Empowering healthcare IoT systems with hierarchical fog-based computing architecture

Wafaa M. Shosha, Reham R. Mostafa, Ahmed Abo Elfetoh

Abstract—IoT-based healthcare systems are changing the way is healthcare delivered, improving the availability, quality, accessibility, and cost-effec-tiveness of healthcare. The vast amount of data generated by these systems, have to be collected, analyzed, stored, and appropriately shared. IoT devices cannot process this huge data volume. Moreover, sending data to cloud is not generally applicable. Therefore, to overcome the limitations of IoT devices and cloud, fog computing was introduced. The advantage of fog computing is bringing the required resources such as storage and computing to the network edge near the source of data to reduce loading on the cloud data center and decrease latency response to the end-user. In this article, a novel healthcare framework based on fog to accelerate response time and reduce resource waste is proposed. Firstly, a detailed survey on emerging healthcare technologies focusing on IoT, cloud computing, and fog-based applications is conducted. Secondly, the fog-based healthcare framework is introduced and use cases scenarios are presented to illustrate the benefits that the framework offers. Finally, an overview of current security and privacy issues for fog computing is provided.

Index Terms—Internet of things (IoT), cloud computing, fog computing, healthcare, security, privacy, patient information system

1 Introduction

Internet of things (IoT), an evolutionary technology that allow smart devices named "Things" to be associated/connected with each other to form a network. This enables various applications to emerge due to the data sensed, gathered and reciprocated between devices, likewise with the environment, with or without human involvement [1]. IoT has become prominent in the healthcare sector due to the emergence of many smart medical devices and sensors that are connected through the Internet. It is making significant improvements in the healthcare industry by changing how healthcare is conveyed, making healthcare available, affordable, and accessible to users anywhere at any time [2].

The IoT evolution generates huge quantities of data that demands massive computing and storage resources. According to Cisco predictions, by 2020 the number of various devices that will connect to the Internet will reach 50 billion [3] and by 2025 will reach 500 billion [4]. Moreover, the data produced by this large number of devices will reach 507.5 Zettabyte by 2019. Concerning healthcare data, nearly 500 petabytes were produced by IoT-based healthcare systems in 2012, while it is expected to reach 25,000 petabytes in 2020 [5]. The real challenge lies in managing this massive amount of data. That is, collecting, analyzing, storing and sharing it.

Due to the limited storage and computational capability of the IoT devices that are employed to monitor patients' healthcare status, they are not capable of handling this massive amount of data generated.

Therefore, cloud computing has been widely accredited to address the challenges mentioned above posed by IoT [6] because it supports IoT environment with centralized data storage and management, scalable resource allocation, powerful computational capabilities, and rapid deployment of the application at the lowest cost [7].

Cloud computing cannot be considered a panacea solution to address all the problems in the IoT, despite the numerous advantages of integrating IoT in the cloud. For instance, in the delay-sensitive applications, such as healthcare, in which real-time response is critical, cloud computing cannot meet its requisites and can seriously affect the Quality of Service (QoS) [8]. Sending and receiving unstructured data to/from the cloud to end users cause tremendous stress in the cloud and the network. Besides, due to the distance of cloud from the edge network, it requires significant bandwidth and a considerable amount of time in transferring data that leads to intolerable delays for providing services [9].

As a consequence, there is a significant need for a new technology that expands the cloud computing facilities at the proximity of IoT devices. Therefore, Cisco [10] proposed a distributed computing infrastructure termed as fog computing layer that provides control, computational, and storage resources closer to the IoT devices. Fog computing isn't a substitution of cloud, yet it supplements it. The fog has to be considered as a light-weight cloud like facility that is placed at the network edge [11]. It provides local data analysis and transit data storage for sensitive data generated by IoT devices. Therefore, many benefits can be provided by an application based on fog computing that positively affects the QoS such as availability, less bandwidth usage, less network congestion,

- *Wafaa M. Shosha is currently pursuing masters degree in in faculty of computers and information science in Mansoura University, Egypt. E-mail: eng.wafaa.shosha@gmail.com*
- *Reham R. Mostafa is currently an assistant professor in faculty of computers and information science in Mansoura University, Mansoura 35516, Egypt. E-mail: reham_2006@mans.edu.eg*
- *Ahmed Abo Elfetoh is currently a professor in faculty of computers and information science in Mansoura University, Egypt. E-mail: elfetouh@gmail.com*

scalability, and improved response time as well as better user experience.

Nowadays, there are growing numbers of publications that utilize fog computing in healthcare systems. However, there is little research regarding the placement of computation tasks as well as the balancing various requirements. In this paper, a cutting-edge framework for IoT using decentralized fog computing paradigm is proposed to provide healthcare service with less bandwidth, real-time analytics, greater mobility, heterogeneity, low latency and maintaining the QoS appropriately.

On the other hand, new security and privacy challenges have emerged due to the unique characteristics of fog computing besides those inherited from cloud computing. Unfortunately, the security and privacy measures for cloud computing can't be employed in fog computing because of its unique features such as large-scale geo-distribution, heterogeneity, and mobility. In this paper, most of these issues and corresponding solutions are discussed briefly.

The remainder of the paper is organized as: Section 2 presents the incentive through analyzing a number of the critical IoT, Cloud, and Fog articles around healthcare system while Section 3 proposes Fog-based healthcare layered system with the complete explanation. Section 4 discusses the challenges of security and privacy in the Fog computing paradigm. Finally, the paper concludes with Section 5.

2 Literature Review

This section briefly describes the state of the art and highlights the requirement to integrate different technologies to offer value-added healthcare services to end-users. Thus, the relevant work is split into three subsections: a) Healthcare systems based on IoT b) cloud-based healthcare system c) Fog-based healthcare System.

2.1 IoT-based Healthcare System

New technologies have been introduced in the healthcare sector such as IoT and smart devices. They have prompted better approaches for conveying healthcare and in this manner improving human health and luxury. Healthcare systems empowered with the IoT vision have provided various features, such as the availability and accessibility, the capacity to make the system more compatible with the individual requirements and high-quality cost-effective healthcare [12]. Accordingly, healthcare sector views IoT as a promising and effective solution because the patient is at the heart of the treatment procedure. Thus, enabling the patients to self-manage their illness. It also allows healthcare specialists to remotely monitor and support the patient by quickly and safely accessing the patient's data as and when they require through connected networked-monitoring devices. [13].

IoT has a multi-layer architecture, as shown in Fig. 1, which can be partitioned into four particular layers [14]. The first layer, from the bottom-up view, is the sensing layer which collects data from the physical world through different types of sensors and IoT devices. The second layer is the network layer which gathers the sensed data from the sensing layer, and transferring it over wired or wireless networks to the service layer for further processing. The third layer is the service layer where the developing of all the services that tend to satisfy the user needs takes place. The interface layer is the top layer that maintains a smooth and interactive middleware between the service layer and the end user or other applications.

Concerning healthcare services, the IoT architecture referred to above is entirely appropriate as follows: In the first layer, patient health-related data is gathered via sensors (e.g., body-worn or implanted sensors) with where the data will be the collected and used in diagnosis and monitoring of the patient's condition. Then all the data is moved through the network layer to the service layer where all the healthcare services are implemented. The outcome of this data processing and analysis stage is introduced to the user (patient or doctors) easily and attractively through the interface layer, where the doctor can use these data for diagnosis. Later, the patient can have a complete description about his medical condition with no effort. This section summarizes some of the proposed solutions regarding IoT-based healthcare system.

