Cloud-Fog Interoperability in IoT-enabled Healthcare Solutions

Redowan Mahmud, Fernando Luiz Koch, Rajkumar Buyya
Cloud Computing and Distributed Systems (CLOUDS) Laboratory
School of Computing and Information Systems
The University of Melbourne, Australia.

ABSTRACT

The issue of utilizing Internet of Things (IoT) in Healthcare solutions relates to the problems of latency sensitivity, uneven data load, diverse user expectations and heterogeneity of the applications. Current explorations consider Cloud Computing as the base stone to create IoT-Enable solution. Nonetheless, this environment entails limitations in terms of multi-hop distance from the data source, geographical centralized architecture, economical aspects, etc. To address these limitations, there is a surge of solutions that apply Fog Computing as an approach to bring computing resources closer to the data sources. This approach is being fomented by the growing availability of powerful edge computing at lower cost and commercial developments in the area. Nonetheless, the implementation of Cloud-Fog interoperability and integration implies in complex coordination of applications and services and the demand for intelligent service orchestrations so that solutions can make the best use of distributed resources without compromising stability, quality of services, and security. In this paper, we introduce a Fog-based IoT-Healthcare solution structure and explore the integration of Cloud-Fog services in interoperable Healthcare solutions extended upon the traditional Cloud-based structure. The scenarios are evaluated through simulations using the *iFogSim* simulator and the results analyzed in relation to distributed computing, reduction of latency, optimization of data communication, and power consumption. The experimental results point towards improvement in instance cost, network delay and energy usage.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; • **Networks** → Network reliability;

KEYWORDS

Internet of Things, HealthCare, Fog computing, Cloud computing, Interoperable architecture

1 INTRODUCTION

In recent years, the concept of IoT has been widely adopted on different aspects of Healthcare specially in applications that involve ubiquitous sensors and actuators communicating through Wireless Sensor Network (WSN) along with solutions for real-time data analysis and recommendation. When applied in critical scenarios, the services are very latency-sensitive and demand faster processing of the generated data [18]. Moreover, the large utilisation of sensors, mobility, and geographic distribution lead to issues of data volume, velocity, and variation, along with requirements for accuracy, security, Quality of Service (QoS), user expectations, and operational costs [6].

Cloud computing services have been widely accredited to support IoT-enabled Healthcare solutions, as presented in [4, 12, 19, 23, 24], providing solutions for scalability, data analysis and reliability [14]. However, the geographical centralisation of Cloud data centres requires that data collected from sensors to be transmitted through multi-hop distance for processing, which adversely affects the latency sensitivity of the solutions. Moreover, management of Cloud resources in heterogeneous Healthcare environments require complex management tasks to avoid continuous revision of that resource allocation in response to uneven and uncertain data loads coming from Healthcare solutions.

Fog computing is a promising solution in this scenario by exploring lightweight and customisable supplementary computing resources closer to the IoT data source in Healthcare solutions [15]. In this solution, traditional edge computing devices such as switches, routers, low-profile computing devices, etc are equipped with computational infrastructure, services, and management models to implement local lean applications [3]. As result, some data processing can executed closer to the data source, distributing resource demands, reducing the need for multi-hope data communication, reducing latency, and promoting service flexibility. Although Fog resources are constrained in terms of energy and computational power, they are flexible enough to customise according to the application context. The complexity arising in managing and operation distributed computing scenarios, cope with the combination of variable demands and constrained computing resources, ensure performance, stability, and security.

Several applications of Fog computing in Healthcare solutions exist in the literature, such as [1, 21, 22]. However, there is still a demand for methods to promote interoperability of services that would allow for settle applications directly from Cloud elements into Fog elements coping with the inherent architectural differences. In this context, the contribution of the paper is listed as:

- A Fog-based IoT-Healthcare solution structure (system architecture and application model) that is interoperable with general Cloud-based Healthcare solutions.

- A reference architecture for Cloud-Fog service integration and orchestration from the perspective of interoperable IoT-Healthcare solutions.
- Performance evaluation of Fog-based IoT-Healthcare solutions through simulation studies using *iFogSim* [8] in respect of deadline satisfied service delivery, cost, energy usage and service distribution.

The paper is organized as follows: Section 2 presents the motivation through an analyze of the state-of-the-art and Section 3 describes the general Cloud-based and proposed Fog-based Healthcare solution structure. Section 4 introduces a integrated reference architecture of Cloud-Fog platform for IoT-Healthcare. Then, In Section 5, performance evaluation of the proposed solution in different use configurations through simulation scenarios developed upon *iFogSim*. The paper concludes with Section 6.

2 MOTIVATION

Table 1: Summary of the literature study

Work	Cloud-based	Fog-based	Interoperable (Cloud ⇌ Fog)
Doukas et al. [4]	✓		
Renta et al. [23]	✓		
Mahmud et al. [19]	✓		
Chen et al. [12]	✓		
Zhang et al. [24]	✓		
Fazio et al. [13]	✓		
Peddi et al. [20]	✓		
Jindal et al. [11]	✓		
Muhammad et al. [7]	✓		
Gupta et al. [9]	✓		
Hossain et al. [10]	✓		
Gia et al. [21]		✓	
Gia et al. [22]		✓	
Ahmad et al. [1]	✓	✓	
Chakraborty et al. [17]	✓	✓	
Dubey et al. [5]	✓	✓	
Negash et al. [16]		✓	
Rahmani et al. [2]		✓	
Interoperable Cloud-Fog IoT-Healthcare (This work)		✓	✓

Table 1 provides a brief summary of our survey on the state-of-the-art in applying Cloud and Fog Computing paradigms in Healthcare solutions. As observed, there is a growing interest in the utilization of Fog computing in IoT-Healthcare solutions, however a clear predominance around Cloud-based approaches.

Gia et al. [21] presents a Fog computing based health monitoring system equipped with data mining, storing and notification facilities at the edge of the architecture. The authors explored the applicability of such arrangement in ECG feature extraction. A template based feature extraction technique is used in smart gateways to analyse the ECG signals. The experimental results indicate to efficient bandwidth usage and service delivery.

Doukas et al. [4] presents the online data management and processing of IoT-enabled pervasive healthcare applications on Cloud. The implemented prototype receives patient data from the IoT devices and forwards to the Cloud for processing. Security issues are observed during every communications among the entities. Representational State Transfer (REST) API based access, scalability

and inter-application interoperability are considered as the main features of the prototype.

Renta et al. [23] focuses on storing Healthcare data received from distributed IoT devices to remote Cloud. The data management system lets the IoT devices to collect user critical data in real-time. Cloud-enabled techniques ensure faster processing of the stored data so that subscribed users can get quick notification during emergency. An alert service also runs in the system based on the predefined health rules and users reaction plan.

