Personal and Ubiquitous Computing (2024) 28:599–613
https://doi.org/10.1007/s00779-024-01802-y

ORIGINAL PAPER

Fog-assisted healthcare framework for smart hospital environment

Tariq Ahamed Ahanger[1] · **Abdulaziz Aldaej**[2] · **Yousef Alharbi**[3]

Received: 30 January 2023 / Accepted: 20 March 2024 / Published online: 20 April 2024

Abstract

The technological revolution brought by the Internet of Things (IoT) has mostly relied on cloud computing. However, to satisfy the demands of time-sensitive services in the medical industry, fog computing, a novel computational platform based on the cloud computing paradigm, has shown to be a useful tool by extending cloud resources to the network's edge. The current paper examines the role of the fog paradigm in the domain of healthcare decision-making, focusing on its primary advantages in terms of latency, network utilization, and power consumption. A fog-computing-based health assessment framework is developed in the current paper. Moreover, based on effective performance parameters, the performance is evaluated and depicted. The results show that the presented strategy can reduce network congestion of the communication network by analyzing information at the local node. Moreover, increased security on health information can be maintained at local fog node, and enhanced data protection from unauthorized access can be acquired. Fog computing offers greater insights into the health condition of patients with enhanced accuracy, precision, reliability, and stability.

Keywords Fog computing · IoT · Artificial intelligence · Smart healthcare

1 Introduction

In the coming decade, the Internet of Things (IoT) is projected to connect millions of gadgets and intelligent things to enable the enormous potential for gathering and transmitting information smartly [13–15]. In recent years, cloud computing has given resources that have made it possible to utilize the IoT environment for ubiquitous computing, storing, and analysis, as well as to create a simply shared pool of resources [16, 18]. Several cloud-based solutions have been presented by the researchers globally, including cloud-based IoT and Ubiquitous Intelligent decision-making [11, 18]. To accommodate the ever-increasing volume of data, all of these systems incorporate certain advantages from the cloud platform. Furthermore, the transition to IoT cannot be viewed as a straightforward cloud computing deployment. By offering decision-making applications to users through a dense globally dispersed IoT paradigm, the cloud conceptualization must be used [6, 7, 9]. According to cloud-based service delivery, the IoT paradigm must ensure the Everything-as-a-Service (XaaS) model, which enables applications and end-users to acquire useful data from every device in a time-sensitive manner [8, 12]. The fog-based computational platform has recently attracted a lot of attention because of its potential to meet needs that the present cloud computing idea has yet to solve. As IoT solutions demand, the revolutionary platform of fog computing enhances the accessibility of computational resources located at the cloud platform to the edge of the network [17, 19]. Conspicuously, service delivery from millions of linked IoT sensors is ensured along with providing users with data analyzing and storing. Its architecture allows for real-time data analysis in geographically dispersed locations with limited data processing and storage capability. This approach aids in considerably reducing the quantity of data transferred between end-devices at the network's edge

---

✉ Tariq Ahamed Ahanger
t.ahanger@psau.edu.sa

Abdulaziz Aldaej
a.aldaej@psau.edu.sa

Yousef Alharbi
y.alharbi@psau.edu.sa

[1] Department of Management Information Systems, College of Business Administration, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

[2] College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

[3] Department of Biomedical Technology, College of Applied Medical Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia

and the cloud infrastructure's core [10]. However, in IoT settings, delivering large-scale connections and services is a difficult challenge. Different difficulties, including connection, dependability, storage, and delay, may have an impact on the quality assurance (QA) due to its geographical location and heterogeneity.

When a large number of devices join a network, malware attacks, the risk of failures, and vulnerability can result in unauthorized access. Conspicuously, the fog platform is confronted with novel security threats that are beyond inherited from cloud computing. The primary goal of the current research is to compare the fog computing paradigm to the traditional cloud computing model in terms of performance and demonstration in healthcare settings. Figure 1 shows the ideology of IoT-Fog-Cloud computing model. The suggested strategy seeks to alleviate or at the very least mitigate the concerns listed above, notably many security breaches in healthcare systems caused by enormous medical data flow between sensors and the cloud. Furthermore, the need to achieve an optimal delay latency in services that are sensitive to it motivates the use of th computing paradigm. This may be accomplished by moving cloud-hosted resources to the network's edge. Based on the aforementioned aspects, the major contribution of the current paper includes the following:

1. In healthcare settings, a comparative analysis is performed between traditional cloud platform and fog-based service delivery;
2. Fog-based medical assessment framework development and deployment for time-sensitive decision-making;
3. Fog-based data communication framework for real-time service delivery.
4. Evaluation of the suggested framework's performance, which acts as the foundation for the novel medical decision-making.

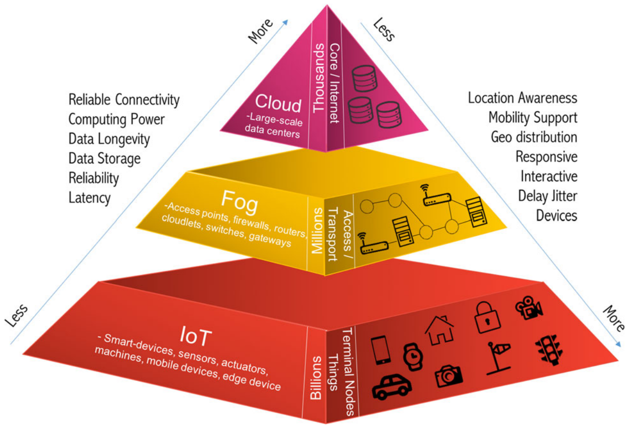


Fig. 1 Fog computing between IoT and cloud platform

Paper organization The remainder of the article is laid out in the following sections. Section 2 delves deeper into state-of-the-art publications on healthcare applications currently accessible in the literature. Section 3 depicts the proposed fog-based system's components, followed by Sect. 4's discussion of the most important benefits given by the fog layer. The suggested fog-assisted health monitoring system is detailed in Sect. 5 followed with a performance assessment study in Sect. 6. Finally, Sect. 7 concludes the paper with the benefits of using the fog computing method in healthcare solutions in conjunction with the cloud, as well as new study topics for future studies.

2 Literature review

This section is focused on the state-of-the-art related works in the current domain of study. In the paper, Monteiro et al. [35] suggest a 3-tier design for individuals with Parkinson's speech problems that are built on service orientation. The suggested design includes an integrated Intel Edison board in the intermediate tier, which acts as a data processing interface and is placed at the patient's house. The fog node takes raw information from the body's wearable intelligent watch, analyzes it, and derives medical characteristics from the patient's voice. Moreover, the presented framework transmits the data to the centralized repository for prolonged utility. The main purpose behind the proposed approach is to simplify the system and move data analysis to the end-user network from the cloud. An IoT-based application is presented by Gia et al. [25] to demonstrate the benefits of the fog computing idea. The authors aimed to improve the quality of medical systems' services by focusing on patients treated both in hospitals and at home. The fog system, which uses a gateway at the edge of the network, works as a supplement to the cloud, assisting data management from medical sensors. Authors used a case study of electrocardiogram (ECG) to illustrate the efficacy of the suggested design. Task scheduling is highlighted by Pham et al. [37] as a crucial factor in the fog-assisted technique as a means of unloading congestion off the network. To offer the most suitable data flow scheduling, the authors use a 3-tier architecture to manage available resources situated both at the fog nodes and cloud platform. Gu et al. [26] proposed a fogging method to assess service distribution in medical systems in terms of quality of service, based on the fog-unit location in the ambiance of the patient. By spreading duties across virtual computers situated in related base stations, the suggested idea intends to aid in the unloading of traffic in the network's core. A smart gateway is built-in