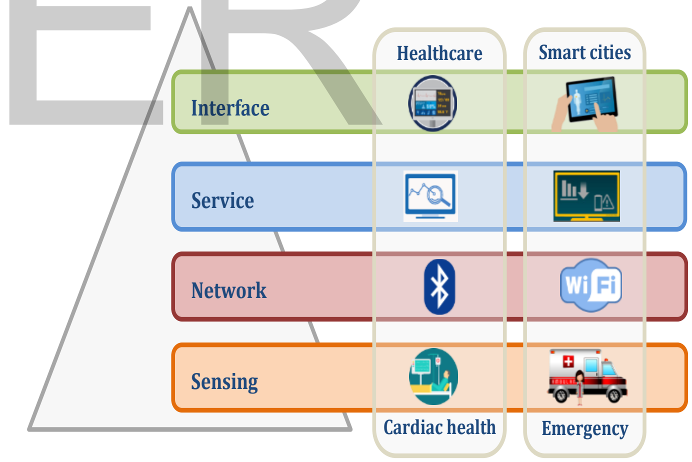

Fig. 1. IoT architecture with its application in healthcare

A wireless sensor-based system was proposed by Suh et al. [15] for chronic heart failure (CHF) patients. The system is based on a three-layer architecture consisting of sensors that measure patient health measurements; web servers which receives data from the first layer, maintaining data integrity, sending alert messages to healthcare providers by means of a text message or email; and databases which performs backup and recovery tasks by applying offline backups. Results revealed that the system recorded a high rate of admissibility and feasibility in aiding CHF patients.

The evolution of IoT technologies has led to increased opportunities in the healthcare domain. RFID technology, the main component of the IoT, use an RFID tag for allowing an automatic tracking and monitoring of any object (such as sensors, patients or devices). This technology is capable of identifying an object that supports location awareness and geographic distribution. Amendola et al. [16] proposed a Night-Care system based on the RFID tags to monitor a person's situation for the duration of the night. This Ambient Intelligence platform incorporated RFID sensors in the user's clothes, furniture or incorporated with other RFID sensors) for gauging the sleep parameters in order to classify the human activity and to recognize abnormal events (e.g., the user presence in bed) that need prompt help.

In spite of the great recognition of RFID technology and the significant advancement it has made in healthcare services and its applications, there are restricted endeavors to accomplish remote healthcare monitoring services since it requires incorporation the Wireless Sensor Networks (WSNs) and RFID technology. The primary purpose of this integration is to face the interoperability challenges between the myriad of heterogeneous devices and the various networking protocols. Moreover, Yang et al. [17] proposed an intelligent platform called iHome system for monitoring elderly people at home consisting of three basic blocks, including iMedBox, iMedPack, and Bio-Patch. Monitoring and reminding services are under the responsibility of iMedPack and Bio-Patch, while iMedBox is utilized as a gateway that gives robust interoperability and incorporation between heterogeneous IoT devices.

Recently, Adame et al. [18] exhibited a hybrid healthcare monitoring system in which RFID and WSN technologies were integrated to provide the location, status, and tracking of patients and assets to improve healthcare services. Real-time tracking was utilized to obtain the patient's location accurately. Moreover, remote monitoring service based on an electronic wristband was provided to reports data and activates alarms from temperature pulse, and movement of the patient. The system was tested in a real hospital environment, and the qualitative and quantitative feedback and evaluation were recorded.

In smart cities, smart health plays a vital role connecting e-health and e-government to provide real-time health monitoring services to patients. Therefore, Rani et al. [19] developed a smart-health system based on IoT to restrain the Chikungunya virus through early diagnosis and preventive measures. This system utilizes the wearable sensors to track the user's vital signs and activities. This data is gathered at the network edge these data are gathered and processed to reduce latency time, and then in an emergency case, an alarm message is sent to specialists.

In recent days, there is an increasing number of aging populations suffering from chronic diseases (e.g., cholesterol, diabetes, hypertension, heart disease, etc.) that require monitoring the health status for early diagnosis of the diseases, especially in developed and developing countries. Accordingly, a smartphone-based wireless body sensor network (WBSN) was proposed by Leu [20] that called Mobile Physiological Sensor System (MoPSS), in which the physiological data of patient was gathered using body sensors embedded in a smart shirt. A smart device was used to process these real-time collected data, and then an alert notification is sent to local caregivers to look after the patients. Then the data are transferred to a remote healthcare cloud via WiFi for monitoring. In order to reduce the response latency, power consumption, and packet loss rate, this system is based on the use of the medium access protocol (MAC) protocol.

The articles reviewed above improve healthcare services using IoT technology are summarized in Table 1. The growing number of medical sensors/devices employed in IoT-based healthcare system has created massive amounts of data that IoT devices can't handle due to its limited storage and computation capabilities [5]. Cloud computing is an approach that addresses the aforementioned problems posed by IoT.

2.2 Cloud-based healthcare system

Cloud-based Healthcare systems mostly have a common architecture model. The system architecture of a cloud-based Healthcare system (Fig. 2) is usually composed of the following components.

- IoT based wearables: wearable devices such as handheld of devices connected to the body (e.g., pulse oximeter, ECG monitor, smartwatches, etc.) can be connected together through Bluetooth, ZigBee, or infrared to form wireless sensor network (WSN) that called wireless body sensor network (WBSN). Such devices have storage and energy constraint.
- Smartphones: smartphones are very useful as an application interface connecting the sensors to the cloud data center to forward sensed data to cloud data centers.
- Cloud datacenter: the central platform for IoT-based-healthcare solutions is cloud datacenter where a broad set of shared resources (storage and computational resources, services, applications, etc.) are available that support IoT based system with reliability and scalability.

Additionally, the application model architecture of the healthcare systems is based on the cloud is similar to the system architecture. The cloud-based Healthcare application flowchart is shown in Fig. 3 consists of two sections: the first is in the users' smartphones while the other is in the cloud. The start of the interaction occurs in the first part of the user's smartphone, by asking for authentication information so that the user can use the system and benefit from different services provided by it. Then the data securely forwarded to cloud for extensive processing. In the Cloud, a repository is used to store all sensed data.