Mahmud et al. [19] presents a framework that enables data analysis and visualization for predicting health-shocks based on predefined health dataset. The framework is based on Cloud computing platform. It incorporates Amazon web services (AWS), geographical information systems (GIS) and Fuzzy rule based summarization technique. The framework can classify health-shocks with interpretability and accuracy using a data model. Besides it can explain the causal factors of health-shocks through linguistic rules.

Chen et al. [12] targets the security aspects of medical data sharing through Cloudlet. Encryption is used in data collection. A trust model is developed to identify reliable destinations (hospital, doctor chambers, etc.) for sharing the data. The trust model helps to connect patients and medical professionals as well. In the data sharing destinations, data are segmented into three parts to store in remote Cloud. In the whole process an Intrusion Detection System (IDS) works actively to prevent malicious attacks.

Zhang et al. [24] proposes a patient-centric cyber-physical system named Health-CPS aiming to ensure convenient and efficient Healthcare service. The Health-CPS solely depends on Cloud computing and data analytics to handle the Big data related issues of different Healthcare applications. The system is composed of several layers such as data collection layer, data management layer and data oriented service layer. The system collects data in a unified standard. It supports distributed storage and parallel processing.

Fazio et al. [13] designs an e-health Remote Patient Monitoring (RPM) system in a Cloud platform named FIWARE. The authors emphasize to speed up the development of the RPM system with the facilities provided by FIWARE. The system targets to assist the patients and optimize the responsibilities of the medical professionals. The association of FIWARE Cloud to the RPM system enhances modularity, scalability and flexibility.

Peddi et al. [20] proposes a Cloud-based mobile e-health calorie system. The system is able to classify different food objects from the meal and with high accuracy can compute the overall calorie. The system incorporates computation offloading from Mobile e-health applications to the Cloud. In Cloud, it employs a broker entity to manage the resources efficiently so that accurate outcome can be generated in tolerable latency. The broker imposes dynamic cloud allocation mechanism to engage and free computing instance in real-time according to the demand.

Jindal et al. [11] propose a technique to calculate heart rate using the smart phone embedded sensors (accelerometer) and Photo-PlethysmoGraphy (PPG) signals. The technique is composed of three step data processing. Later, the technique requires Cloud association to select perfect PPG signals through deep learning mechanisms and classify the signals to estimate heart rate. The technique is evaluated by processing the TROIKA dataset. According to the authors, the technique is able to predict heart rate accurately.

Muhammad et al [7] discusses an IoT-Cloud-based Healthcare solution for voice pathology monitoring of the users. The proposed solution incorporates a voice pathology detection system that applies local binary pattern on voice signal represented through Mel-spectrum technique. A machine learning classifier is also used to conduct the pathology. According to the authors, the association of Cloud computing improves the accuracy and the accessibility of the Healthcare solution to a certain extent.

A Cloud-based IoT-enabled predictive physical activity analysis model for the users is discussed by Gupta et al. in [9]. The model encompasses embedded sensors, Cloud computing and XML Web services for faster, secure and reliable data collection, processing and communication. The model is evaluated from different perspectives (service adaptation, prediction analysis, efficiency and security). The model also enables alert to the ailing person notifying abnormality or complications during physical activity.

The impact of Healthcare Industrial IoT (HealthIIoT) in observing real-time health issues of aged and disable people is discussed by Hossain et al. in [10]. HealthIIoT is able to monitor, track, and store users healthcare data for consistent treatment. The HealthIIoT-enabled framework collects ECG data from smart phones and other sensors. Later send the collected to the cloud so that Doctors can access and assess the data seamlessly. Cloud-based data analytics is used to detect the abnormality and error of the health data.

Another work of Gia et al.[22] presents a Fog-based health monitoring system that can provide consistent remote monitoring of cardiac patients at low cost. The system is comprised of energy efficient IoT sensors and smart gateways. The sensors collect ECG, respiration rate and body temperature data and wirelessly send to the gateways for automatic analysis and notification. Besides, it can assist in visualizing the outcome in an effective and re-usable way.

Ahmad et al. [1] proposes a Fog-based Healthcare framework. The framework acts as an intermediate layer between the Cloud and end IoT devices. It enhances data privacy and security at the edge level along with Cloud Access Security Broker (CASB). In Fog environment, the framework can be deployed in a modular approach. In addition the framework is capable of aggregating data from multiple sources with adequate cryptographic assessment.

Chakraborty et al. [17] discusses a Fog-based computation platform that can deal with latency-sensitive Health data. A programming model is proposed to handle geographically distributed large scale Healthcare applications. The model is evaluated through processing of heart rate related Healthcare data. According to the authors, the proposed Fog-based Healthcare solution improves data accuracy, service delivery time and retains data consistency.

Dubey et al. [5] discusses about service oriented architecture of Fog computing to validate and evaluate raw health data sensed through IoT devices. In the proposed system, resource constrained embedded computing instances conduct the data mining and the data analysis. The instances are also responsible to identify important patterns form the Health data and forward them towards Cloud for further storage and usage. The basic intension of the work is to highlight the big data processing with low power Fog resources.

Negash et al. [16] focuses on implementing a smart e-health gateway for Fog computing to assist IoT-enabled Healthcare services. Such smart e-health gateways are placed in geographically distributed network and each gateway is responsible to manage a set of IoT devices directly associated with the patients. The cluster of smart e-health gateways are supported with data analytics and adaptive configurations. The proposed system is able to monitor the patients independent to his/her movement.

Another Fog-based smart e-health gateway is presented by Rahmani et al. in [2]. The authors exploit possible placement of smart e-health gateway so that it can offer real-time local storage, data processing and data analysis. The Fog-based system can effectively cope up with mobility, energy and reliability related issues. Based on the concept a prototype of smart e-health gateway named UT-GATE is also developed. An IoT-based Early Warning Score (EWS) is used to evaluate the performance of the system.

We observed that there is an opportunity to contribute with studies around the interoperability between Cloud and Fog-based platforms. We target a Fog-based IoT-Healthcare solution where both the system architecture and application model follows the Cloud-like structure to promote the interoperability. Besides, we explore how Cloud-Fog interoperable IoT-Healthcare solution structure can lead towards enhanced service integration and orchestration.

3 HEALTHCARE SOLUTION STRUCTURE

In this section, at first based on the literature study, we discuss a general structure (system architecture and application model) of the Cloud-based IoT-Healthcare solutions. Later, a Fog-based IoT-Healthcare solution structure in proposed which can be interoperable with the Cloud-based solutions.