Rahmani et al. [38] based on a similar concept, to improve mobility, energy expenditure, and overall delay in medical applications. To gather and assess healthcare data in real-time reliably, a fog computing node is positioned near healthcare equipment. In Cao et al. [20], a real-time analytic method for assessing falls due to encephalic vascular disease patients was proposed. As claimed by the authors, it was the first healthcare system to use the fog computing paradigm in a large-scale real-time application. For job allocation among end-devices, the described method works in conjunction with the cloud. Many people suffer from chronic heart disease, especially the elderly, and early diagnosis can help improve treatment outcomes. Azmi et al. [1] present a remote monitoring system for health checks. The authors' medical solution combines machine learning algorithms with a computational component to present applications including perception and medical emergency management. An intelligent sensor is situated between IoT devices and cloud computing platforms, and it decides if data is to be forwarded to the cloud, if enhanced powerful analysis is required, or delivered to the gateway, using the same idea as the fog computing concept. Furthermore, the application of deep/machine learning techniques reduces the delay for healthcare warnings, improving patient awareness of health condition in the identification of anomalies. Masip-Bruin et al. [34] investigated the impact of a healthcare monitoring framework for patients having lung illnesses. The authors demonstrate that discovering potential anomalies through real-time monitoring aids in more effective illness management when the doctor or caregiver is promptly alerted. Masip-Bruin et al. [33] proposed a breath-support device that can adjust the oxygen amount according to the patient's needs. The suggested system, which uses a hybrid method of the fog-cloud platform, gathers all data from healthcare sensors via edge computational equipment, assesses information, and responds by the requirement. Even though IoT sensors provide more effective healthcare services, several issues about the security and authenticity of medical data remain unresolved. In this case, Alrawais et al. [4] propose a new approach for enhancing an authentication scheme using revoked certificates, based on the fog computing idea. A management security framework is proposed by Linthicum et al. [31] as a means to aid decisive measures for security issues with minimal or no human interaction. A novel vision of fog computing proposed by Sarkar et al. [39] for comparison with the traditional cloud architecture for delay latency and energy consumption. Furthermore, Varghese et al. [41] stated that when the idea of fog computing is used, 90% of data transmitted from the remote application to the centralized repository is decreased, and latency may be lowered by roughly 20%. This occurs as a result of the analysis module being positioned nearby to the local user where the information is created. As a result, just a portion of the data is transmitted to the cloud for processing when it is needed. The fog computing paradigm is examined by Sarkar et al. [39], where the authors highlighted the benefits of distributed computing at the network's edge to address real-time and latency-sensitive applications. The authors contrasted the fog idea with the cloud platform for energy usage and carbon emissions in the context of IoT technology. Ahmad et al. [2] developed a model to sense medical data and facilitate the interchange of information among medical physicians and patients, based on the same scenario. In terms of using mobile operating systems to enable fog-assisted service delivery, Dantu et al. [22] proposed an effective framework for android operating system devices as a way to show that smartphones may dependably act as edge nodes. On a contrary, owing to a diverse network, implementation is difficult. Alharbi et al. [3] suggested a technique to secure vital information from eavesdropping by encrypting and decrypting communications from IoT devices using a twofold protection approach utilizing a Virtual Private Network (VPN) server. Aside from the approaches for encrypting and decrypting communications, the proposed prototype also uses challenge-response authentication to improve data security. Although the notion of applying security techniques yields positive outcomes, the suggested fog server does not employ encryption since it is intended to be used in a hospital environment. Moreover, all crucial data is placed at the fog node, and the data required for further analysis is communicated to the cloud. Safe data aggregation is demonstrated by Okay et al. [36], where the authors show how to build the fog computing secure data aggregation protocol. Aside from the obvious benefits of reducing the quantity of data kept on the cloud, the suggested system also protects data against privacy breaches. The overall transmission and execution delay of the information accumulation technique enhances as the data quantity at the fog node and cloud increases.

Comprehensively, the literature on fog computing in healthcare has useful contributions. These efforts are taken into account in this study's suggestion for a fog-assisted health monitoring system. Moreover, Table 1 depicts the comparative analysis with the state-of-the-art related research works in the current domain.

3 Resource shifting to fog-node server

This section covers some of the fog computing tier's services, with an emphasis on healthcare solutions. A conceptual healthcare system is depicted in Fig. 2, which is in charge of receiving and processing healthcare information from IoT devices connected through communication protocols including Bluetooth and Wi-Fi. A fog server node is a processing/controlling unit with its hardware and operating system. It is in charge of receiving all data from medical and environmental IoT devices, processing it by application

Table 1 State-of-the-art comparative analysis studies (1: available, 0: not available)

Related Work	Fog	IoT	Temporal analysis	Health care	Cognitive decision	User-centered	Time-sensitive	Precision	Numerical	Stability	Reliability	Security protocols
Monteiro et al. [35]	0	1	0	1	0	0	1	1	0	0	0	0
Gia et al. [25]	0	1	1	1	0	0	0	0	0	0	0	0
Pham et al. [37]	0	1	0	1	0	0	0	0	0	0	0	1
Gu et al. [26]	0	1	0	1	0	0	1	1	0	0	0	0
Masip-Bruin et al. [34]	0	0	0	1	0	0	1	1	0	0	0	0
Alrawais et al. [4]	0	0	0	1	0	0	1	1	0	0	0	0
Sarkar et al. [39]	0	1	0	1	0	0	0	1	0	0	0	0
Varghese et al. [41]	0	1	0	1	0	0	0	1	0	0	1	0
Alharbi et al. [3]	0	1	1	1	0	0	0	1	0	0	0	1
Proposed technique	1	1	1	1	1	1	1	1	1	1	1	1

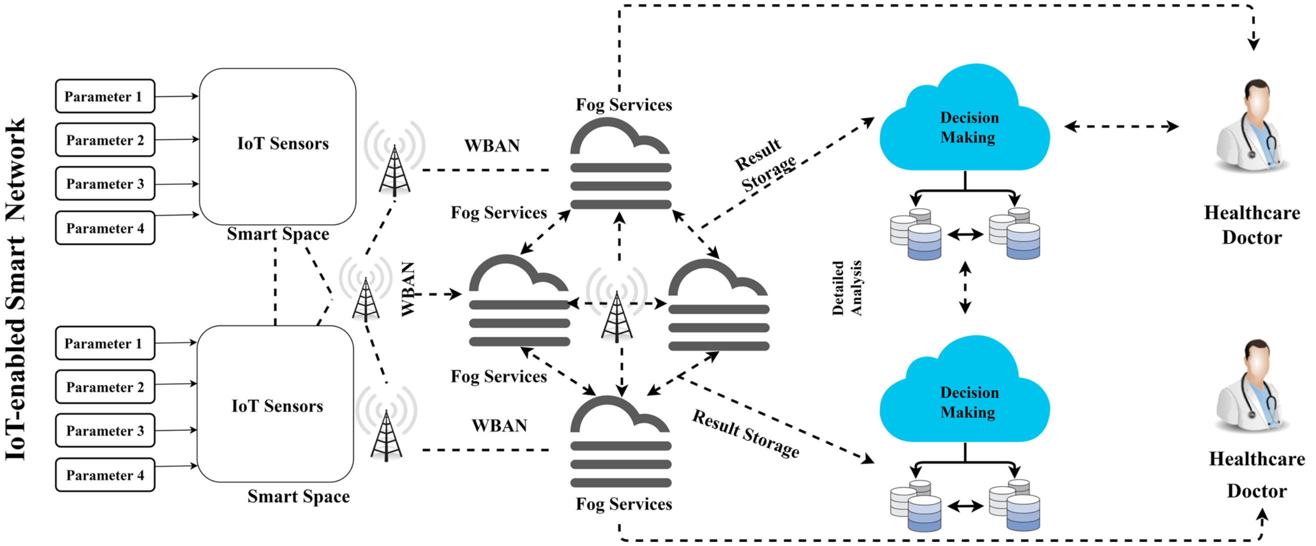


Fig. 2 Conceptual model of fog computing-based healthcare service delivery

of data compression, and encryption. Furthermore, analysis is performed locally by data correlation with prior requests' data. After the data from the analysis is retrieved, the fog-computing node operates automatically in the event of an anomaly. For instance, if a temperature sensor monitors a patient's temperature at a higher threshold, an alert signal is generated to the concerned doctor or nurse. Cloud computing is also used by the fog-computational node. The abstracted data is transmitted for prolonged cloud storage once the received data from the sensors is processed. The doctor and the patient's family may maintain the medical records up to date in this way, allowing for further research exploration. Major components of fog server as shown in Fig. 3 are detailed ahead.