TABLE 1
SUMMARY OF THE MOST RELEVANT PROPOSALS REGARDING IOT-BASED HEALTHCARE SYSTEMS

	References	Year	Description	Methodology	Benefits	Limitations
1	Suh et al. [15]	2011	The IoT based system to facilitates monitoring, and treatment for chronic heart failure patients	Leveraging sensor technologies and wireless communications for remote monitoring of a patient with congestive heart failure.	The feedback system was provided to regulate CHF patients readings	Security implementation is needed Short time monitoring
2	Amendola et al. [16]	2014	An ambient intelligent platform aimed to monitor the state of a patient during the night.	RFID technology	Detecting and reporting abnormal events such as the presence or absence of the user in the bed.	Lack of interoperability between heterogeneous devices and multiple network protocol
3	Yang et al. [17]	2014	An intelligent home based platform to provide remote monitoring for elderly people	Integration between Wireless Sensor Networks (WSNs) and the RFID tags	Interoperability between heterogeneous devices and multiple network protocols	High energy consumption
4	Adame el al. [18]	2016	The system benefits from the integration of WSN and RFID technology to provides remote health monitoring for smart healthcare environment	Optimal integration of different IoT technologies for tracking the location and health of patients	A real-time tracking system	High power consumption Hardware limitation
5	Rani et al. [19]	2018	Scheme for early diagnosis and preventive measures to control the chikungunya virus	Smart health (integration between e-health and e-government)	Real-time feedback system	Security implementation is needed
6	Leo et al. [20]	2018	Real-time healthcare monitoring system to record vital signs of users via integration of smartphone and sensor	Mobile Physiological Sensor System (MoPSS)	Convenient and cost-effective healthcare solution	High energy consumption because of using smartphone continuously to transfer and display the data

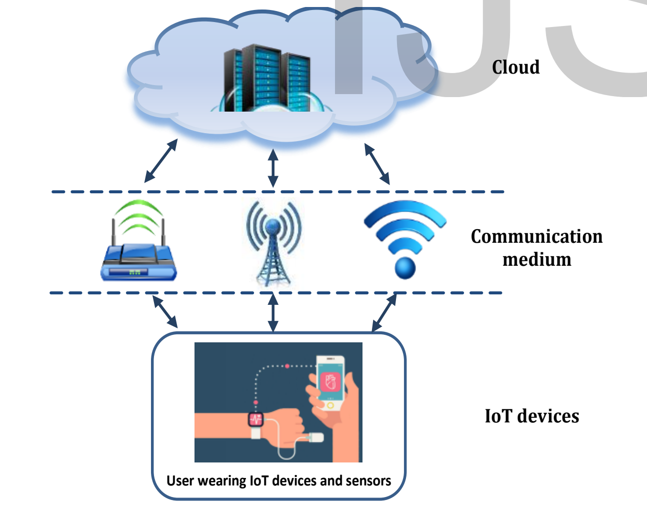

Fig. 2. Cloud-based healthcare system architecture

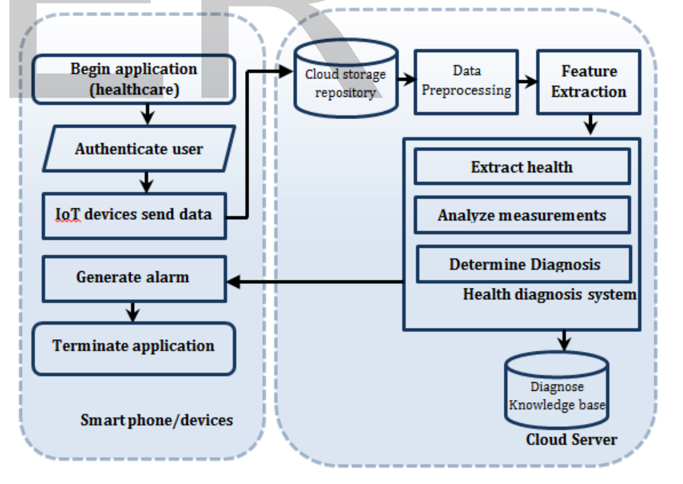

Fig. 3. Cloud-based healthcare system architecture

Later, they are processed through a Knowledge-base with predefined references and guidance to determine a diagnosis. After the data has been analyzed, the health condition of the patient is determined, and the outcome of application can take many forms (ex. user's health context data raw, a doctors' alert, an automatic call to the ambulance in the high-risk conditions, etc.). This cycle is repeated until the user terminates the application on his Smartphone. This section presents some of the proposed literature to the cloud-based healthcare system.

The HealthIIoT framework was proposed by Hossain [21] for monitoring of elderly and disabled people through sensors and smart devices to track electrocardiogram (ECG) and other health vital signs continuously. The evolution of cloud computing paved the path for gathering immense amounts of data by sensors. Such data can be accessed by healthcare units at all times from any location. Later, the gathered patient's data is stored in the cloud and processed to detect any abnormality or error in the received health data. Authors have used the watermarking techniques for the security of data to be communicated.

Mahmud et al. [22] present a context-aware framework to identify various socio-economic, demographic and geographical impacts on public health. It integrates Amazon web services (AWS) with a geographic information system (GIS) to capture, visualize, and store big data. Subsequently, the framework collected contextual data as well as healthcare related data from different remote locations and applying a predictive model based on fuzzy model to generate understandable linguistics to classify health shocks. They utilized real-time data collected from Pakistan's rural and tribal areas to illustrate the novelty of the work.

Jindal et al. [23] proposed an application that is used during intensive motion (e.g., sports) to calculate heart rate of an individual, by applying deep learning on photoplethysmography (PPG) signal collected by smartphones and wearables devices during exercise. The framework fuse PPG signal and accelerometer data, and employ deep belief networks with Restricted Boltzmann Machines (RBM) implemented in the cloud to classify selected PPG signals in real-time and to estimate heart rate. Experiments reveal that the application is able to estimate heart rate accurately.

Another cloud-based architecture was proposed by Sandhu et al. [24] with the aim to predict the H1N1 infected patients and put prevention measures to control the infection rate and to stop the outbreak of H1N1. The framework comprises three processing components: 1) the random decision tree is used to assess H1N1 virus-infected patients based on their respective symptoms. Therefore, based on this initial assessment several control measures are proposed and patients are monitored using a personalized monitoring system. 2) Outbreak Role Index (ORI) determined the probability of a user receiving or spreading the infection. 3) Social Network Analysis (SNA) is used to present the infected user graph and alert healthy users about regional exposure. The system used Amazon computing resources, and the results showed the system's ability to provide a high degree of accuracy in classification.

Sareen et al. [25] introduced a healthcare system based on cloud to contain the spread of Zika virus. The system was based on the use of 1) Naive Bayesian Network (NBN) to classify patients into infected or uninfected according to their symptoms, and 2) Google Maps to point out the risk areas to prevent out-breaks. The government and the healthcare sector receive information on risky sites to take appropriate actions to prevent the spread of the virus. Experimental results reveal high accuracy in the diagnosis of Zika virus and low error rates regarding the identification of high-risk location.

Muhammad et al. [26] proposed a voice pathology detection framework built on the cloud which integrates the IoT with the cloud. This framework applies the local binary pattern on voice signal for feature extraction, and machine learning classifier for diagnosing the pathology. The results show that their detection system improves the accuracy of classification than other existing works.

Verma and Sood [27] presented a cloud-centric health diagnosis framework for predicting the potential disease severity levels. This framework was developed for taking care of student health. Data generated by medical devices and sensors is analyzed on the cloud, and the user result is created containing the user's profile data, potential illness with severity level, and the disease probability of occurrence. The severity of the disease is handled by utilizing the alarm generation mechanism. The framework results perform adequately in terms of prediction accuracy compared to current schemas.

A cloud-based smart home environment (CoSHE) was presented by Pham et al. [28] for real-time remote monitoring of elderly people staying alone at home. CoSHE integrates environmental sensors, wearable sensors, a home service robot, and a cloud-based infrastructure. CoSHE accumulates physiological signals and the associated behavior/location context data. So, the patient's comprehensive information enables healthcare specialists to better understand the patient's health status. The system uses non-invasive sensors in monitoring the entire home though the energy consumption is too high.