3.1 General Cloud-Based Solutions

Almost every Cloud-based IoT-Healthcare solution follows a common system architecture and application model. They only differs from the functionality of the applications.

The **system architecture** of a Cloud-based IoT-Healthcare solution (Fig. 1) is usually comprised of several entities;

IoT sensors or wearable devices: In Healthcare solution, hand held or body connected devices for example; pulse oximeter, ECG monitor, smart watches, etc. perceive health context of the users. These devices can connect themselves with other user premises equipment through Bluetooth, ZigBee and Infrared transmission. Generally the data sensing frequency of these devices are fixed and seamlessly generate health data once turned on. However, most of such devices are subject to resource and energy constraint.

Smart phones: Smart phones are used in many Healthcare solutions significantly. Since IoT devices are lack of networking and processing capabilities, Smart phones assist them in providing application interface and sending generated data towards Cloud datacentre. Smart phones maintain a persistent communication with the IoT devices to receive the sensed data. The data receiving frequency of smart phones can be adjustable through the application. The embedded sensors on Smart phone like accelerometer, Global Positioning System (GPS), etc. can perceive the contextual data.

Cloud datacentre: The Cloud datacentre is the premier platform for IoT-enabled Healthcare solutions. In addition to large scale computation, it facilitates storage, utility services with reliability and scalability. Cloud resources (computational infrastructure, services, etc.) are orchestrated in a structural way and are virtualized. The components within a Cloud datacentre those assist in Healthcare
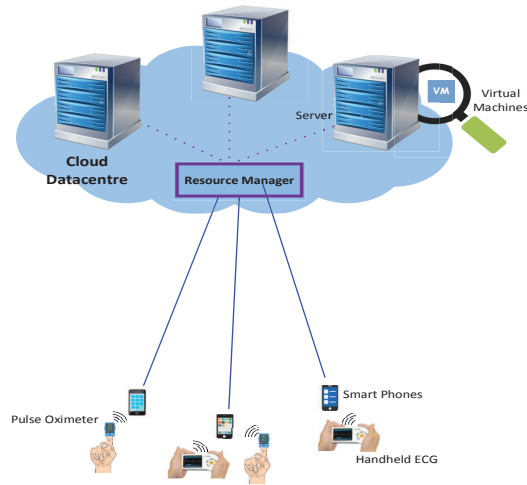
Figure 1: Cloud-based Healthcare system architecture

solutions can be listed as follows:

• *Resource Manager:* Resource manager is responsible for coordinating the Cloud resources while dealing with IoT-enabled Healthcare data. It actually deploys, manages and monitors both the infrastructures and services that made-up the Healthcare solution. It can schedule, terminate and scale the resources according to the demand, load and context. It also ensures higher level access control to the resources. In addition, Resource Manager defines the dependencies between resources so that they can be run and executed in the correct order.

• *Servers:* The Cloud datacentres encapsulate a set of Servers that can either be homogeneous or heterogeneous in respect of hardware configurations (memory, cores, capacity, and storage). In Cloud-based Healthcare system, two types of Servers are used predominantly; *Application Server* and *Database Server*. In Application Server the backend applications, web-services are hosted whereas Database Server solely handles the data repository and associate operations. In a Server, a group of policies set by the Resource Manager is implemented for allocating bandwidth, memory and storage to the residing instances. The Sever-applied policies include important information regarding the type of processing cores, database sharding and their mutual sharing or replication among the instances. Service provisioning and load balancing policies are also observed within the server.

• *Virtual Machines:* Instances within a Server is termed as Virtual Machines (VM). Each VM has access to the hardware resources provided by the host Server. A VM itself encapsulates some metadata regarding accessible memory, processor and storage size. In Healthcare solutions, relevant applications and web services are run in the VMs of Application server. The large volume of Health data are managed distributively within the VMs of Database server. While operating a Healthcare solution, allocated instances of both types communicate simultaneously. Images of the operating VMs can be replicated so that the Healthcare solutions can be made fault tolerant to a certain extent. Migration of the tasks are also possible among the VMs.

Like the system architecture, the **application model** of different Cloud-based Healthcare solutions are also similar. The generalized model of Cloud-based Healthcare applications can be described through a flowchart as show in Fig.2.

The Cloud-based Healthcare application are usually divided in to two parts. One part runs in the Smart phones of the users and another part executes in the VMs of Cloud. At the initiation of the application in user's Smart phone, it asks for the authentication information. It can include user password, biometric recognition. Not only in the Smart phones, this authentication information is also applied to the Cloud for privacy protection.

Through the application, Smart phones are seamlessly connected with the IoT sensors or wearable devices to receive Health data of the users. Smart phones itself can perform some preprocessing over the data. However, for extensive processing, the data is sent to the Cloud securely. The secured transfer of data can be ensured through application and network centric cryptography.

In the VMs of Cloud, the other part of the application receives data from the authorized Smart phones and conduct data abstraction. Through data abstraction, essential information are extracted from the raw sensed data and represented in a simplified form so that they become suitable for further analysis.

At the later phase, data analysis is conduct. Data analysis can include aggregation of users historical data, data mining, pattern recognition, feature extraction, template matching techniques. In this case, association of relevant information from data repository of the Healthcare solution can be required. In some cases, external third-party software services are also used for analysing the data.

After analyzing the data, users Health condition is evaluated based on the outcome of the analysis. This evaluation can be done either by comparing the analysed data result with predefined statistics or by direct association of the medical professionals.

The final outcome of the Healthcare application can be a data tuple of the user's Health context or a notification message to the users. In general, the Health context is preserved for consistent monitoring of the user and the message is send back to the user's Smart phone. This cycle continues until user terminate the application at his/her Smart phone.

Based on the applicability of the Healthcare solution, associate application can perform stream or batch data processing. Resource
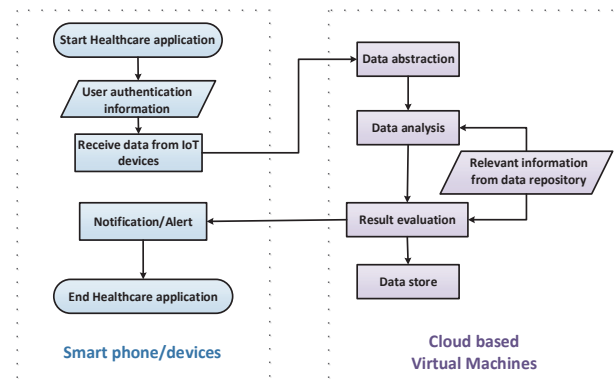

Figure 2: Cloud-based Healthcare application model

requirements of the applications can also vary time to time with the nature of incoming data load. Besides, a application can be run on a single VM or can be run in distributed manner on multiple VMs. However, most of the Cloud-based Healthcare applications perform serialized operation on the data. Parallel processing can be initiated when the Healthcare solution is comprised of multiple applications and deals with diverse Healthcare data.