1. **Local/remote data repository:** The remote storing component is required for saving data from healthcare IoT devices in a remote data repository for immediate assessment. Information may be stored in a variety of forms, including kind, size, and priority, using the storage. The data can also be encrypted and compressed if necessary. Another feature of a remote data repository is that many capabilities including data filtration, assessment, and normalization are likewise repository-depended. Moreover, if fog and cloud databases are not connected, the remote repository retains the information in a temporary location till interlinking between fog and cloud is restored.
2. **Data filtration unit:** It is developed to gather healthcare vitals, such as the medical symptoms of patients, and abstract the essential data. Unwanted data, such as noise and electromagnetic interference, is eliminated in the component, and the user data is recorded in a remote repository. By removing unnecessary data from the data acquired by the sensors, the filtering unit enables data minimization.
3. **Data compression unit:** Data compression techniques can be used in some situations to reduce the amount of bandwidth needed in the network for delivering medical data. Data compression methods come in a variety of shapes and sizes. There are two types of compression

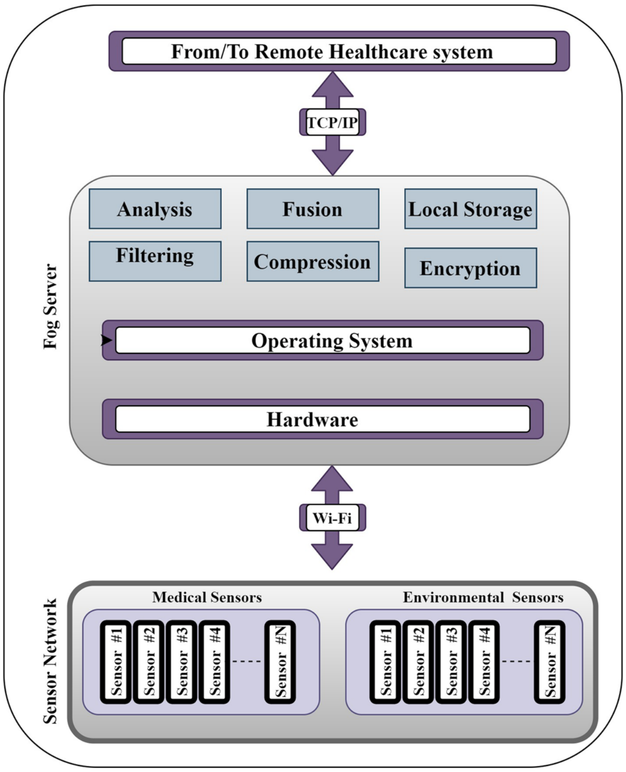


Fig. 3 Major components of fog server

methods: lossless and lossy. When it comes to medical data, the lossless method is preferable since data loss might lead to an incorrect diagnosis. However, as medical IoT devices have restricted power consumption power, this unit is not commonly employed in cloud-based systems. As an example, it is eliminated in fog computing applications by positioning fog node nearby to the patient. Sensors can transmit information to the fog-computational platform, which is responsible for storing, analyzing, and securing the information before delivering it to the centralized repository.

4. **Data fusion unit:** It is the processing unit for combining multiple types of information from the single source to acquire useful attributes from a specific user and ensure that duplicate data is supplied. Consequently, remote information assessment may be increased, while bandwidth costs are decreased at the same time.
5. **Data analysis unit:** This component enables the medical framework to assess the raw information provided by the IoT sensors locally. As a result, the system's overall performance can be improved since the delay latency and telecommunication congestion between the healthcare framework and centralized cloud are decreased. As an instance, in the event of a medical vulnerability, the framework will react more quickly since the data would be analyzed locally rather than being processed in the cloud. Furthermore, in a fog environment, possible connection losses and bandwidth restrictions can be avoided.

4 Beneficial aspects of fog computing

Effective resource utilization is the most important criterion in healthcare applications since resource management failure can have significant repercussions, ranging from sensor node malfunction to inaccurate illness diagnosis. The energy consumption of sensor nodes, as well as the time delay of acquired information shown at patient interfaces, have to be carefully examined. Each of these has been detailed ahead:

1. **Energy efficiency:** Because the bulk of IoT devices/sensors have extremely short battery life, energy spending is constantly a hot issue in the literature. Even though energy is mostly utilized for data transmission, sensing and execution activities are equally important. Hu et al. [21] proposed a systematic technique for determining where a given job should be carried out. By shifting workloads from the cloud to the fog computing platform, the simulations showed that fog-based computation has an improved energy consumption effectiveness. Authors who used fog computing techniques can save up to 40% on energy consumption.
2. **Latency:** The fog paradigm has a significant benefit over cloud-assisted frameworks in that it enables a computational module to be placed closer to devices/sensors. As a result of the decreased physical distance, the overall delay can be considerably reduced [21]. Furthermore, time-sensitive service delivery that requires rapid detection and response to activities might benefit from the adoption of presented ideology, as computational-focused activities can be shifted from sensors with minimal computing power to a capable unit that can handle the processing quicker [26]. Craciunescu et al. [21], who created a fall detection algorithm, presented an example of a time-sensitive framework utilizing an edge computing technique. According to the authors, the fog algorithm enables efficient gathering and processing of medical data by shifting data analysis to an enhanced computing unit positioned at the edge-fog layer.
3. **Security aspects:** A healthcare solution's IoT applications must all be safe. Any security compromise makes the framework vulnerable to unauthorized access, resulting in serious repercussions. Due to a large number of networked devices and a variety of IoT systems, security is one of the most explored issues in the literature. Because no healthcare system can be guaranteed to be completely secure, doctors and medical professionals must set an optimal vulnerability level for each application [32]. Some of the security threats are discussed ahead:
    (a) *Authentication:* It is a crucial need in the IoT domain since the number of networked devices is often extremely large. Furthermore, for energy consumption, IoT devices are severely constrained inability to perform cryptographic operations. Constrained devices, on the other hand, can use a fog node to outsource resources like computational processing and storage, allowing protocols to be executed. Keeping data protected from unauthorized access is a top issue in the healthcare industry. Dsouza et al. [24] offer a policy assessment approach for ensuring information communication by health agents in a safe way over fog computing platform, which addresses the key issues of security in medical settings.
    (b) *Privacy:* Security and privacy are 2 extremely significant problems needed by the majority of IoT applications, not just in healthcare. Even though data encryption is performed, the long distance it travels from the user's computer to the cloud, the more likely its information may be intercepted by hackers. As a result of its proximity to end-devices, the deployment of a fog paradigm enables strengthening the entire security framework. In light of the significance of security in the medical framework, Huang et al. [27]

proposed a technique for safeguarding medical data from unauthorized access. The authors created an improved medical system based on this framework to cope with privacy breaches caused by doctors' engagement in the healthcare procedure.

(c) *Encryption:* Encryption complements the fog layer in comparison to the cloud platform, and information processing by the fog computing platform is transmitted to the cloud. As a result, since healthcare information is vital data, it is recommended to be encrypted before cloud transmission. In light of this, the Aazam et al. [1] presented an additional layer of encryption in a fog computing framework for information security.

5 Proposed fog-assisted medical framework

The aforementioned sections examined the key features of the fog paradigm and emphasized its important advantages in the medical industry. This section details the deployment of a fog-assisted node server for medical service delivery, as well as a comparison of the outcomes to the traditional cloud approach. A healthcare system, in general, uses several networks to link medical equipment to the cloud. Wireless networks that are employed in IoT situations include personal, local, and broad networks [30]. A wireless network formed by sensors and actuators is also another approach to link medical sensors in the healthcare industry. This architecture was created to allow devices to run on very little power, extending battery life [28]. The architecture used in the current research allows a patient to have medical vitals gathered and assessed by an intelligent fog-node server at home or in a hospital to improve life quality and avoid illnesses. The recommended design of the given medical system follows a 3-tier approach, as shown in Fig. 4. All of the sensors and actuators in the first layer are connected through transmission protocol (including 3 G, 4 G, and Wi-Fi). There are 2

Table 2 IoT device specifications

Device/sensors	Model	Power in watts
Fog server	Rasberry Pi Zero W	3.9
NodeMCU	ESP8266	5
Heart rate monitor	AD8232	3
Pulse	SEN-11574	3
Temperature and humidity	DHT11	0.3
Light	LDR GL5528	0.31
Data center	Virtual machine	199
Noise	SEN-12642	0.9