All of the solutions mentioned above provide healthcare services are summarized in Table 2. However, these continuous transmission and retrieval processes huge volume of data between IoT devices and cloud raises the cloud-based service complexity. Due to the geographically centralized nature of the cloud, it demands consistent high-speed Internet with high bandwidth and minimal delay that leads to the massive energy consumption. Therefore, a new trend in computing called fog computing was introduced to overcome the cloud computing pitfalls by moving the computing near the source of data to decreases the data volume that must be transferred to cloud data centers.

2.3 Fog-based healthcare system

The fog-based system with three-layer architecture is shown in fig. 4. The layers are the IoT/end-users layer, a fog-layer, and the cloud-layer. IoT/end-users collects data from a myriad of devices. The fog layer contains domains which are controlled by the same or different service providers. Each fog-domain contains one or more fog nodes that can include devices such as network devices, personal computers, smartphones, etc.

IoT system generates massive volumes of data at high speed and requires real-time processing. Therefore, it benefits from fog computing where fog empowers online and real-time data analytics even when connectivity with the cloud is weak or lost. This means less network congestion and faster real-time response; making it ideal for internet healthcare systems. IoT-based healthcare system using fog computing has become more reliable, scalable, and extraordinary accomplished more than ever before. This section presents some of the associated solutions to the fog-based healthcare system.

TABLE 2
Summary of the associated works of cloud-based healthcare system

	References	Year	Description	Methodology	Benefits	Limitations
1	Hossain and Muhammad [21]	2016	Framework for monitoring elder people in the platform of ECG	Industrial IoT- Enabled Framework	The patient's information's are secured by adding watermark to it	No alert generation Short time monitoring
2	Mahmud et al. [22]	2016	A cloud based context aware framework to identify the impact of socio-economic, demographic and geographical conditions on public health	Integrating Amazon web services (AWS), with geographical information systems (GIS) and Fuzzy rule based summarization technique	The framework facilitates the healthcare professional to understand the impact of environmental and cultural norms that caused the health-shocks	no adequate comparisons have been made with any benchmarking experimental studies
3	Jindal et al. [23]	2016	Application that determines the heart rate of an individual during intensive motion	deep learning mechanisms	Technique is able to predict heart rate accurately	Need security High energy consumption
4	Sandhu et al. [24]	2016	Cloud-based healthcare service to keep track the H1N1 virus for early diagnosis	Social Network Analysis	System is able to predicts H1N1 infected patients and provides preventions to control infection rate	Security implementation is needed
5	Sareen et al. [25]	2017	Framework to resist Zika virus by identifying the risky-prone area	IoT- based cloud Framework	High security is provided to user's information	Did not consider the communication with cloud
6	Muhammad et al. [26]	2017	Voice pathology detection system using IoT and cloud frameworks	A local binary pattern for feature extraction and an extreme learning machine for classification	Technique is able to predict voice pathology accurately	Increase latency which degrades the performance
7	Verma and Sood [27]	2018	Framework to predict the feasible disease in the users and generate an alert message	Scale-based, pattern-based, frequency-based methods	Real-time feedback system	Security implementation is needed
8	Pham et al. [28]	2018	Real-time smart home healthcare service for people staying alone Develop a robot assistant to monitor the dehydration level of the user	Cloud-based smart home environment	The system is useful for elder people and disabled people	Energy consumption is too high

A Fog-based service directed architecture was proposed by Dubey et al. [29] with a use case for speech disorders. A smart fog node gathers, analyzes, and filters patients' data prior to sending to the cloud. Thus, helping to reduce power and band-width needs. The proposed system, according to experimental results, dramatically reduced energy consumption and im-proved the overall healthcare system performance.

Monteiro et al. [30] proposed Fog computing interface (FIT) used with Android smart-watches that are paired with a smart tablet to diagnose patients with Parkinson's disease. The watch collects, processes, and analyzes speech data. In the fog layer, they system extracts features such as volume, spectral centroid, and energy from speech. Later, it forwards such features to the cloud for analyses. According to experimental results, the pro-posed system allowed the remote processing of large-volume of audio data in reduced duration.

Ahmad et al. [31] presented a framework known as Healthfog for supporting the healthcare sector, by deploying fog computing at the network edge. Cloud Access Security Broker (CASB) has been introduced as an integral part of Healthfog to implement specific security policies to enhance data privacy and security. The results show that Healthfog decreases the additional communication cost that is typically high in similar systems.

Gia et al. [32] presented a health monitoring system based on cloud that provided cost-effective remote monitoring and automatic reporting for cardiovascular patients. The system contains a low energy consumption sensor and a smart gateway act as a fog node. The sensor gathers vital signals such as the respiration rate, ECG, and temperature. Then, the collected data is transmitted wirelessly to a smart gateway for analysis and real-time alert. Furthermore, the results are available for efficient reuse.

Another fog-assisted healthcare system was proposed by Sood and Mahajan [33] to diagnose and counter the Chikungunya virus. The proposed system adopted wearable sensors to collect user data and decision tree to classify user's infection based on their symptoms. The system benefited from temporal network analysis (TNA) for distinguishing the vulnerable infected location, protecting the uninfected user, and generating a notification to the interested governmental agencies toward making prompt control strides in averting the chikungunya infection.

Verma et al. [34] utilize the concept of fog computing to pro-vide smart homes with a distant health monitoring system. The system was based upon triggering-based data transmission methodology in processing real-time patient's data at fog layer, and analyzing the mined events data by calculating the patient's temporal health index (THI). Experimental results showed a superior performance in real-time decision-making process.

Another work by Gia et al. for supporting diabetic patients with cardiovascular disease was proposed in [35] based on fog computing. The system increased the accuracy of diseases analysis and diagnosis by monitoring room data such as temperature, humidity, and air quality along with patient's data such as body temperature, ECG, blood glucose, and patient's movement. Moreover, the system offered many services by leveraging smart gateway at the network edge such as local data processing, real-time notification, and locally distributed data. Cryptography algorithms were used to secure the system to protect the collected data. Results showed better enhancement in decision making and power consumption.

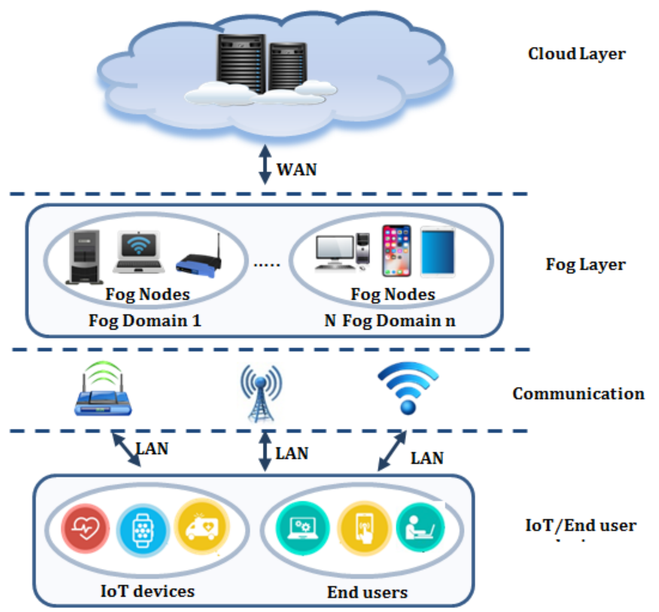

Fig. 4. Fog-based healthcare system architecture

All of the solutions mentioned above to empower healthcare services with fog computing vision are summarized in Table 3. Despite the increasing number of publications that used fog computing in health care systems, little effort has been made to discuss the placement of computing tasks or the differentiation of various requirements.