3.2 Interoperable Fog-Based Solutions

Fog computing environment is comprised of specialized networking devices named Fog nodes to perform diverse computational tasks at the network edge (Fig. 3). Fog nodes are distributively arranged in hierarchical Fog levels. A Fog node can be equipped with processing cores, memory, storage and network bandwidth. The lower level Fog nodes (Smart phones, cast devices, set top box, car media player, etc.) reside very closer to the IoT devices and usually offer interfaces of the associate applications. Therefore, for a particular Fog-based Healthcare solution, a lower level Fog node can be termed as the *Application gateway node*. Application gateway node can process the sensed Health data or can forward to the upper level Fog nodes named *Computational nodes* for processing. In a Fog node, resources (cores, memory, storage, bandwidth, etc.) can be virtualized and shared in the form of Micro Computing Instances (MCI).

In Fog environment, all nodes are not kept computationally active always. Computational unit of the Fog nodes can be turned off when the data load gets reduced and can be activated according to the demand. Hence, the Fog environment can be made scalable and energy efficient. Besides, on each communication link among the nodes, security features can be applied for data privacy and intrusion protection. Thus, reliable data transfer can be ensured.

However, inherently Fog and Cloud differs from each other in respect of resource capacity, capability and orchestration. Therefore, Cloud-based IoT-Healthcare solutions loose interoperability when they are intended to place in Fog. To facilitate placement of Cloud-based IoT-Healthcare solutions in Fog environment, a cluster-based Fog **system architecture** is discussed in the following paragraphs.
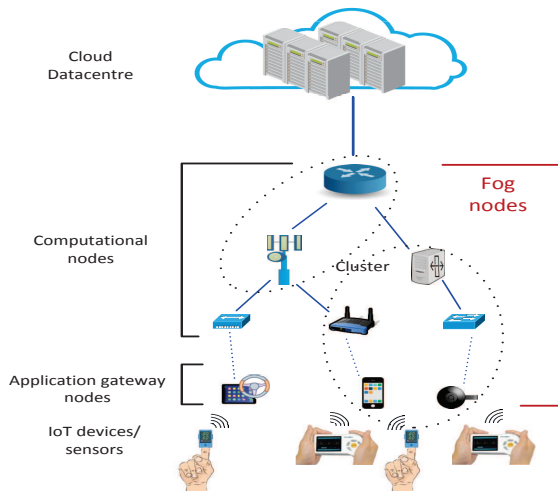

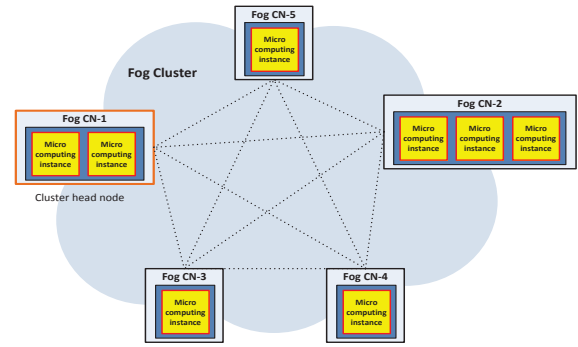**Figure 3: Generalized Fog environment**

Figure 4: Fog-based Healthcare system architecture

Multiple nodes from similar or different Fog levels can form cluster among themselves with faster networking standards (Fig.4). While forming cluster inter-nodal communication latency are given higher priority. In a cluster, some nodes execute the applications while others either host database or maintains communication with the other clusters. Generally each Fog cluster is responsible for a particular Healthcare solution. A single Healthcare solution can also be run in multiple clusters. The isolated nodes those do not belong to any cluster in such architecture only perform as a networking device. The number of computationally active node within a cluster can be scaled up according to the load.

In a cluster, all the secured inter and intra-cluster communication are handled by a particular node named *Cluster head node*. According to the general Fog architecture, each Fog node can receive health data from other connected node. In a cluster, whenever a node receives data, it checks the relevance of the data with the associate Healthcare solution and notifies the Cluster head node. The Cluster head node based on the notification either forwards the data to the corresponding cluster or schedules the data to MCIs of the same cluster for processing according to the application model.

Besides, Cluster head node sets resource and service provisioning policies for the other nodes, balances the load among the nodes, controls and secures access and communication, monitors activities of the MCIs and preserve associate meta-data. In order to ensure consistency of the Healthcare solution during uncertain node failures, Cluster head node can replicate the image of MCIs from that node to other node of the cluster. If a Cluster head node fails, another node from the same cluster which is priorly defined can act as the Cluster head node. Cluster head node can also distribute its responsibilities to the others ensuring no performance degradation.

Moreover, MCIs from same node, cluster or Healthcare solutions can share data and content with each other under the supervision of corresponding Cluster head node. Since MCIs are not rich in resource capacity, large scale health care applications and database are placed in them distributively. Allocated resources to an MCI can be provisioned dynamically based on the context of the Healthcare solution. Each MCI can be managed and configured independently without violating QoS of the others.

The aforementioned cluster-based Fog architecture is resemblanced to the Cloud-based system architecture in some cases. The cluster itself symbolizes the Cloud datacentre where Fog nodes

are deployed like the Servers. The Cluster head node performs as the Resource Manager of the cluster. Inside the Fog nodes, MCIs, similar to VMs, execute the Healthcare applications and handle the database operations. However, some features of such Fog-based Healthcare solution, mentioned in Table 2, enhances its applicability to the real world.

Table 2: Enhanced features of the proposed Fog system

Facts	Fog	Cloud
	Cluster	Datacentre
Confederation	Easy	Hard
Number of Nodes/Servers	High	Few
Inclusion/Exclusion of Nodes/Servers	Flexible	Difficult
Proximity to data source (hop)	One/Two	Multi
Geographical orchestration	Distributed	Centralized
Communication latency from data source	Low	High
Real-time interaction	Possible	Hard
	Nodes	Servers
Tolerance to failure	High	Low
Communication path/link	Variable	Fixed
Energy usage	Less	High
	Cluster head node	Resource Manager
Tolerance to failure	High	Low
Communication path/link	Variable	Fixed
Energy usage	Less	High
	MCIs	VMs
Management/Maintenance	Simple	Complex
Subject to Under/Over provision	Less	Higher
Configuration	Adjustable	Rigid
Price	Low	High

The Cloud-like arrangement of the components and the enhanced features from different perspectives make this cluster-based Fog architecture efficient to run Cloud-based IoT-Healthcare solution observing desired QoS and affordable service cost.