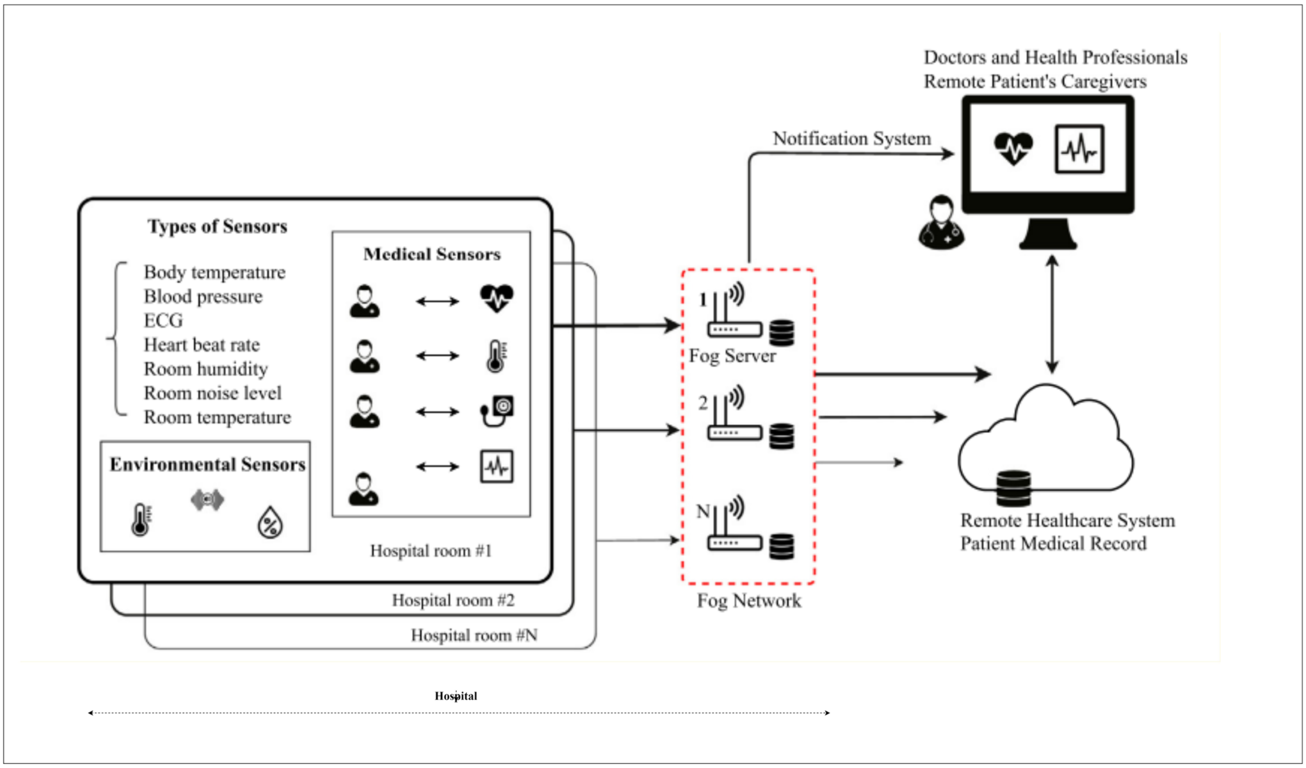


Fig. 4 Proposed data flow mechanism

types of sensors: *healthcare* and *environmental* sensors. The *healthcare* devices are in charge of acquiring the user's vital indicators, such as heart rate, body temperature, and electrocardiogram (ECG). Table 2 depicts the list of IoT sensors incorporated in the current research. The primary API for service delivery is hosted on a fog-node unit and executes on a Raspberry Pi connected to the Zero W Board, a popular platform for IoT development. This board is equipped with an embedded CPU, static and dynamic memory, and transmission unit [40]. The OS is built using Python programming language that handles all of the medical sensor demands. Its primary function is to take raw data, process it, and store the information in remote storage. The remote storage aids in the caching of data required for real-time processing as well as the storage of medical data if the internet connection is interrupted. In addition, the fog server is in charge of data accumulation. The data accumulation unit gathers all of the attributes from a single user, calculates the average measure, and sends it to the normalization unit before transferring the information for storing and visualizing in the cloud. When information is needed, the normalization module compresses it and sends it to the security module. The information is encrypted and transmitted to the cloud in JavaScript Object Notation (JSON) format.

To offer Machine-to-Machine communication, the primary application additionally supports the Message Queuing Telemetry Transport (MQTT) protocol [29]. MQTT was created to function on IoT sensors with limited resources and extensively utilized due to its ease of use and low bandwidth usage. The manner in which messages are exchanged is one of MQTT's most distinguishing features. It is built on a subscription architecture, with a broker component to accept, queue, and deliver signals from healthcare devices to computation devices including fog server and/or cloud applications [5, 23]. The 3rd module of the presented framework is the centralized computational framework of cloud computing. This is where the final component of the system is located. The service is transferred from the fog-computational node to the cloud layer for assessment when a job demands more powerful computational capabilities. Cloud layer serves acts as a permanent storing location and offers a grant to visualizing user information via the internet on the ThingsBoard open-source IoT platform [42].

5.1 Communication sequence

The various components stated before interact in a synchronized manner with the fog computing node in the provided paradigm. Initially, IoT data is collected indiscriminately from sensors implanted in hospitals and healthcare facilities. Based on the time-sensitive data acquisition, the parametric data is transferred to the attached Raspberry Pi (fog computing device). The fog device is equipped with an ARM Cortex-A53 quad-core CPU running at 2.1 GHz and 2GB LPDDR2 SDRAM, as well as the Raspbian Stretch operating system and Apache HTTP server 2.4.34. The data is sent over WiFi, which adheres to the IEEE 802.15.4 standard for safe and cost-effective data connection. The fog node performs real-time local computations on the acquired data and sends a warning alert signal to the doctors for medical parameters that are potentially harmful to the patient's health. Furthermore, the fog computing node uses HTTP RESTful APIs to communicate with cloud services. It uploads input data and downloads results using the HTTP POST method. The data communication is carried out utilizing the IEEE 802.11 WiFi protocol, which is widely available and easy to implement. Table 3 shows the wireless communication protocol's data transmission standard. Furthermore, Microsoft Network Monitor 3.4 is used to track network bandwidth usage. Amazon EC2 cloud with 1vCPU, 2GB RAM, 3GB SSD, Windows Server 2016 is utilized for cloud-based data analysis. Monitoring authorities can do 2 crucial jobs at the cloud level. For starters, regularized real-time monitoring of patient data can be done from remote locations. Software APIs built with

Table 3 Data communication techniques for IoT technology

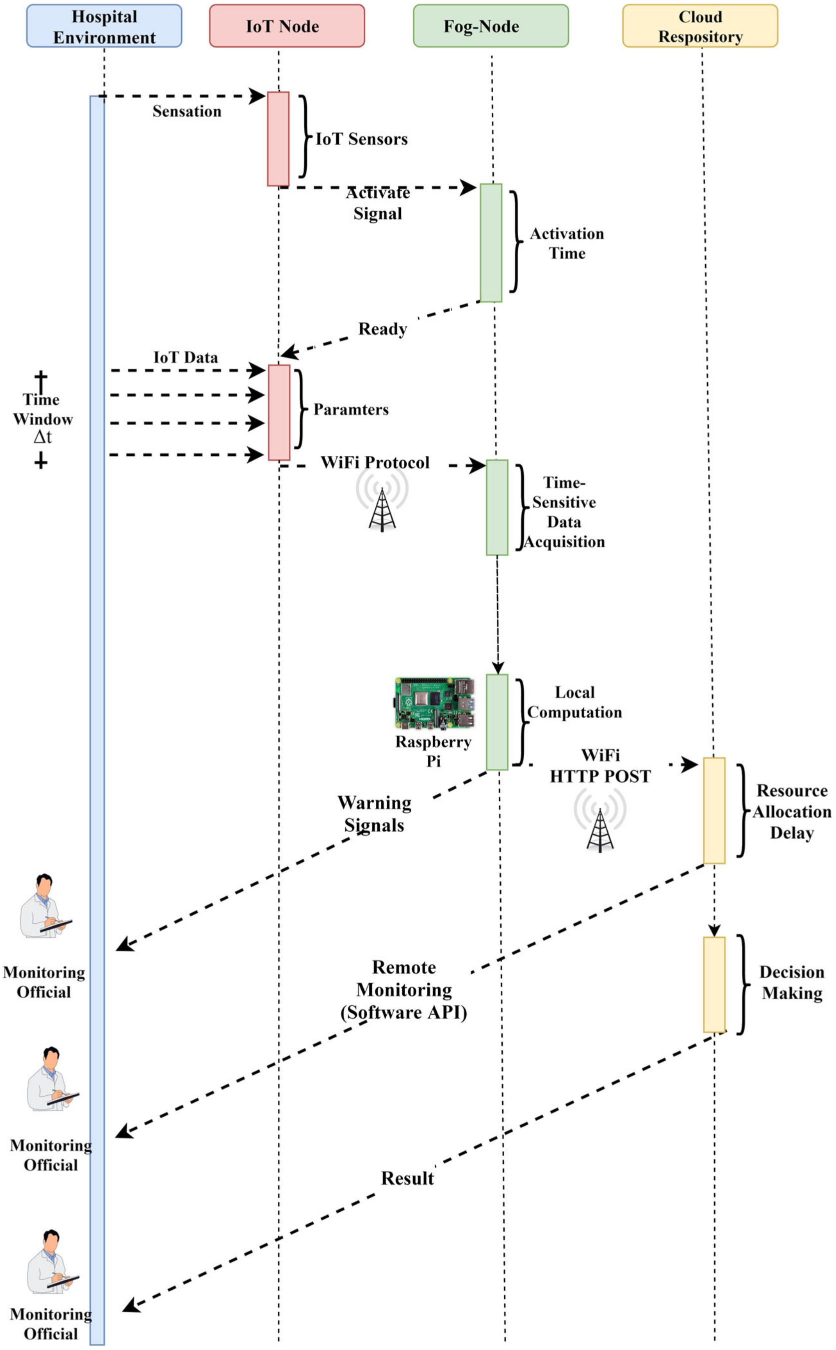
Type	Bluetooth	RFID[NFC]	IrDA	Wi-Fi	UWB	ZigBee
Rate	2.1 Mbps	106 K to 424 Kbps	14.4 Kbps	1 M to 300 Mbps	53 M to 480 Mbps	20 K to 250 Kbps
Band	2.4 GHz	13.56 MHz	850 nm to 900 nm	2.4 G–5 GHz	3.1 G to 10.6 GHz	868 M to 2.4 GHz
Distance	20–200 m	20 cm	0–1 m	50 m	0–10 m	10–75 m
Network nodes	8	2	2	50	-	65000
Security	128 bits AES	High	High	High	High	128 bits AES
Power (mW)	1–100	<1	-	>1000	<1	-
Cost(in $)	2–5	<1	-	25	20	5