TABLE 3
Summary of the important articles of fog-based healthcare systems

No.	References	Year	Description	Methodology	Benefits	Limitations
1	Dubey et al. [29]	2015	A service-oriented architecture for telehealth applications	data mining and the data analysis techniques	big data processing with low power Fog resources	Need Security
2	Monteiro et al. [30]	2016	A fog computing interface (FIT) is a smart gateway used for processing the data of clinical speech	Integration of IoT devices, fog, and cloud to process and analyze the clinical speech data of patients with Parkinson and speech disorders	reduce network traffic and latency	High energy consumption
3	Ahmad et al. [31]	2016	Fog-based Healthcare framework	Cloud Access Security Broker and cryptographic primitives	Reduces the communication cost Secured system	High energy consumption
4	Gia et al. [32]	2017	Fog-based health monitoring system that can provide consistent remote monitoring of cardiac patients at low cost.	Integration of IoT devices, fog, and cloud to provides continuous remote ECG monitoring and automatic reporting and analysis	A low-cost health monitoring system	Need security Response time is high
5	Sood, and Mahajan [33]	2017	Framework for the early detection of chikungunya and to generate an alert message to the user about risky locations	Use wearable devices, decision tree, and temporal network analysis (TNA)	Deliver effective healthcare service Reduce energy consumption	Security implementation is needed
6	Verma and Sood [34]	2018	A remote patient health monitoring in smart homes by using the concept of fog computing	Event triggering based data transmission	Improve energy efficiency, performance, communication latency	Security implementation is needed
7	Gia et al. [35]	2019	A smart Fog-based system for continuous, remote monitoring glucose, ECG and other signals in real-time.	Simultaneous monitoring using different types of signals to improve the accuracy of diseases analysis	Efficient regarding energy consumption and QoS.	Need security

3 Proposed Fog-Based Healthcare Framework

Fog computing success relies on the executed fog devices at the network edge which must be able to perform successful pro-cessing at the very early stage. It's mean that fog devices must be capable of dealing successfully with large data generated quickly, filtering, and transferring essential data to the cloud. In this section, the healthcare system/architecture based on multi-layer fog is introduced, which significantly changes the way organizations offer healthcare service.

The proposed system, as shown in fig. 5, compromises mainly of four layers: IoT device layer, the fog aggregate nodes layer, the fog server layer, and the cloud layer. Each layer performs its required function, thus providing adequate services to neighboring layers.

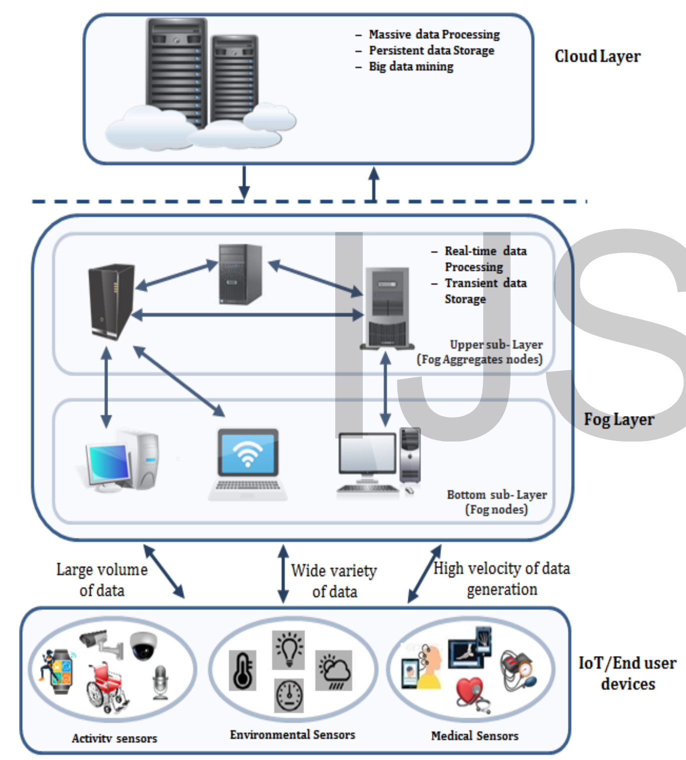

Fig. 5. Proposed Fog-based healthcare system architecture

a) IoT sensor/devices layer

It comprises of various IoT sensors/devices which are in charge of gathering health-related data and other events within or surrounding the user's environment and securely synchronizing this data with the cloud platform. These IoT devices interact with each other and need to provide a connection to a gateway or a fog node using a suitable communication protocol. Generally, IoT devices can be categorized into three main classes [36]: body sensor networks, personal sensor networks, and multimedia devices.

- Body Sensor Networks (BSN): consist of multiple types of biomedical sensors that form a network and are attached to a patient's body for monitoring vital signs and physiological data such as blood pressure, body temperature, ECG and EEG and heart rate. The BSN's topological structure is dynamically or statically constructed according to the different situation.
  - In cases wherever patients are in bed or moving slowly in the indoor areas, mech or tree network structure are proper.
  - In cases where patients stroll in the outdoor area, i.e., in a high mood of mobility, the star network structure is appropriate.
- Personal sensor networks (PSN): set of environment sensors whose goal is to capture and retrieve contextual data concerning the patient and their environment (light, temperature, and humidity).
- Multimedia devices: encompass visual and audio sensing devices (e.g., cameras and microphones) that are used for detecting daily activities of the person, posture recognition, human presence, and fall detection.

According to frequency of their receipt, the data gathered by sensors can be categorized into three types:

- Constant: Data is transferred continuously.
- Interval: Data is sent periodically, after a standard time period.
- Instant: Data is transferred immediately when an event occurs.

IoT devices interact with each other and connect to fog nodes using different communication technologies, like WiFi, ZigBee, and Bluetooth [37].

- WiFi protocol: The most widely used wireless communication protocol (IEEE 802.11) has a transfer rate up to 54 Mbps within 100 meters range. However, its downfall is consuming too much energy.
- ZigBee: an efficient wireless networking protocol (IEEE 802.15.4) used for sensory data because of its low data rate, little power consumption, and low cost.
- Bluetooth technology: an industry standard for short-range RF-based connectivity for mobile personal devices. The (IEEE 802.15.1) range is 10 meters and a maximum data transmission rate of 1 Mbps.

The selection of communication protocol mostly relies on the application and the specific usage state. For example, in transferring a massive number of documents wirelessly, Wi-Fi is ideal. Otherwise, Bluetooth suits short-range, low energy connections.

b) Fog computing layer

Fog computing layer acts as a bridge between IoT devices and cloud computing layer. It is built from multiple geographically distributed smart gateways called fog nodes for perform-ing various computational tasks on the network edge. Fog nodes were equipped with processing pins, storage, and net-work bandwidth. Through geographical distribution and connection between smart gateways, an intermediate layer to accommodate effective healthcare services without latency in response, and without limiting patient mobility is formed.