However, in this Fog-based system architecture, nodes are distributed and their underlying MCIs are constrained in capacity. Placement of large-scale Healthcare application on single MCI is not feasible. Besides, on a single node there may not be additional MCIs to accommodate resources for the whole application. Placement of IoT-Healthcare application in such system will not be as straightforward as the Cloud. Therefore, it is required to transform the Cloud-based application model to a Fog compatible one without affecting the generality and the task consistency. The Fog-based **application model** for a Healthcare solution is described below.

In Fog, a single application can be considered as a collection of Application Modules. As mentioned earlier, each Cloud-based Healthcare application performs some common and serialized operations on the received data. Each Application Modules can be designed in such a way so that it can perform atleast one particular operation on the data. Besides, MCIs can be provisioned to execute at most one module within it. Based on the observation, each Cloud-based Healthcare application can be segmented into four Application Modules as shown in Fig.5.

The data-dependency among the modules is drawn with a unidirectional sequential data flow. The inter-module data-dependency delay can affect the application service delivery adversely. Therefore, in defining the service delivery deadline collective inter-module data-dependency delay of the modules should be given higher priority. The detail of modules can be described as follows:

● *Client Module:* Client Module provides the initial interface of the corresponding application. Connected IoT devices send the data signal to the application through this module. Authentication, data receiving frequency calibration, data aggregation from multiple IoT sources are handled by this module. Data pre-prossessing is also done by this module so that scattered data signals from IoT devices transform to the formatted raw data. In addition, based on the combined response from the subsequent modules, the Client Module can manage the activities of the associate actuators.

● *Data Filtering Module:* Raw data forwarded from the Client Module contains some additional data (authentication, application meta-data, etc.) with actual Healthcare data. Data Filtering Module extract the Healthcare data and discard its irrelevant parts so that they can be fed into the subsequent module for processing.

● *Data Processing Module:* The filtered data from Data Filtering Module is processed in this module. This module actually incorporates multiple tasks such as data analysis, comparison and result evaluation. To assist this module external data, techniques and software components can be applied. In this case, necessary communications should be handled by the corresponding MCI, Fog node and cluster.

● *Event Handler Module:* After processing the data in Data Processing Module, the outcome can invoke any event of interest. The Event Handler Module identifies the most appropriate response to that event. The Event Handler Module can preserve the response for further usage or can send back to the Client module to determine the action against the response.

Since working dimension of all the modules are different, their resource requirement varies from one to another. Client Module should be placed closer to the IoT devices for better performance of the application. In Fog, it can be placed on the Application Gateway Node. The subsequent modules can be placed to the particular cluster for that Healthcare solution without violating the data flow. All the modules can be placed on different MCIs of a single node or can be placed on different nodes. However, Data Processing Module require additional resources compared to others module and failure to provide necessary resources for this module can crate a service bottleneck for the solution. The Cluster head node should be made aware of this fact prior to place that module.

In constrained Fog environment, distributed development and deployment is the best way to manage large-scale IoT-Healthcare applications. The proposed application model facilitates modular development of the applications and the associate inter-module data dependency paves the way for its distributed deployment in constrained Fog environment. Thus Cloud-based IoT-Healthcare applications can be customised to place in Fog environment.
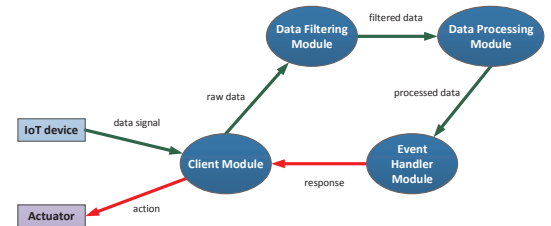
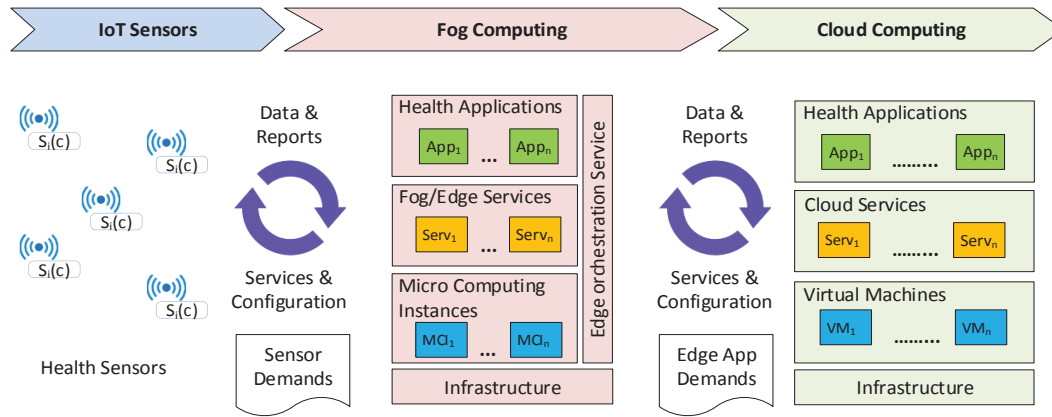**Figure 5: Fog-based Healthcare application model**

Figure 6: A reference architecture of Cloud-Fog integration for interoperable IoT-Healthcare solutions

4 INTEGRATED ARCHITECTURE

Fig. 6 depicts our proposal for a reference architecture that provides the elements to support integration between Fog and Cloud computing infrastructure while supporting interoperable IoT-Healthcare solutions. The goal is provide the basic models to construct end-to-end solutions including sensors, and distribute application and services, like data analysis, machine learning, context inference, and recommendation systems. The key research questions are:

- How to promote the integration of IoT/Sensors and distributed service environments?
- How to support service orchestration of distributed service environments and Fog Computing, considering the requirements for local service support, limitations of computational resources, networking and communication, and the local environment?
- What are the issues of security and privacy in this environment? How to develop strategies for distributed analysis and security measures?

