i / P_i \neq 0)$ and $(\forall P_i \subseteq \delta f(R))$ and $\left(\forall f(RDA) \Rightarrow (B_Q)_i\right)$ such that $(B_Q)_i \Rightarrow (B_A)_j\, at(t_j)$. Thus according to the order of blocks the (B_Q) is followed by (B_A) at two distinct intervals of time (i, j). The process of prioritization is further assigned as $\left(B = B_{1(P1)}, B_{2(P2)}, B_{3(P3)}....\right)$ and the order of intervals in priorities is further evaluated as shown in Eq. 10.

$$\Sigma(P) \Rightarrow \lim_{n\to\infty}\left[\left\{\frac{\delta(B_A)_i \oplus \delta(P_i)}{\delta t_i}\right\} \cup \left\{\frac{\delta(B_Q)_j \oplus \delta(P_j)}{\delta t_j}\right\}\right] \tag{10}$$

The order of evaluation and priority extraction is labeled as $\left(\forall (B_Q)_i \Rightarrow P_i\right)$ and $\left(\forall (B_A)_j \Rightarrow P_j\right)$ such that $(P_j \neq P_i)$ as the relative alignment of blocks are independent of time (t). Typically, the priorities (P) are further justified as Eq. 11.

$$\Sigma(P) \Rightarrow \mathrm{Re}\,cmd\left[\left\{\frac{\delta(B_A)_i \oplus \delta(B_Q)_j}{\delta t}\right\} \cup \left\{\Sigma\left(P_{(i,j)}\right)\right\}\right] \tag{11}$$

Thus according to Eq. 11, the recommendation of priorities in resource allocation and scheduling is aligned accordingly. Consider the parameters as in Eq. 11, the blockchain is redistributed as per Eq. 9 and the cycle is confined until the recommendation order of task-offloading is reached. In general, the task offloading process is activated within the blockchain (B_Q) and (B_A). The recommendation mode is subjected as below.

$$\mathrm{Re}\,cmd(R) \Rightarrow \lim_{n\to\infty}\left[\left\{\frac{\delta(B_A)_i \oplus \delta(B_Q)_j}{\Delta\mathrm{T}}\right\}_{(i,j)} \otimes \cup \left\{\frac{\delta(P_i \oplus P_j)}{\delta t_j}\right\}_{(i,j)}\right] \tag{12}$$

According to Eq. 12, the functional values of each recommendation variables (B_Q) and (B_A) are dependent on priorities (P_j, P_i) at two distant time instances. The medical priorities on resources are extended and validated for effective sharing. The resultant observation and validation is discussed in successive section.

VIII. RESULTS AND DISCUSSIONS

In this section, the zero-trust scenario of edge-node and edge-server communication is validated. The process of resource allocation and distribution is monitored and streamlined as per the RDA and RM as discussed in previous sections.

A. *Experimental Setup*

The implementation is setup on 500 IoMT users/costumers participating in federated local model learning process under the edge server. The users are grouped with a cluster of edge connectivity ratio and computed on the local resources independent on the centralized federated server setup. The central server is processed on intel i7-770HQ CPU with 32GB RAM and NVIDIA A100 Tensor Core GPU cards. The computational servers are aided with the clusters of master and worker nodes configuration under kubernetics for effective resource pooling and resource monitor configurations. The generic customization for cloud-IoMT configuration and third party communication protocols are standard in the setup and experimental process.

B. Validations and Observations

In Fig. 4, we have demonstrated a primary goal of training and validating the users/costumers in the IoMT framework for Medical User recognition. The training and validation is conducted in three scenarios and 60:40 is consolidated for further processing.

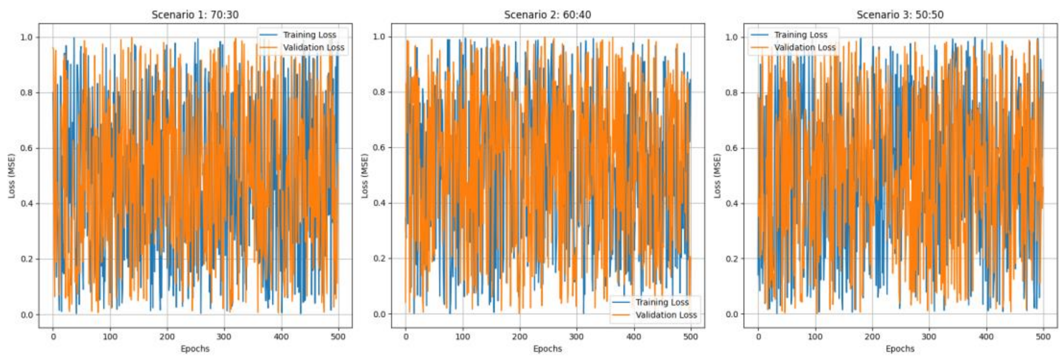

Fig. 4: Training and validation model of IoMT consumer devices in Federated Learning Model (Centralized)