Fog computing layer consists of two sub-layers:

- The fog lower sub-layer (called fog aggregate nodes layer) comprises of gateways fit for performing little to medium computation. Instances of such gateways are PCs, small workstations, and smartphones that are closer to the IoT devices and generally offers associated applications an interface. The greater part of the computations required by the IoT devices is handled by this layer. Moreover, it can respond quickly because of its proximity to the IoT devices. Real-time data analysis techniques are used to analyze data generated by different IoT devices with higher data rates. To sum up, these gateway nodes can handle the sensed data or redirect it to the upper level fog node.
- The fog upper sub-layer (called fog servers layer): is utilized for dealing with the complete data reported by the lower layer of fog and reinforcing this layer with its higher computational capacities. That means that large-scale computation that can't be processed by the fog lower sub-layer nodes and non-critical are generally discharged to the upper sub-layer of fog. Furthermore, the fog nodes in this layer preserve the security of the healthcare data by securing communication the accumulated data from unauthorized access. Finally, it handles the distribution of the workload on the cloud servers. In a fog environment, a node can be turned off according to the data load or activated upon request. Thus, the fog paradigm is energy efficient because it is scalable. Moreover, it can ensure reliability of data transfer since data privacy protection, and intrusion detection can be applied on each communication link.

c) Cloud layer

The cloud layer is in charge of a definitive and long-term stockpiling, handling substantial scale computations, and managing nodes in other layers. Additionally, it presents a graphical user interface (GUI) to the user for visualization and commentary.

In order to illustrate the benefits that the proposed fog-layered architecture offers, a use case of remote health monitoring system is presented as shown in fig. 6. This system supports patient self-monitoring by providing notification services such as reminders for medication or notification for doing a predefined exercise from the doctor, and physician online/offline monitoring through accessing data obtained from diverse IoT user devices within healthcare infrastructure such as hospital, smart home, and day-care centers.

Patient vital body signs are gathered using various health sensors, and then transmitted to a smart gateway in a fog layer using any wireless communication protocol for real-time processing. This data is mined and analyzed in the fog layer, and the abnormal estimations trigger an alert system that sends notifications or makes an emergency call to the local health caregivers. If there are no abnormal estimations, data is stored locally and transferred to the cloud when network traffic and bandwidth allows. Otherwise, if there aren't any predefined services at that point, it cooperates with the medicinal services cloud supplier to support the patient.

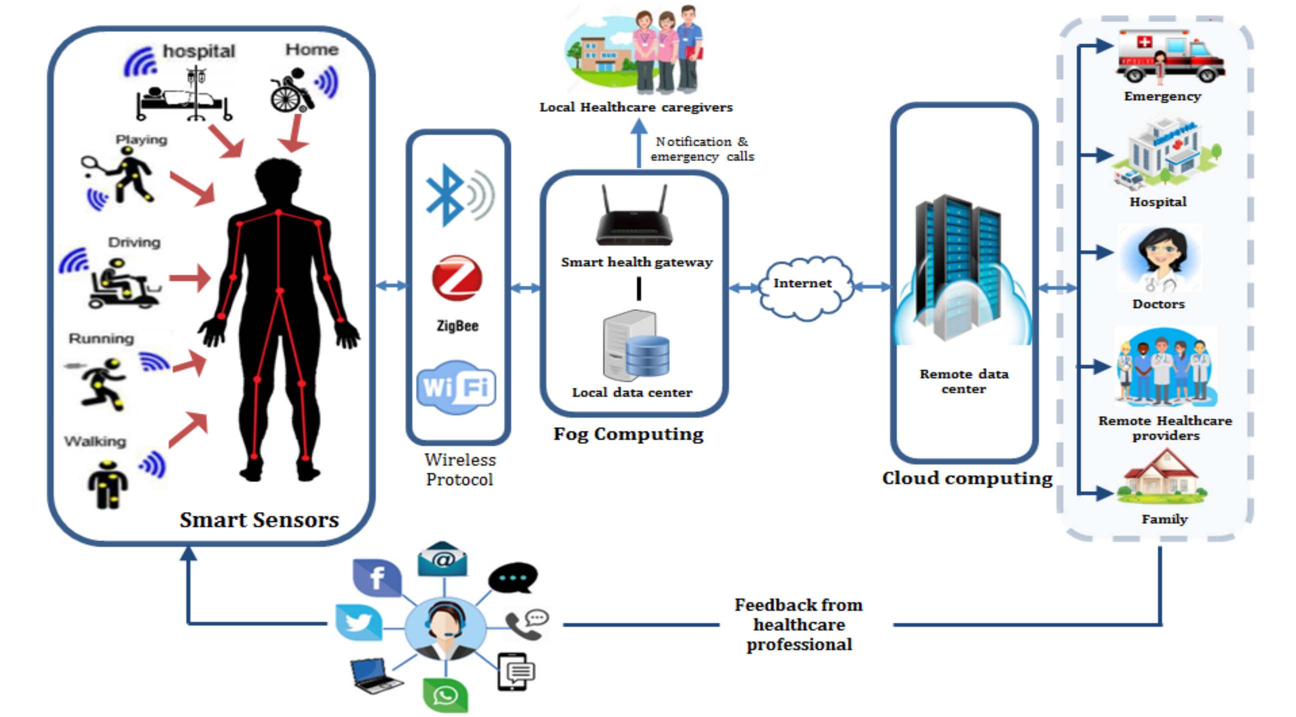

Fig. 6. Use case of remote healthcare monitoring system

In such a case, the data is sent for permanent storage and further processing on the cloud using advanced machine learning algorithms. Thus, providing the patient with forecasts regarding his health status. The physicians can access the cloud, check the therapeutic information, give the patient an advice or a prescription, or talk to the patient.

The main advantage of using such architecture is that the notification system is automated and does not require the physician intervention because the service is provided through the fog layer in real-time.

4 Security and Privacy Issues of Fog Computing

Data sensitivity in health-related system is important. Thus, the security prerequisites are critical due to the potential adverse consequences if the data is tampered with. Accordingly, in order to address privacy and security issues of IoT healthcare systems, security and privacy frameworks are required to achieve the following:

1. Confidentiality: guarantees that a patient's health data is inaccessible by unauthorized users.
2. Integrity: guarantees that the health data is not modified in transit by anyone other than the concerned person, and this, as a result prevents incorrect treatment. Besides, the integrity of the stored data should not be compromised.
3. Availability: ensures the continuity of the IoT healthcare (either local/global cloud) services to authorized users on demand.
4. Authentication: enables an IoT device for verifying the peer's identity with which it is communicating.
5. Authorization: ensures that only authorized entities have the required permits to perform the operation they request to make on network services or resources.

Because fog computing is considered as important expansion of cloud computing at the network edge, certain problems, especially security and privacy issues, will continue to persist. Several service providers, that are used to deploy the fog network, are not fully reliable, and devices are vulnerable. Moreover, fog computing has given rise to many new challenges in privacy and security due to its distinct properties such as scalability, support for mobility, decentralized infrastructure, and heterogeneity which may influence the utilization of fog computing in IoT system. On the other hand, as a result of minimizing the amount of data being sent to the cloud, fog computing is a more secure infrastructure in comparison to the cloud.