the OS-SDK provided with the device can be used to create the visualization. The notifications can also be generated. Figure 5 depicts the complete communication sequence.

5.2 Use-case: hospital scenario

Fog processing enables computation, analysis, and decisive services to be performed near to the data source, which is efficient and faster than conventional techniques. A large number of medical caregivers may be required to ensure patient care on a ward at a hospital. For example, specifically for patients who insist that medical symptoms be taken regularly. If fewer number employees respond to the patients' healthcare requirements, a faulty diagnosis may be made, leading to a worsening of the patient's condition or even death. These experts may be assigned to more essential responsibilities by incorporating a fog-computational node to analyze and regulate the information provided by the IoT devices and healthcare sensors, allowing them to provide better service

Fig. 5 Communication sequence



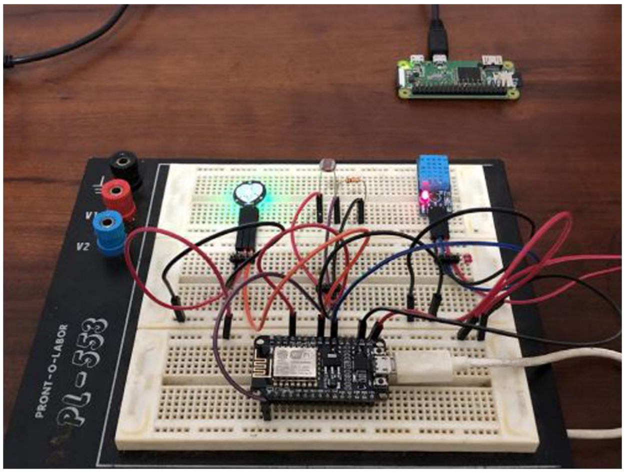


Fig. 6 Fog-node server prototype

to their patients. A doctor or other health expert can be alerted promptly if the system identifies any abnormalities. The ability to utilize information saved in the centralized computational unit for in-depth analysis and illness prevention is an advantage provided by fog computing. The fog approach improves privacy and security by collecting, processing, and analyzing all medical data locally. The only component of the healthcare data that is transmitted to the centralized platform for prolonged storing and visualizing is the patient's medical history.

6 Experimental simulation

6.1 Simulation environment

Two distinct types of experimental situations were used to assess the efficacy and effectiveness of the presented fog-assisted healthcare framework. The first is the conventional approach, which uses a router to link all of the IoT actuators to the underneath cloud-based application. Secondly, the fog server is installed in the intermediate layer and uses the idea of fog computing. Figure 6 depicts a prototype of the suggested healthcare application scenario, which includes a fog-computational node as well as IoT sensors including a heart sensor, illumination device, fever sensor, and humidity preceptor that are all directly linked via wireless communication to the ESP8266. Figures 7 and 8 depict the hardware modules for data computation and accumulation. The findings were derived from a mean of 30 experiments.

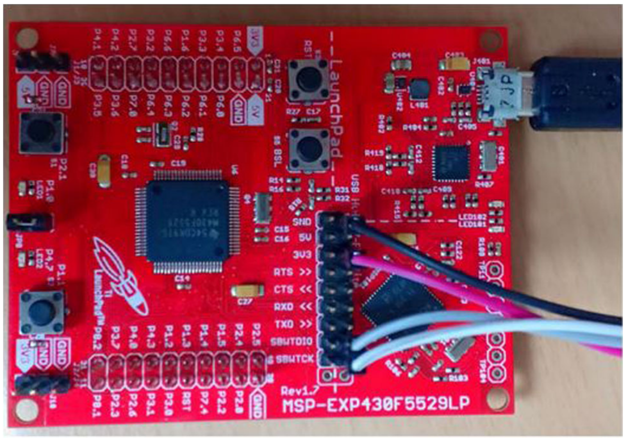


Fig. 7 MSP-EXP430F5529LP for data processing

Fig. 8 Raspberry Pi module for data accumulation

6.2 Network efficiency performance assessment

A unique communication link is distributed across different healthcare service APIs in a distant cloud architecture, which raises the risk of network traffic congestion. Because the limited network availability is shared across all of the medical sensors, a high volume of network traffic has a direct influence on total delay. As a result, due to bandwidth constraints, a single communication may experience a longer delay. Figure 9 shows the result of dividing up the bandwidth

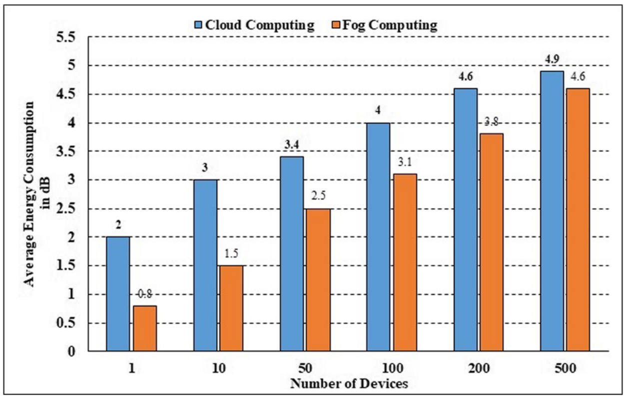
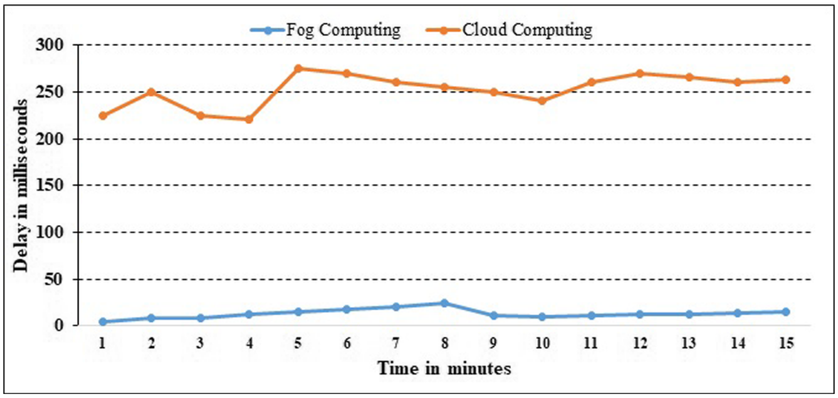


Fig. 9 Energy consumption

Fig. 10 Mean delay latency



across sensors as the number of requests increases. Different from cloud-model, in a fog environment, fog servers can be positioned closer to end devices, and due to which, the network delay can be considerably reduced. Once the system is configured/allocated before usage, the cloud infrastructure requires apps to be housed on powerful virtual machines. In most cases, a single virtual machine is assigned to manage all service requests from medical sensors, but in a fog environment, several fog servers can be assigned to perform a single function at the same time. However, because the virtual machines on the fog servers are less powerful in terms of processing capability, the overall energy consumption is lower than in cloud systems.