We envision the following challenges and opportunities of Cloud-Fog-based services while integrating them for interoperable Healthcare solutions:

- *Intelligent Health Sensors*: implementing basic, self-configurable Computational Intelligence services at the sensor devices themselves; even considering the potential limitation of computing capability, it would be possible to implement micro-services for contextualization, learning, and self-adjustment of sensor devices, providing solution on the lower-end data collecting and analysis process, i.e. between Sensors and Edge Services.
- *Service Orchestration Cloud-Edge Service Management*: creating services to correlate resource demand and performance information from Cloud Computing and Edge Service structures to coordinate resource allocation, service management, and adaptation to improve service performance and accuracy. The model of *Edge Orchestrations Services* must be able to relate information about Fog Computing infrastructure, e.g. existing computation power, available services, and others and try to accommodate local applications and Services

to distribute the processing between Fog Computing and Cloud Computing demand This model works based on *Edge App Demands* , which provide public manifest describing the resources demands, in terms of computational power, services, and infrastructure, that Cloud Services publish so that the Edge Orchestration Services can evaluate if it can accommodate part of the processing on the Fog Computing.

- *Service Orchestration in Sensor-Edge Service Management*: creating services to correlate resource demand between applications and Sensors and promote adjustment o sensor configurations to cope with application demands. This model works based on *Sensor Demands*, which is a public manifest describing configuration demands for the associated sensors to accommodate the processing requirements on the Fog Computing and Cloud Computing services; e.g config-uration about rate of data sampling, interval between data transmissions, maximum data batch sizes, collect accuracy, and others.
- *Distributed Health Care applications*: orchestration and local distribution of services between Cloud Computing and Fog computing elements to promote intelligent Health Care applications. The data which is critical to the operations of the local infrastructure will be analysed and processed immediately by the edge computing layer. This item will help to address the challenge of turning big data into smart data and stringent patient privacy and security rules.
- *Security and Privacy Solutions*: security must become fluid and adaptive an IoT and Edge Computing environments. This line of research encompasses distributed services to correlate data from multiple layers to infer security issues, intrusion detection, behaviour deviances, privacy threats, and others.This item will help to address the challenge of (3) stringent patient privacy and security rules.

The goal of the Cloud-Fog Orchestration Process is to balance the best distribution of applications and services considering: (i) current requirements of executing applications in terms e.g. of QoS, frequency of data requirement, etc; (ii) computational capacity and service availability on Fog Computing devices, and; (iii) existing sensor and tier possible configurations.

5 PERFORMANCE EVALUATION

In order to demonstrate the feasibility of our proposed Fog-based IoT-Healthare solution and iteroperation with Cloud-based solution, we simulate both the environment and integrated architecutre using iFogSim [8] simulation toolkit. In two folds we conduct the simulation. At first the performance of Fog cluster-based IoT-Healthcare solution is compared to the Cloud-based solution in terms of network delay, energy usage and cost considering computational resources are sufficient in Fog. Later the service distribution in Cloud-Fog integration is demonstrated under different number of sensors and CPU utilization of the services while executing applications considering limited computational resources in Fog. In simulation, synthetic workload is used as the real-world workload to simulate such environment in large scale is not currently available. The simulation metrics are summarized in Table 3.

Table 3: Simulation parameters

Parameter	Value
Simulation Duration	300 sec
Cloud Datacentre:	
Network latency from source	100 ms
Cost of VMs	0.8-0.12 $/min
Energy consumption of VMs	10-15 Mega Joules
Average VMs per Server	10-15
Fog cluster:	
Network latency from source	10 ms
Average Intra-cluster network latency	5-10 ms
Cost of MCIs	0.01-0.03 $/min
Energy consumption of MCIs	2-3 Mega Joules
Average MCIs per Server	3-10
Applications service delivery deadline	250 ms - 650 ms
Average data processing time of applications in Fog with a particular service	180-200 ms
Average data processing time of applications in Fog with a particular service in Cloud	100-120 ms
Data sensing interval of the IoT sensors	200-600 ms

In the simulation experiment, Fog resources can host different number of services of various CPU utilization rate to process data coming from distributed sensors trough associate applications. Here we assume, the applications are scheduled to the services based on the frequency distribution (data sensing interval) of the corresponding sensors and when the capacity of Fog exceeds, the applications are forwarded to Cloud-based services for execution. We conduct the experiments by varying number of the applications, number of the sensors and CPU utilization rate of the services.

5.1 Case Scenarios

In remote Cloud-based solution, sharing same communication link by multiple Healthcare applications reduces the bandwidth segment, creates network congestion and higher data round-trip time. As a result, average network delay perceived by the applications becomes high in Cloud (Fig.7). Conversely, in Fog-based solution, average network delay for data availability to the applications is
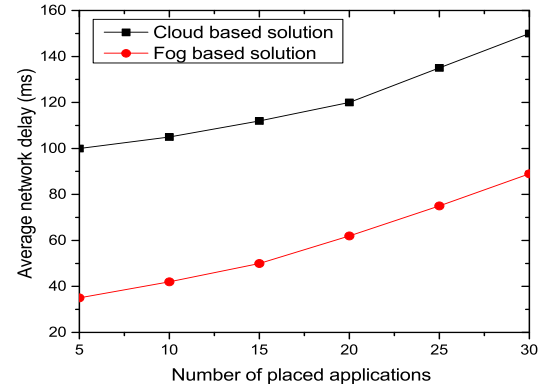
Figure 7: Network delay in Fog and Cloud-based solution

low as there exist multiple communication link between data source and proximate computing components. Moreover, the Cluster head node can control the data flow to reduce the network delay.

In Cloud-based Healthcare solution, usually a single VM executes an application whereas in Fog-based solution, multiple MCIs collectively execute an application. Compared to a VM, an MCI is lightweight and consume less amount of energy. Therefore, the overall energy usage of MCIs while executing increasing number of Healthcare application is less than the VMs (Fig.8).
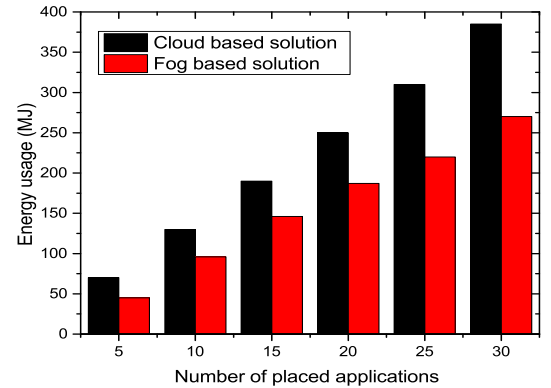
Figure 8: Energy usage in Fog and Cloud-based solution

In addition, single Application Module in Fog requires less resources than the whole application. If an MCI is provisioned according to the requirements of a module, resource over provisioning is less likely to be happen. In Cloud-based solution, it is difficult to provision VMs in such way as the configuration of the VMs are predefined. Therefore, service charge for MCIs can be adjustable according to the context of the module whereas for VMs, whatever the usage is, service charge required to pay for the whole. As a result, in Fog-based solution, total instances cost is less compared to the Cloud-based solution (Fig.9).