In IoT application, fog computing handles the security and privacy issues is as follow:

- *Authentication:* Verifying the authenticity of user's devices subscribed to fog services is a prerequisite for fog network. The authentication process becomes a tremendous challenge in the fog-based system as the IoT devices are restricted in many ways including energy, processing, and storage. Furthermore, the decentralization nature of fog network and the mobility of users present a tremendous impediment to the accomplishment of authentication. Therefore, traditional PKI-based authentication is not efficient. In-stead, in order to minimize authentication load and reduce delay, cooperative authentication methods [38, 39] were proposed that encourage fog nodes to share user's identity verification.
- *Authorization:* After verifying the identity of users and/or IoT devices, they must be given distinctive privileges in order to access different services pro-vided by the system. Therefore, to ensure system security and user privacy, the presence of authorization architecture is fundamental. Traditional access control mechanism such as role-based access control [40] and attribute-based access control [41] is not suitable to be used in fog computing environment due to its decentralized infrastructure. Therefore, the design of a distributed access control mechanism to be applicable to fog computing is a challenging task due to the mobility of users and dynamic device management.
- *Privacy:* Fog computing contributes to privacy-preserving due to the local processing/storage of sensitive data (generated from the end users) at the net-work edge, leading to reduce the transmission of sensitive data to the cloud. Otherwise, privacy leakage could occur due to the increased communication among IoT-fog-cloud layers that form the fog architecture. To preserve data privacy, sensitive data must be encrypted before being moved to the fog node. Many privacy-preserving techniques (e.g., homomorphic encryption [42], differential privacy [43]) have been proposed which can be used to preserve data privacy in fog architecture. Usage privacy and location privacy are also critical challenges in the fog computing environment, that must be considered and achieved.
- *Intrusion detection:* If there is no proper intrusion detection mechanism deployed in the system, malicious (internal or external) attackers can compromise the fog architecture and penetrate any entity at any time. The intrusion detection mechanism is capable of detecting any malicious activity or policy violations on both the IoT device and the fog nodes by observing and analyzing log file, user login information, and access control policies. Therefore, malicious attacks such as port scanning or denial-of-service (DoS) could be identified and mitigated before they are crossed within the system. Due to the heterogeneous and de-centralized nature of fog computing, traditional intrusion detection systems such as Host-based Intrusion Detection Sys-

tems (HIDS) [44], Network-based Intrusion Detection Systems (NIDS) [45]) are not very efficient to be applied. Therefore, designing an intrusion detection system is a challenges task.

- *Integrity:* The user's control over data is given over to fog nodes, at the point when the user's data outsourced to fog nodes. Because fog nodes are close to the network edge, the integrity of data is being put at risk as it continues to experience a wide range of internal and external attacks. For this purpose, Zhu et. al and Yu. et. al. [46, 47] proposed data possession protocols in order to guarantee the integrity of the out-sourced data. However, due to numerous reasons these protocols are not suitable to be applied in fog computing scheme. Firstly, user's data are transitory stored on fog nodes which can process the data in the way they see feasible including the deletion of useless data. Therefore, the fog node behavior is not guaranteed to be credible towards the user data. Secondly, multiple fog nodes may contain user data due to user mobility. Hence, checking data integrity in each node is an inefficient solution. Therefore, secure data possession protocols that are crucial for fog computing environment.
- *Light weight security protocols:* In order to allow IoT devices (limited in storage and computational capability) to offer real-time services, it is imperative to de-ploy lightweight security protocols in securing fog structure. Service response delay relies on the latency of fog nodes because complex computational operations are performed to create user responses. There-fore, computational operations have to be lightweight on both IoT devices and fog nodes. To sum up, fog computing layer should utilize a variety of light-weight security protocols (i.e., data encryption, digital signature, and authentication) [48] to provide reliable services and preserve data privacy.

Regardless of the various advantages of fog computing, there are various challenges to consider. Two of the most significant challenges are security and privacy. The development and application of new security and privacy mechanisms in accordance with the Fog computing and its distinctive features will empower Fog computing vision to demonstrate its maximum capacity in IoT systems

5 Concusions

The emergence of healthcare based on IoT have greatly enhanced the quality of healthcare and drastically reduced expenses. However, these systems generate an unprecedented amount of unstructured health-related data. IoT objects are characterized by constrained storage and computing resources, that cannot deal with this high volume of data. Moreover, transferring data from/to cloud requires substantial time which may cause latency issues. Consequently, fog has been integrated into IoT-based system to bring computing resources at the network edge.

In this paper, the literature review was presented, and the motive for modifying the traditional fog-based healthcare structure was shown. Then, a novel healthcare solution that alters the traditional healthcare system structure which is based on fog-based has been proposed. Efficient utilization of fog computing in the proposed system makes it possible to deal with and overcome current challenges and contributes significantly to decrease latency and costs of healthcare delivery.

6 References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2347–2376, 2015.

[2] J. Gubbia, R. Buyyab, S. Marusica, and M. Palaniswamia, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions,” Futur. Gener. Comp. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[3] D. Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” Cisco White Paper, 2011.

[4] J. Camhi, “Former Cisco CEO John Chambers Predicts 500 Billion Con-nected Devices by 2025,” Business Insider, 2015.

[5] B. Feldman, E.M. Martin, T. Skotnes, “Big Data in Healthcare Hype and Hope,” October 2012. Dr. Bonnie 360, 2012. http://www.west-info.eu/files/big-data-inhealthcare

[6] A. Botta, W. de Donato, V. Persico, and A. Pescapé, “Integration of cloud computing and internet of things: a survey,” Futur. Gener. Com-put. Syst. **56**, 684–700 (2016)

[7] C. Stergiou, KE. Psannis, BG Kim, and B. Gupta, “Secure integration of IoT and cloud computing,” Future Generation Comp. Syst., vol. 78, pp. 964-975, 2018.

[8] V. Stantchev, A. Barnawi, S. Ghulam, J. Schubert and G. Tamm, “Smart items, Fog and cloud computing as enabler of servitization in healthcare,” Sensor and Transducers Journal, vol. 185, no.2, pp. 121-128, 2015.

[9] M. Firdhous, O. Ghazali, S. Hassan, “Fog computing: will it be the future of cloud computing,” in Proceedings of the 3rd International Con-ference on Informatics & Applications, Kuala Terengganu, pp. 8–15, 2014

[10] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, “Fog computing and its role in the internet of things,” in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (ACM, New York), pp. 13-16, 2012

[11] A. Munir, P. Kansakar, and SU. Khan, “IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things,”, IEEE Con-sumer Electronics Magazine, 2017

[12] M. Maksimovic and V. Vujovic, “Internet of Things based e-health sys-tems: ideas, expectations and concerns,” Handbook of Large-Scale Distributed Computing in Smart Healthcare, Scalable Computing and Communications, Springer, 2017.