6.3 Delay latency

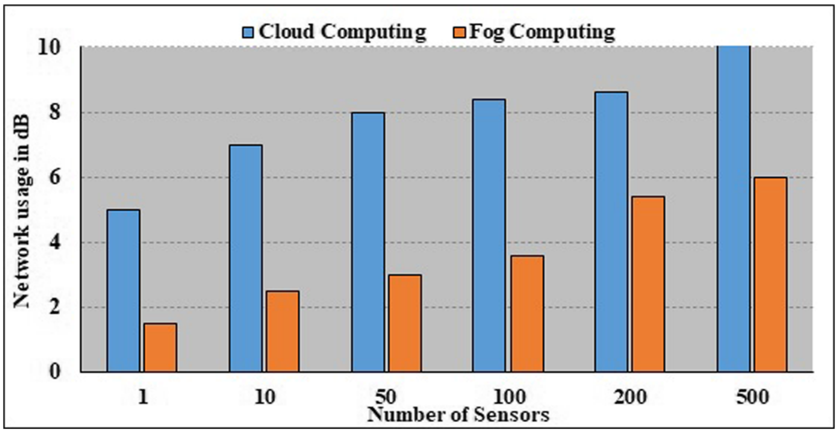
By utilizing many fog servers, the speed of the healthcare system may be enhanced due to the ability of a single application to run on multiple fog nodes. Figure 10 illustrates the advantages of using the proposed method.

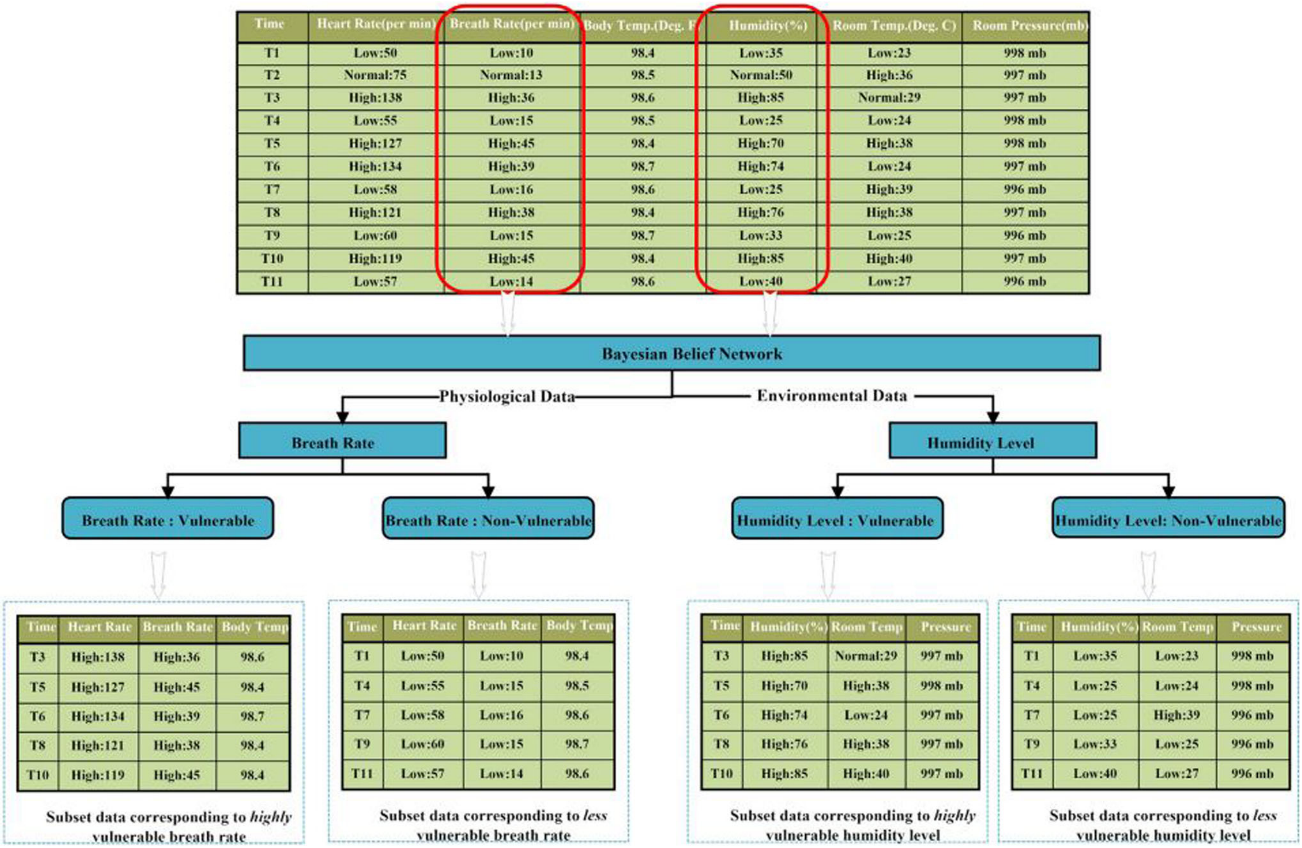
In this set of experiments, assuming that a heartbeat rate is sampled once every second for 24 h with a size of 2 bytes, the network traffic of this particular message is 172.8-kilo Bytes (kB) per sensor in the first scenario, where the sensor sends the data directly to the cloud for processing. For example, if the fog computing concept is used to send the same sort of message, the fog server will be in charge of receiving all messages sent by the sensor and processing them locally. In this instance, just a tiny portion of the data is transferred to the cloud for long-term storage. The fog server then collects all incoming messages from the same patient and types for 6 h, calculates the mean value, and sends just one message to the cloud. As a result, just four messages are sent to cloud each day. After real-time processing, the fog server discards everything else. If a certain piece of data is found to be anomalous during the analysis, the fog server can activate, sending an alarm notification to the doctor or caregiver. A real-time monitoring system hosted on the Thingsboard platform exemplifies this aspect.

6.4 Network utility

Processing data locally has many advantages, including the decrease of delay described above, as well as the reduction of bandwidth usage, which lowers total costs. Figure 11 shows the overall network use for a certain healthcare application dependent on the number of sensors used. As shown in the diagram, when sensors broadcast data to the cloud at all times, the network may get congested, depending on the available bandwidth. In fog-based applications, on the other hand, once

Fig. 11 Network utility





Time	Heart Rate(per min)	Breath Rate(per min)	Body Temp.(Deg. F	Humidity(%)	Room Temp.(Deg. C)	Room Pressure(mb)
T1	Low:50	Low:10	98.4	Low:35	Low:23	998 mb
T2	Normal:75	Normal:13	98.5	Normal:50	High:36	997 mb
T3	High:138	High:36	98.6	High:85	Normal:29	997 mb
T4	Low:55	Low:15	98.5	Low:25	Low:24	998 mb
T5	High:127	High:45	98.4	High:70	High:38	998 mb
T6	High:134	High:39	98.7	High:74	Low:24	997 mb
T7	Low:58	Low:16	98.6	Low:25	High:39	996 mb
T8	High:121	High:38	98.4	High:76	High:38	997 mb
T9	Low:60	Low:15	98.7	Low:33	Low:25	996 mb
T10	High:119	High:45	98.4	High:85	High:40	997 mb
T11	Low:57	Low:14	98.6	Low:40	Low:27	996 mb

Time	Heart Rate	Breath Rate	Body Temp
T3	High:138	High:36	98.6
T5	High:127	High:45	98.4
T6	High:134	High:39	98.7
T8	High:121	High:38	98.4
T10	High:119	High:45	98.4

Subset data corresponding to *highly* vulnerable breath rate

Time	Heart Rate	Breath Rate	Body Temp
T1	Low:50	Low:10	98.4
T4	Low:55	Low:15	98.5
T7	Low:58	Low:16	98.6
T9	Low:60	Low:15	98.7
T11	Low:57	Low:14	98.6

Subset data corresponding to *less* vulnerable breath rate

Time	Humidity(%)	Room Temp	Pressure
T3	High:85	Normal:29	997 mb
T5	High:70	High:38	998 mb
T6	High:74	Low:24	997 mb
T8	High:76	High:38	997 mb
T10	High:85	High:40	997 mb

Subset data corresponding to *highly* vulnerable humidity level

Time	Humidity(%)	Room Temp	Pressure
T1	Low:35	Low:23	998 mb
T4	Low:25	Low:24	998 mb
T7	Low:25	High:39	996 mb
T9	Low:33	Low:25	996 mb
T11	Low:40	Low:27	996 mb

Subset data corresponding to *less* vulnerable humidity level

Fig. 12 Bayesian Belief Network classification

the local data is analyzed at the edge of the network, network traffic may be significantly reduced, preventing communication obstruction and associated delays.