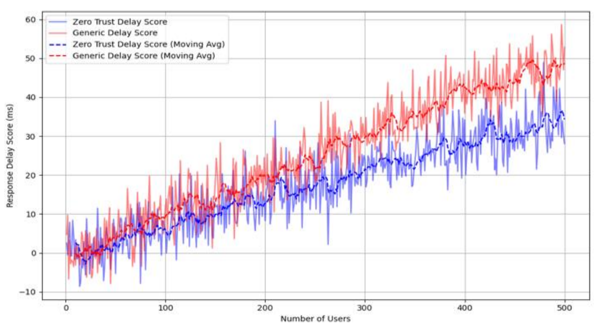

Fig. 5: Representation of ZT and Non-ZT based communication and delay score

The Zero-Trust (ZT) enabled processing of resource allocation via blockchain is demonstrated in Fig. 5 and Fig. 6 accordingly, the customization of ZT and non-ZT (i.e.) generic approach's delay score is computed and validated. The outcome is represented with the overall ZT based communication channel with minimal delay as the user's/consumers density is increased. Whereas the execution stream of 50 processes is represented in Fig. 6 and the proposed ZT channel has demonstrated a close improvisation in delay time compared to the existing approach. The delay change improvisation is predominated with maximizing the user density.

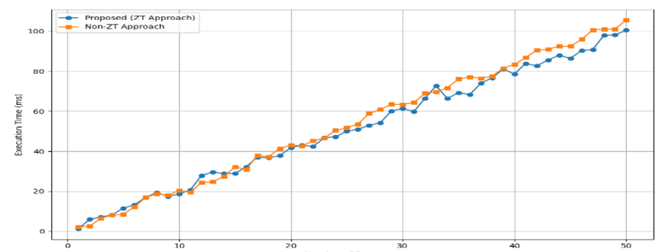

Fig. 6: Processes/Task distribution with respect to execution time for the ZT and non ZT approach

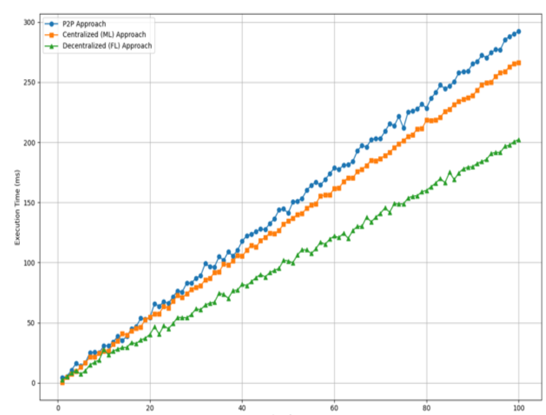

Fig. 7: Processes/Task distribution with respect to execution time for P2P, Centralized and Distributed (FL) models

The process distribution and execution time for 100 tasks is demonstrated in Fig. 7 under regular Peer-to-Peer (P2P) communication approach, machine learning i.e. centralized approach and federated learning i.e. decentralized approach [21]. The representation has secured the minimal execution time in Federated Learning model as the edge-devices compute the initial resource recommendation and streamlines the logs of resource allocation to centralized unit for effective scheduling. Whereas in Fig. 8, a snapshot of maximum 20 processes/tasks is demonstrated for ease. The performance matrix is derived from Fig. 7 with an addition to CPU/GPU occupancy and performance ratio computation. The representation secures a safe-zone computation of CPU/GPU occupancy with the GPU performance over dominating the CPU under allocation process.