[13] F. Andriopoulou, T. Dagiuklas and T. Orphanoudakis, “Integrating IoT and Fog Computing for Healthcare Service Delivery,” Components and Services for IoT Platforms, Springer International Publishing Switzerland, 2017

[14] L. Da Xu, W. He, S. Li, “Internet of things in industries: a survey,” IEEE Transactions on Industrial Informatics, vol. 10, pp. 2233–2243, 2014

[15] M. K. Suh, C. A. Chen, J. Woodbridge, M. K. Tu, J. I. Kim, A. Nahapetian, L.V. Evangelista, and M. Sarrafzadeh, “A remote patient monitoring system for congestive heart failure,” Journal of Medical System, vol. 35, no. 5, pp. 1165-1179, 2011.

[16] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, G. Marrocco, “Rfid technology for IoTbased personal healthcare in smart spaces,” IEEE Internet Things Journal, vol. 1, no. 2, pp. 144-152, 2014.

[17] G. Yang, L. Xie, M. Mantysalo, X. Zhou, Z. Pang, L.D. Xu, S. Kao-Wal-ter, Q. Chen, L.-R. Zheng, “A health-IOT platform based on the inte-gration of intelligent packaging, unobtrusive bio-sensor, and intelli-gent medicine box,” IEEE Trans. Ind. Inf., vol. 10, no. 4, pp. 2180-2191, 2014.

[18] T. Adame, A. Bel, A. Carreras, J. Meli-Segu, M. Oliver, R. Pousa, “CUI-DATS: An RFID–WSN hybrid monitoring system for smart healthcare environments, Future Generation Computer Systems, pp. 602–615, 2016.

[19] S. Rani, S. H. Ahmed, and S. C. Shah SC, “Smart health: a novel paradigm to control the chickungunya virus,” IEEE Internet Things Journal, 2018.

[20] F. Leu, C. Ko, I. You, K.-K. R. Choo, and C.-L. Ho, “A smartphone-based wearable sensors for monitoring real-time physiological data,” *Comput. Elect. Eng.*, vol. 65, pp. 376-392, Jan. 2018.

[21] M. S. Hossain, G. Muhammad, “Cloud-assisted Industrial Internet of Things (IIoT)—enabled framework for health monitoring,” Computing Networks, vol. 101, pp. 192–202, 2016.

[22] S. Mahmud, R. Iqbal and F. Doctor, "Cloud enabled data analytics and visualization framework for health-shocks prediction, "Future Gener-ation Computer Systems, pp. 169–181, 2016.

[23] V. Jindal, "Integrating Mobile and Cloud for PPG Signal Selection to Monitor Heart Rate During Intensive Physical Exercise," In Proceedings of International Conference on Mobile Software Engineering and Systems (MOBILESoft ’16), ACM, pp. 36–37, 2016.

[24] R. Sandhu R, H. K. Gill, S. K. Sood, “Smart monitoring and controlling of pandemic influenza A (H1N1) using social network analysis and cloud computing,” Journal of Computer Science, pp. 11–22, 2016.

[25] S. Sareen, S. Sood SK, S. Gupta, “Secure Internet of Things-based cloud framework to control Zika virus outbreak,” International Journal of Technology Assessment in Health Care, vol. 33, no. 1, pp. 8-11, 2017.

[26] G. Muhammad, S. K. M. Rahman, A. Alelaiwi, A. Alamri, "Smart health solution integrating IoT and cloud: A case study of voic pathology monitoring", *IEEE Communication Magazine*, vol. 55, no. 1, pp. 69-73, Jan. 2017.

[27] P. Verma, S. Sood, “Cloud-centric IoT based disease diagnosis healthcare framework,” Journal of Parallel Distributed Computing, vol. 116, pp. 27-38, 2018.

[28] M. Pham, Y. Mengistu, H. Do, W. Sheng, “Delivering home healthcare through a cloud-based smart home environment (CoSHE),” Future Generation Computer System, vol. 81, pp. 129-140, 2018.

[29] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya, “Fog Data: Enhancing Telehealth Big Data through Fog Computing,” In Proceedings of the ACM conference on ASE Big Data and Social Informatics, p.14, ACM, Oct. 2015.

[30] A. Monteiro, H. Dubey, L. Mahler, Q. Yang, K. Mankodiya, "Fit: A fog computing device for speech tele-treatments", *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, pp. 1-3, 2016.

[31] M. Ahmad, M. B. Amin, S. Hussain, B. H. Kang, T. Cheong, and S. Lee, “Health Fog: a novel framework for health and wellness applications,” The Journal of Supercomputing, vol.72, no.10, pp.3677–3695, 2016.

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

[33] S. K. Sood, I. Mahajan, “A fog based healthcare framework for chikungunya,” IEEEE Internet of Things Journal, pp. 1 – 8, 2017.

[34] P. Verma, and S. K. Sood, “Fog assisted-IoT enabled patient health monitoring in smart homes,” IEEE Internet of Things Journal, vol. 5, no.3, pp. 1789-1796, 2018

[35] T. N Gia, I. B. Dhaou, M. Ali, and A. M. Rahmani, “Energy efficient fog-assisted IoT system for monitoring diabetic patients with cardiovascular disease,” Future Generation Computer Systems 2019

[36] H. Mshali, T. Lemlouma, M. Moloney, and D. Magoni, “A survey on health monitoring systems for health smart homes,” International Journal Industrial Ergonomics, vol. 66, pp. 26–56, 2018.

[37] A. Sula, E. Spaho, K. Matsuo, L. Barolli, F. Xhafa, and R. Miho, “A new system for supporting children with autism spectrum disorder based on iot and p2p technology,” International Journal of Space-Based and Situated Computing, vol. **4**, pp. 55–64, 2014.

[38] X. Lin and L. Xu, “Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks,” IEEE Trans. Veh. Technol., vol. 62, no. 7, pp. 3339–3348, 2013.

[39] J. Zhou, X. Lin, X. Dong, and Z. Cao, “PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed Healthcare Cloud Computing System,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 6, pp. 1693–1703, 2015.

[40] S. Salonikias, I. Mavridis, and D. Gritzalis, “Access Control Issues in Utilizing Fog Computing for Transport Infrastructure,” in Proc. of CRITIS, pp.15–26, 2015.

[41] A. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” in Proc. of EUROCRYPT, 2011, pp. 568–588.

[42] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “Eppa: an efficient and privacy-preserving aggregation scheme for secure smart grid commu-nications,” IEEE Transactions on Parallel and Distributed Systems, Vol. 23, 2012

[43] C. Dwork, “Differential privacy,” ICALP 2012, Lecture Notes in Com-puter Science, vol. 4052, Springer, Heidelberg , 2011

[44] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, “Intrusion Detection Techniques in Grid and Cloud Computing Environment,” IEEE IT Professional Mag, vol. 12, no. 4, pp. 38–43, 2010.

[45] H. Hamad and M.A. Hoby, “Managing Intrusion Detection as a Service in Cloud Networks,” Int. J. Comput. Appl., vol. 41, no. 1, pp. 35–40, 2012.

[46] Y. Zhu, H. Hu, G. Ahn, and M. Yu, “Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244, 2011.

[47] Y. Yu, M.H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, “Identity-based Remote Data Integrity Checking with Perfect Data Pri-vacy Preserving for Cloud Storage,” IEEE Trans. Inf. Forensic Secur., vol. 12, no. 4, pp. 767–778, 2017.

[48] M. Katagi, and S. Moriai, “Lightweight Cryptography for the Internet of Things,” Sony Corporation, pp.7–10, 2008.