6.5 Classification efficiency

The suggested model's classification performance is defined by the estimation of 3 different performance metrics: specificity (Spe), precision (Pre), and sensitivity (Sen) (Sen). The classifiers include conventional Bayesian Belief Network with fog computing (BBN-f), Bayesian Belief Network with cloud computing(BBN-c), and Bayesian Belief Network with fog and cloud computing(BBN-fc), for data categorization in the fog computing environment. Furthermore, it should be highlighted that just the computing approach is changed during deployment, while the rest of the model remains the same. Figure 12 shows an instance of data classi-

Table 4 BBN classification efficiency (*Pre* precision, *Spe* specificity, *Sen* sensitivity)

Model	BBN-fc			BBN-f			BBN-c		
Dataset	Pre	Spe	Sen	Pre	Spe	Sen	Pre	Spe	Sen
4000	95.35%	93.94%	94.62%	94.82%	91.02%	92.67%	94.42%	91.14%	90.11%
8000	94.78%	93.84%	94.02%	93.72%	93.24%	93.77%	93.02%	93.69%	91.14%
12000	95.57%	93.57%	94.42%	93.82%	92.13%	94.04%	92.09%	92.45%	91.01%
16000	95.75%	93.95%	93.12%	94.62%	91.04%	92.89%	94.12%	92.67%	92.49%
20000	93.86%	94.98%	94.64%	93.82%	92.22%	91.09%	93.63%	93.25%	90.69%
24000	94.54%	94.82%	93.12%	94.21%	93.14%	91.07%	94.09%	93.09%	89.86%
28000	94.82%	93.93%	92.21%	92.23%	90.81%	90.14%	92.14%	91.89%	89.16%
32000	94.62%	92.54%	94.62%	94.12%	91.45%	90.15%	94.06%	90.89%	91.34%
36000	94.87%	92.30%	95.42%	93.44%	93.10%	90.04%	92.18%	90.42%	93.14%
40000	94.42%	93.01%	93.42%	93.22%	92.89%	92.10%	93.18%	90.14%	91.30%

fication using BBN model. In addition, as shown in Table 4, the average of the results for various datasets.

1. For the datasets provided, the presented model is capable of reporting an overall precision of 94.85%. BBNc and BBN-f, on the other hand, were able to achieve precision values of 93.29% and 93.82%, respectively. As a result, in the current context, the proposed BBM-fc model is significantly more exact than other computing techniques.
2. When it comes to specificity, the provided model outperforms BBN-f (92.10%) and BBN-c with a score of 93.63 %. In terms of specificity analysis, the BBN-fc model outperforms other models.
3. The importance of sensitivity analysis in achieving the efficiency of the presented model cannot be overstated. The suggested healthcare model with BBN-fc achieves a high value of 94.16%, compared to BBN-f values of 91.83% and BBN-c values of 91.04%.

The BBN-fc model outperformed state-of-the-art computing models in many simulations, indicating that it is exceptionally successful in the given circumstance.

6.6 Reliability

The reliability analysis is a crucial tool for evaluating the proposed model's overall efficiency. To assess the improvement, the findings are compared for traditional monitoring, cloud computing, fog computing, and cloud-fog computing. As previously stated, cloud-fog-based healthcare model is highly effective because it is based on state-of-the-art computing approaches. Figure 13 demonstrates that the suggested cloud-fog model may obtain an average reliability of 92.69% across a variety of datasets. In comparison, the traditional system obtained 85.09% reliability rating, cloud obtained a 89.21% dependability value, and fog computing obtained a 90.32% reliability value. As a result, the presented cloud-fog healthcare modeling's superior trend for reliability analysis shows the effectiveness of healthcare assessment in the intelligent framework of hospitals and healthcare centers.

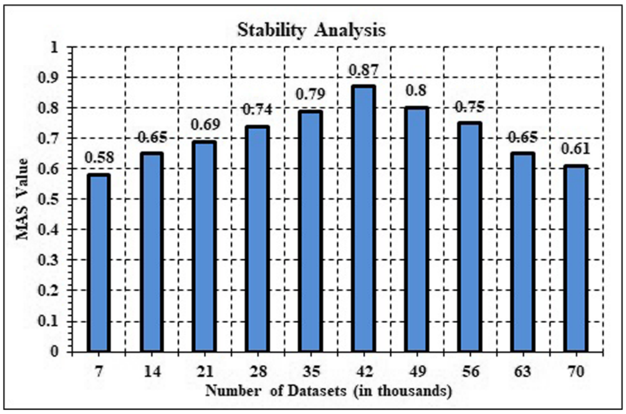
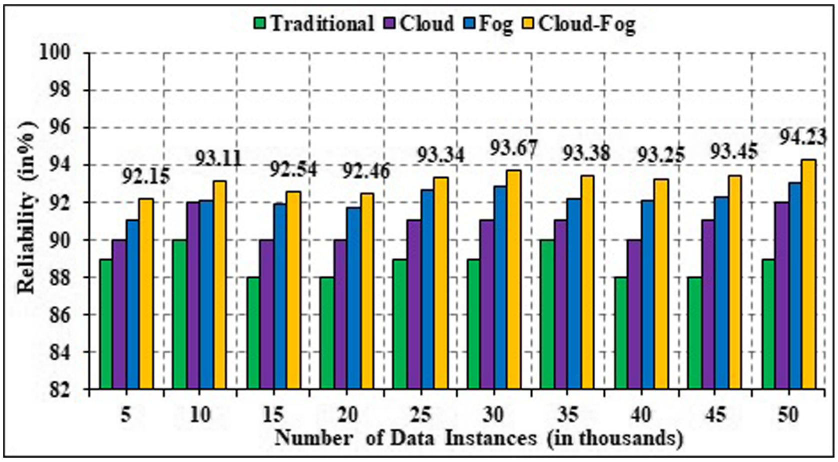


Fig. 14 Stability analysis

6.7 Stability

The system's resistance to processing huge datasets is the topic of the stability analysis. As the size of the datasets grows, the model must be stabilized in order to manage massive IoT data. The System Precise Shift (SPS) is used to assess system stability. It is a probabilistic number used to assess the stability estimation of a modeling technique. SPS values range from 0 to 1. The number 0 denotes the least stable state, whereas 1 denotes the most stable state. The total results of the provided technique are shown in Fig. 14. It has been discovered that the proposed cloud-fog model can register a minimum value of 0.58 and a maximum value of 0.87, yielding an average value of 0.73. As a result, the provided model can be inferred to be extremely efficient and stable.

Fig. 13 Reliability analysis



7 Conclusion

The novel vision of fog-node-based computation was introduced in the domain of medical care in the current article. It was thoroughly detailed, and its performance was assessed using real-world tests in comparison to a typical strategy relying only on cloud computing. The primary advantages of this method in terms of patient health parameter monitoring and control have been discussed. A thorough examination of the major resources made available by locating computational analysis and storage at the network's edge, with an emphasis on e-Health solutions, was conducted. The authors demonstrated a complete deployment of a fog-assisted health monitoring system to aid health professionals in decision-making and illness prevention. Fog computing, in general, provides techniques for dealing with enormous amounts of data created by the Internet of Things devices. By locating cloud resources close to the source of the produced data, healthcare solutions can benefit from shorter processing times and lower energy use. Because data is analyzed locally, the fog tier also helps to reduce data traffic in the network's core. As a result, just a tiny quantity of data is transferred to a cloud infrastructure. Furthermore, because health records are thought to contain highly sensitive information, all confidential medical information may be stored locally, increasing data security.