However, in Cloud-Fog integration for interoperable Healthcare solutions, it is very important to determine the load distribution of the services between Fog and Cloud. In this phase of performance
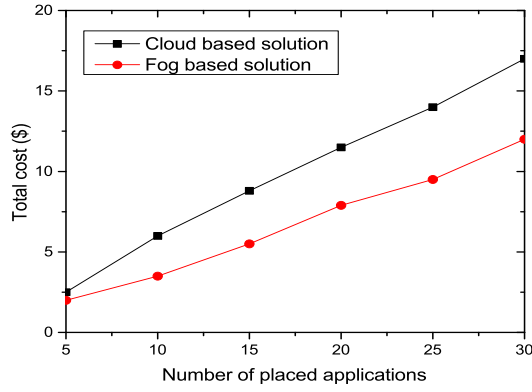
Figure 9: Instances cost in Fog and Cloud-based solution

evaluation, the integration of Cloud-Fog in service distribution is discussed.

Fig.10 depicts the Cloud-Fog service distribution on increasing number of sensors. For lower number of sensors, associate applications can be handled by the Fog-based services. With the increasing of sensors, the number of services in Fog also increases and until a particular point, it is not required to send the applications to Cloud. However Fog resources are not abundant. After reaching a maximum number of running services with specific CPU utilization rate, for Fog resources it is not possible to accommodate more services and applications are required to send to Cloud for services. In this case, number of Fog running services become constant whereas the number of Cloud services begin to increase.
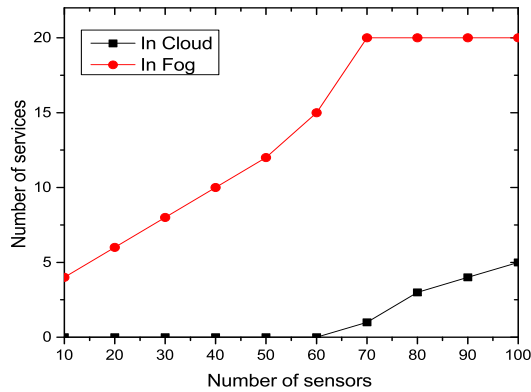

Figure 10: Integration of Cloud-Fog varying number of sensors

Fig. 11, shows number of available services in Fog computing platform and the Cloud-Fog integrated service distribution by varying CPU utilization rate of the services on a particular number of sensors (three scenarios of sensor number in this case; 50, 100, 200). With low CPU utilization rate of services, Fog itself can handle majority of the applications for lower number of sensors. However, as the service CPU utilization rate and number of sensors increase, with all the services available in Fog, the application demand can not be satisfied. In this case association of Cloud becomes necessary.
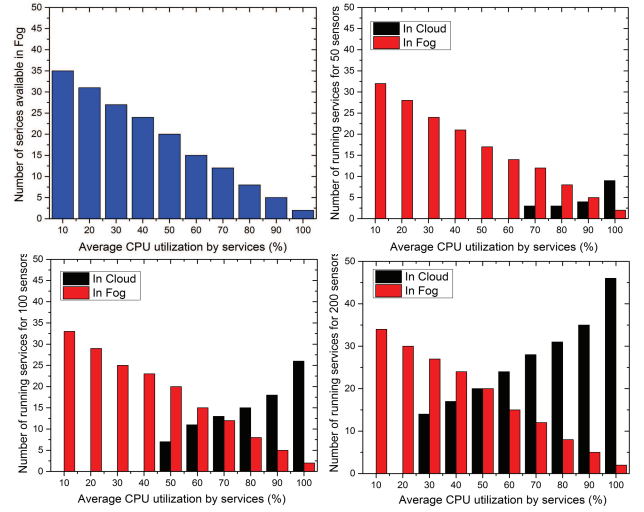

Figure 11: Integration of Cloud-Fog varying number of service CPU utilization

For Cloud, the number of running services also increase with the CPU utilization rate of the services and number of sensors.

6 CONCLUSIONS AND FUTURE DIRECTIONS

In past several years the Cloud computing and its association to many aspects of education, industry and medical services has been studied extensively. Many potential and widely accepted Cloud-based solutions are currently available. With the inclusion of modern techniques like the Internet of Things (IoT), these Cloud-based solutions become more dynamic and user oriented. However, Cloud itself has some limitation due to its geographically centralized architecture and multi-hop distance from the IoT data source. Real-time interaction between user and computing platform often get disrupted by these inconvenience of the Cloud. For IoT-enabled Healthcare solutions sometimes failure of real-time interaction can provoke life threatening incident. Therefore, a new computing paradigm named Fog is coined at the edge network. It helps to meet the limitations of Cloud computing. However, due to differences between these two computing platforms, available Cloud-based solution can not be directly placed to Fog environment.

In this work, we analyzed the literature review and gets the motivation to generalize the Cloud-based IoT-Healthcare solution structure both in terms of system architecture and application model. Later, we propose an interoperable Fog-based IoT-Healthcare solution that extends the general Cloud-based IoT-Healthcare solution structure with some enhanced features. The integration of both the interoperable solution structure is discussed through a reference architecture. However, we analysis the performance of both solution structure and their integration through simulation studies in iFogsim. The performance of Fog-based solution is improved in terms of service distribution, instances cost, energy usage and network delay.

The proposed Fog-based IoT-Healthcare solution (system architecture, application model) can be extended for further research.

Some potential future research scopes in this direction are listed below:

- *Intelligence at the Cluster:* Artificial intelligence can be applied to the Fog cluster to predict the future data load, chances of nodal failure, network topology and associate data flow.
- *Placement of the Application Modules:* Different policies to place the Application Modules within the cluster can be explored. Latency, QoE and QoS-aware module placement can enhance the acceptability of Fog in practical world.
- *Module sharing and re-usability:* Applications belonging to the same Healthcare solution can share executing modules among themselves. As a result computational load can be optimized. Besides, deployed modules of recently terminated application can be re-used for other application. To perform such operations, necessary techniques and policies are required to be developed.
- *Cluster resource management:* In order to meet increasing service demand, Fog cluster is required to be scaled up. Efficient approaches for managing resource can be investigated those can meet the service demand without scaling up the cluster. Such resource management approaches can reduce the energy usage within the cluster and cost of deploying additional resources.
- *Pricing and billing:* A framework for pricing and billing of Fog cluster resources can be pursued. Incentive and reward based resource sharing among multiple Fog cluster can also be explored.
- *Mobility and Edge-centric affinity:* The mobility of the user and edge-centric affinity of the applications should be handled together by the Fog cluster for better performance.
- *System prototype:* We plan to develop a prototype of IoT-Healthcare solution for Sleep Apnea analysis comprising the interoperable and integrated Cloud-Fog architecture.