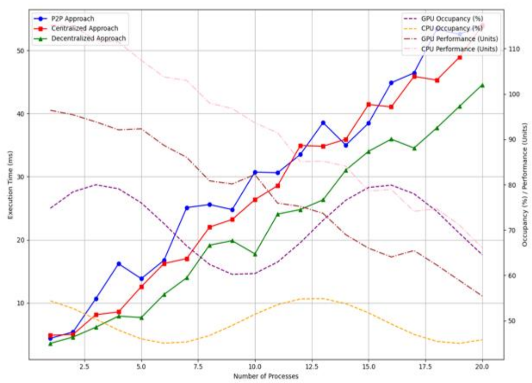

Fig. 8: CPU/GPU occupancy and performances estimation with respect to the process/tasks execution time.

Table.2: Comparative analysis on Average Latency in resource offloading and recommendation process

Scheme	Configuration	Performance Matrix	Average Latency (ms)	Accuracy (%)
LSCCOA [18]	CPU/300MHz User:1200 Network: LTE	Throughput: 1166.2 bps	39592	88.32
Zero-Trust-Edge[19]	CPU/1.4 GHz Users: 100 Network: P2P + WiFi	Throughput: 7.5 Mbps	3000	93.76
Proposed FL/Blockchain based ZT schema	CPU: 1.4 GHz GPU: A100 Tensor Core Users: 500 Network: 4G(LTE)+ WiFi + 5G	Throughput: 28.4 Mbps	4G/LTE: 1278 5G: 785	94.92

In this approach, the resource scheduling and task offloading recommendation is predominantly discussed and validated. The overall user/consumer recommendation of the resources and comparison with existing infrastructure and technique is shown in Table. 2. The proposed blockchain based FL model on ZT channel has scored the minimal latency of 1278ms in 4G/LTE network and 785ms on 5G network of the IoMT users. Typically, the recommendation model has secured higher band of resource allocation and optimization with effective scheduling. The use of GPU in the setup has added an advantage for improvising the latency compared to the trivial CPU setup of computation [20]. The proposed system has leveraged the use of blockchains authentication and mapping with federated learning to secure Zero-Trust scenario of Medical information computing.

The proposed framework is developed with an objective to enhance the social relevance in cyber-physical systems such as improvising the data communication channel via Zero-Trust communication scenarios. The model has successfully demonstrated the effective utilization on distributing the resources and computation layers across the edge-devices such as IoMT/IoT and the centralized computation servers for developing a global training model. The federated learning model, developed in local (edge) and global (servers) are effective in handling the resources and thus contributing in reducing the global carbon foot-print contribution.

IX. CONCLUSION

The proposed system has validated the task offloading and priority based resource recommendation for medical applications under zero-trust architecture design and observed under 5G spectrum. The proposed system has validated the simulative framework of task categorization via blockchain based federated learning environment. The selective tasks are successfully aligned under the resource distribution agent (RDA) and the proposed blockchain based task prioritization algorithm. The active and time locked tasks are identified via blockchain active model approach to customize the task-offloading and provide a reliable recommendation model. The proposed system has demonstrated minimal latency in task-offloading from regular scheduling approach to the RDA based scheduler. The latency effectiveness is accompanied with minimal false-positive recommendations, high detection rate and low operational cost for 5G spectrum. In near future, the approach can be integrated and tested on 6G networks for effective resource scheduling and recommendation under interoperable communication channels and operating standards.

Acknowledgement: The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Group Project under grant number (RGP.2/556/45). This research is supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R195), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCE

[1] Wang, B., Wang, C., Huang, W., Song, Y., & Qin, X. (2020). A survey and taxonomy on task offloading for edge-cloud computing. IEEE Access, 8, 186080-186101.
[2] Kim, S. (2020). New application task offloading algorithms for edge, fog, and cloud computing paradigms. Wireless Communications and Mobile Computing, 2020, 1-14.
[3] Cai, J., Liu, T., Wang, T., Feng, H., Fang, K., Bashir, A. K., & Wang, W. (2024). Multi-source fusion enhanced power-efficient sustainable computing for air quality monitoring. IEEE Internet of Things Journal.
[4] Wang, E., Yang, Y., Wu, J., Liu, W., & Wang, X. (2018). An Efficient Prediction-Based User Recruitment for Mobile Crowdsensing. IEEE Transactions on Mobile Computing, 17(1), 16-28. doi: 10.1109/TMC.2017.2702613.
[5] Fang, K., Chen, J., Zhu, H., Gadekallu, T. R., Wu, X., & Wang, W. (2024). Explainable-AI-based two-stage solution for WSN object localization using zero-touch mobile transceivers. Science China Information Sciences, 67(7), 170302
[6] Zuo, C., Zhang, X., Yan, L., & Zhang, Z. (2024). GUGEN: Global User Graph Enhanced Network for Next POI Recommendation. IEEE Transactions on Mobile Computing, 23(12), 14975-14986. doi: 10.1109/TMC.2024.3455107
[7] S. T. Ahmed, V. V. Kumar and J. Jeong, "Heterogeneous WorkloadBased Consumer Resource Recommendation Model for Smart Cities: eHealth Edge–Cloud Connectivity Using Federated Split Learning," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 4187- 4196, Feb. 2024.
[8] Dai, S., Wang, M. L., Gao, Z., Huang, L., Du, X., & Guizani, M. (2019). An adaptive computation offloading mechanism for mobile health applications. IEEE Transactions on Vehicular Technology, 69(1), 998-1007.
[9] Yadav, R., Zhang, W., Elgendy, I. A., Dong, G., Shafiq, M., Laghari, A. A., & Prakash, S. (2021). Smart healthcare: RL-based task offloading scheme for edge-enable sensor networks. IEEE Sensors Journal, 21(22), 24910-24918.
[10] Dong, C., Sun, Y., Shafiq, M., Hu, N., Liu, Y., & Tian, Z. (2023). Optimizing Mobility-Aware Task Offloading in Smart Healthcare for Internet of Medical Things Through Multi-Agent Reinforcement Learning. IEEE Internet of Things Journal.
[11] Han, F., Yang, P., Du, H., & Li, X. (2024). Accuth+: Accelerometer-Based Anti-Spoofing Voice Authentication on Wrist-Worn Wearables. IEEE Transactions on Mobile Computing, 23(5), 5571-5588. doi: 10.1109/TMC.2023.3314837
[12] Li, J., Zhu, M., Liu, J., Liu, W., Huang, B., & Liu, R. (2024). Blockchainbased reliable task offloading framework for edge-cloud cooperative workflows in IoMT. Information Sciences, 668, 120530.
[13] Wu, C. K., Cheng, C. T., Uwate, Y., Chen, G., Mumtaz, S., & Tsang, K. F. (2022). State-of-the-art and research opportunities for next-generation consumer electronics. IEEE Transactions on Consumer Electronics, 69(4), 937-948.
[14] Alekseeva, D., Ometov, A., & Lohan, E. S. (2022, October). Towards the advanced data processing for medical applications using task offloading strategy. In 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 51-56). IEEE.
[15] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE Internet of Things Journal, 8(13), 10248-10263.
[16] Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A maturity framework for zero-trust security in multiaccess edge computing. Security and Communication Networks, 2022.
[17] Chi, H. R., de Fátima Domingues, M., Zhu, H., Li, C., Kojima, K., & Radwan, A. (2023). Healthcare 5.0: In the perspective of consumer Internet-of-Things-based fog/cloud computing. IEEE Transactions on Consumer Electronics vol. 69, no. 4, pp. 745-755, Nov. 2023.
[18] Anajemba, J. H., Yue, T., Iwendi, C., Alenezi, M., & Mittal, M. (2020). Optimal cooperative offloading scheme for energy efficient multi-access edge computation. IEEE Access, 8, 53931-53941.
[19] 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.
[20] Kumar, Y., & Singla, R. (2021). Federated learning systems for healthcare: perspective and recent progress. Federated Learning Systems: Towards Next-Generation AI, 141-156.
[21] Ali, B., Gregory, M. A., Li, S., & Dib, O. A. (2024). Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing. Computer Networks, 241, 110197.
[22] Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors, 24(4), 1328.
[23] Javeed, D., Saeed, M. S., Adil, M., Kumar, P., & Jolfaei, A. (2024). A federated learning-based zero trust intrusion detection system for Internet of Things. Ad Hoc Networks, 162, 103540.
[24] Ahmed, S. T., Kumar, V. V., Singh, K. K., Singh, A., Muthukumaran, V., & Gupta, D. (2022). 6G enabled federated learning for secure IoMT resource recommendation and propagation analysis. Computers and Electrical Engineering, 102, 108210.
[25] Liu, Y., Su, Z., Peng, H., Xiang, Y., Wang, W., & Li, R. (2024). Zero Trust-Based Mobile Network Security Architecture. *IEEE Wireless Communications*, *31*(2), 82-88.