A multi-tenant method is becoming a popular option to cater to many customers due to the rising number of networked IoT devices. However, in terms of service quality needs, effective resource allocation and job scheduling have not been thoroughly investigated. Furthermore, because of the variety of the fog environment, the interaction between devices tends to be more complicated. As a result, in healthcare applications, a trust management framework among these devices is important. These are some ideas for further research.

Acknowledgements This study is supported via funding from Prince Sattam bin Abdulaziz University under the project number (2023/01/26 407)

Data Availability The data used to support the findings of this study are available from the corresponding author upon request.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Aazam M, Huh E-N (2014) Fog computing and smart gateway based communication for cloud of things. In: 2014 International Conference on Future Internet of Things and Cloud, pages 464–470. IEEE
2. Ahmad M, Amin MB, Hussain S, Kang BH, Cheong T, Lee S (2016) Health fog: a novel framework for health and wellness applications. J Supercomput 72(10):3677–3695
3. Alharbi S, Rodriguez P, Maharaja R, Iyer P, Subaschandrabose N, Ye Z (2017) Secure the internet of things with challenge response authentication in fog computing. In: 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), pages 1–2. IEEE
4. Alrawais A, Alhothaily A, Hu C, Cheng X (2017) Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput 21(2):34–42
5. Bandyopadhyay S, Bhattacharyya A (2013) Lightweight internet protocols for web enablement of sensors using constrained gateway devices. In: 2013 International Conference on Computing, Networking and Communications (ICNC), pages 334–340. IEEE
6. Bhatia M (2020) Fog computing-inspired smart home framework for predictive veterinary healthcare. Microprocess Microsyst 78:103227
7. Bhatia M (2020) Game theory based framework of smart food quality assessment. Trans Emerg Telecommun Technol 31(12):e3926
8. Bhatia M, Kaur S, Sood SK (2020) IoT-inspired smart toilet system for home-based urine infection prediction. ACM Transactions on Computing for Healthcare 1(3):1–25
9. Bhatia M, Kaur S, Sood SK, Behal V (2020) Internet of things-inspired healthcare system for urine-based diabetes prediction. Artif Intell Med 107:101913
10. Bhatia M, Kumari S (2021) A novel IoT-fog-cloud-based healthcare system for monitoring and preventing encephalitis. Cognitive Computation 1–18
11. Bhatia M, Manocha A (2020) Cognitive framework of food quality assessment in IoT-inspired smart restaurants. IEEE Internet of Things Journal
12. Bhatia M, Sood S, Sood V (2020) A novel quantum-inspired solution for high-performance energy-efficient data acquisition from IoT networks. Journal of Ambient Intelligence and Humanized Computing, pages 1–20
13. Bhatia M, Sood SK (2017) A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: a predictive healthcare perspective. Comput Ind 92:50–66
14. Bhatia M, Sood SK (2017) Game theoretic decision making in IoT-assisted activity monitoring of defence personnel. Multimedia Tools Appl 76(21):21911–21935
15. Bhatia M, Sood SK (2018) An intelligent framework for workouts in gymnasium: M-health perspective. Comput Electr Eng 65:292–309
16. Bhatia M, Sood SK (2019) Exploring temporal analytics in fog-cloud architecture for smart office healthcare. Mob Netw Appl 24(4):1392–1410
17. Bhatia M, Sood SK (2020) Quantum computing-inspired network optimization for IoT applications. IEEE Internet of Things Journal 7(6):5590–5598
18. Bhatia M, Sood SK, Kaur S (2019) Quantum-based predictive fog scheduler for IoT applications. Comput Ind 111:51–67
19. Bhatia M, Sood SK, Kaur S (2020) Quantumized approach of load scheduling in fog computing environment for IoT applications. Computing 1–19
20. Cao Y, Chen S, Hou P, Brown D (2015) Fast: a fog computing assisted distributed analytics system to monitor fall for stroke mitigation. In: 2015 IEEE international conference on networking, architecture and storage (NAS), pages 2–11. IEEE
21. Craciunescu R, Mihovska A, Mihaylov M, Kyriazakos S, Prasad R, Halunga S (2015) Implementation of fog computing for reliable e-health applications. In: 2015 49th Asilomar Conference on Signals, Systems and Computers pages 459–463. IEEE

22. Dantu K, Ko SY, Ziarek L (2017) Raina: reliability and adaptability in android for fog computing. IEEE Commun Mag 55(4):41–45
23. De Caro N, Colitti W, Steenhaut K, Mangino G, Reali G (2013) Comparison of two lightweight protocols for smartphone-based sensing. In: 2013 IEEE 20th Symposium on Communications and Vehicular Technology in the Benelux (SCVT), pages 1–6. IEEE
24. Dsouza C, Ahn G-J, Taguinod M (2014) Policy-driven security management for fog computing: preliminary framework and a case study. In: Proceedings of the 2014 IEEE 15th international conference on information reuse and integration (IEEE IRI 2014), pages 16–23. IEEE
25. Gia TN, Jiang M, Rahmani A-M, Westerlund T, Liljeberg P, Tenhunen H (2015) Fog computing in healthcare internet of things: a case study on ECG feature extraction. In: 2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing, pages 356–363. IEEE
26. Gu L, Zeng D, Guo S, Barnawi A, Xiang Y (2015) Cost efficient resource management in fog computing supported medical cyber-physical system. IEEE Transactions on Emerging Topics in Computing 5(1):108–119
27. Huang H, Gong T, Ye N, Wang R, Dou Y (2017) Private and secured medical data transmission and analysis for wireless sensing healthcare system. IEEE Transactions on Industrial Informatics 13(3):1227–1237
28. Kashi SS, Sharifi M (2012) Connectivity weakness impacts on coordination in wireless sensor and actor networks. IEEE Communications Surveys & Tutorials 15(1):145–166
29. Kayal P, Perros H (2017) A comparison of IoT application layer protocols through a smart parking implementation. In: 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), pages 331–336. IEEE
30. Lee W, Nam K, Roh H-G, Kim S-H (2016) A gateway based fog computing architecture for wireless sensors and actuator networks. In: 2016 18th International Conference on Advanced Communication Technology (ICACT), pages 210–213. IEEE
31. Linthicum DS (2017) Connecting fog and cloud computing. IEEE Cloud Computing 4(2):18–20
32. Madsen H, Burtschy B, Albeanu G, Popentiu-Vladicescu FL (2013) Reliability in the utility computing era: towards reliable fog computing. In: 2013 20th International Conference on Systems, Signals and Image Processing (IWSSIP), pages 43–46. IEEE
33. Masip-Bruin X, Marín-Tordera E, Tashakor G, Jukan A, Ren G-J (2016) Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems. IEEE Wireless Commun 23(5):120–128
34. Masip-Bruin X, Marín-Tordera E, Alonso A, Garcia J (2016) Fog-to-cloud computing (f2c): the key technology enabler for dependable e-health services deployment. In: 2016 Mediterranean ad hoc networking workshop (Med-Hoc-Net), pages 1–5. IEEE
35. Monteiro A, Dubey H, Mahler L, Yang Q, Mankodiya K (2016) Fit: a fog computing device for speech tele-treatments. In: 2016 IEEE international conference on smart computing (SMARTCOMP), pages 1–3. IEEE
36. Okay FY, Ozdemir S (2018) A secure data aggregation protocol for fog computing based smart grids. In: 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), pages 1–6. IEEE
37. Pham X-Q, Huh E-N (2016) Towards task scheduling in a cloud-fog computing system. In: 2016 18th Asia-Pacific network operations and management symposium (APNOMS), pages 1–4. IEEE
38. Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P (2018) Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Futur Gener Comput Syst 78:641–658
39. Sarkar S, Misra S (2016) Theoretical modelling of fog computing: a green computing paradigm to support IoT applications. Iet Networks 5(2):23–29
40. Upton E, Halfacree G (2014) Raspberry Pi user guide. John Wiley & Sons
41. Varghese B, Wang N, Nikolopoulos DS, Buyya R (2020) Feasibility of fog computing. In: Handbook of Integration of Cloud Computing, Cyber Physical Systems and Internet of Things, pages 127–146. Springer
42. Vilela PH, Rodrigues JJPC, Solic P, Saleem K, Furtado V (2019) Performance evaluation of a fog-assisted IoT solution for e-health applications. Futur Gener Comput Syst 97:379–386