ACKNOWLEDGEMENT

REFERENCES

[1] Ahmad, Mahmood and Amin, Muhammad Bilal and Hussain, Shujaat and Kang, Byeong Ho and Cheong, Taechoong and Lee, Sungyoung. 2016. Health Fog: a novel framework for health and wellness applications. *The Journal of Supercomputing* 72, 10 (01 Oct 2016), 3677–3695.

[2] Amir M. Rahmani and Tuan Nguyen Gia and Behailu Negash and Arman Anzanpour and Iman Azimi and Mingzhe Jiang and Pasi Liljeberg. 2017. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems* (2017).

[3] Bonomi, Flavio and Milito, Rodolfo and Zhu, Jiang and Addepalli, Sateesh. 2012. Fog Computing and Its Role in the Internet of Things. In *In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (MCC '12)*. ACM, 13–16.

[4] C. Doukas and I. Maglogiannis. 2012. Bringing IoT and Cloud Computing towards Pervasive Healthcare. In *In Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 922–926.

[5] Dubey, Harishchandra and Yang, Jing and Constant, Nick and Amiri, Amir Mohammad and Yang, Qing and Makodiya, Kunal. 2015. Fog Data: Enhancing Telehealth Big Data Through Fog Computing. In *In Proceedings of the ASE Big-Data & SocialInformatics 2015 (ASE BD&SI '15)*. ACM, New York, NY, USA, Article 14, 6 pages.

[6] F. Fernandez and G. C. Pallis. 2014. Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective. In *In Proceedings of the*

4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH). 263–266.

[7] G. Muhammad and S. M. M. Rahman and A. Alelaiwi and A. Alamri. 2017. Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring. *IEEE Communications Magazine* 55, 1 (January 2017), 69–73.

[8] Gupta, Harshit and Vahid Dastjerdi, Amir and Ghosh, Soumya K. and Buyya, Rajkumar. [n. d.]. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Software: Practice and Experience, 2017* ([n. d.]).

[9] Gupta, P. K. and Maharaj, B. T. and Malekian, Reza. 2017. A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres. *Multimedia Tools and Applications* 76, 18 (01 Sep 2017), 18489–18512.

[10] M. Shamim Hossain and Ghulam Muhammad. 2016. Cloud-assisted Industrial Internet of Things (IIoT) âĂŞ Enabled framework for health monitoring. *Computer Networks* 101, Supplement C (2016), 192 – 202. Industrial Technologies and Applications for the Internet of Things.

[11] Jindal, Vasu. 2016. Integrating Mobile and Cloud for PPG Signal Selection to Monitor Heart Rate During Intensive Physical Exercise. In *In Proceedings of International Conference on Mobile Software Engineering and Systems (MOBILESoft '16)*. ACM, New York, NY, USA, 36–37.

[12] M. Chen and Y. Qian and J. Chen and K. Hwang and S. Mao and L. Hu. 2017. Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing. *IEEE Transactions on Cloud Computing* PP, 99 (2017), 1–1.

[13] M. Fazio and A. Celesti and F. G. MÃąrquez and A. Glikson and M. Villari. 2015. Exploiting the FIWARE cloud platform to develop a remote patient monitoring system. In *In Proceedings of the IEEE Symposium on Computers and Communication (ISCC)*. 264–270. https://doi.org/10.1109/ISCC.2015.7405526

[14] M. Hassanalieragh and A. Page and T. Soyata and G. Sharma and M. Aktas and G. Mateos and B. Kantarci and S. Andreescu. 2015. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. In *In Proceedings of the IEEE International Conference on Services Computing*. 285–292. https://doi.org/10.1109/SCC.2015.47

[15] Mahmud, Redowan and Ramamohanarao, Kotagiri and Buyya, Rajkumar. 2017. Fog Computing: A Taxonomy, Survey and Future Directions. In *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, Di Martino Beniamino, Yang Laurence, Kuan-Ching Li, and Esposito Antonio (Eds.). Springer.

[16] Negash, Behailu and Gia, Tuan Nguyen and Anzanpour, Arman and Azimi, Iman and Jiang, Mingzhe and Westerlund, Tomi and Rahmani, Amir M. and Liljeberg, Pasi and Tenhunen, Hannu. 2018. *Leveraging Fog Computing for Healthcare IoT*. Springer International Publishing, Cham, 145–169.

[17] S. Chakraborty and S. Bhowmick and P. Talaga and D. P. Agrawal. 2016. Fog Networks in Healthcare Application. In *In Proceedings of 13th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. 386–387.

[18] S. M. R. Islam and D. Kwak and M. H. Kabir and M. Hossain and K. S. Kwak. 2015. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* 3 (2015), 678–708.

[19] Shahid Mahmud and Rahat Iqbal and Faiyaz Doctor. 2016. Cloud enabled data analytics and visualization framework for health-shocks prediction. *Future Generation Computer Systems* 65, Supplement C (2016), 169 – 181. Special Issue on Big Data in the Cloud.

[20] Sri Vijay Bharat Peddi and Pallavi Kuhad and Abdulsalam Yassine and Parisa Pouladzadeh and Shervin Shirmohammadi and Ali Asghar Nazari Shirehjini. 2017. An intelligent cloud-based data processing broker for mobile e-health multimedia applications. *Future Generation Computer Systems* 66, Supplement C (2017), 71 – 86.

[21] T. N. Gia and M. Jiang and A. M. Rahmani and T. Westerlund and P. Liljeberg and H. Tenhunen. [n. d.]. In *In Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*.

[22] T. Nguyen Gia and M. Jiang and V. K. Sarker and A. M. Rahmani and T. Westerlund and P. Liljeberg and H. Tenhunen. 2017. Low-cost fog-assisted health-care IoT system with energy-efficient sensor nodes. In *In Proceedings of 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*. 1765–1770.

[23] Tsiachri Renta, Pelagia and Sotiriadis, Stelios and Petrakis, Euripides G.M. 2017. Healthcare Sensor Data Management on the Cloud. In *In Proceedings of the 2017 Workshop on Adaptive Resource Management and Scheduling for Cloud Computing (ARMS-CC '17)*. ACM, New York, NY, USA, 25–30.

[24] Y. Zhang and M. Qiu and C. W. Tsai and M. M. Hassan and A. Alamri. 2017. Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. *IEEE Systems Journal* 11, 1 (March 2017), 88–95.