The Journal of Supercomputing (2023) 79:3999–4020
https://doi.org/10.1007/s11227-022-04788-7

IoT-fog-based healthcare 4.0 system using blockchain technology

Israr Ahmad[1] · Saima Abdullah[1] · Adeel Ahmed[1]

Accepted: 24 August 2022 / Published online: 17 September 2022

Abstract

Real-time tracking and surveillance of patients' health has become ubiquitous in the healthcare sector as a result of the development of fog, cloud computing, and Internet of Things (IoT) technologies. Medical IoT (MIoT) equipment often transfers health data to a pharmaceutical data center, where it is saved, evaluated, and made available to relevant stakeholders or users. Fog layers have been utilized to increase the scalability and flexibility of IoT-based healthcare services, by providing quick response times and low latency. Our proposed solution focuses on an electronic healthcare system that manages both critical and non-critical patients simultaneously. Fog layer is distributed into two halves: critical fog cluster and non-critical fog cluster. Critical patients are handled at critical fog clusters for quick response, while non-critical patients are handled using blockchain technology at non-critical fog cluster, which protects the privacy of patient health records. The suggested solution requires little modification to the current IoT ecosystem while decrease the response time for critical messages and offloading the cloud infrastructure. Reduced storage requirements for cloud data centers benefit users in addition to saving money on construction and operating expenses. In addition, we examined the proposed work for recall, accuracy, precision, and F-score. The results show that the suggested approach is successful in protecting privacy while retaining standard network settings. Moreover, suggested system and benchmark are evaluated in terms of system response time, drop rate, throughput, fog, and cloud utilization. Evaluated results clearly indicate the performance of proposed system is better than benchmark.

✉ Israr Ahmad
rao_israr@yahoo.com

Saima Abdullah
abdullahsaima@yahoo.com

Adeel Ahmed
adeelmcs@gmail.com

[1] Department of Computer Science and IT, The Islamia University of Bahawalpur, Punjab 63100, Pakistan

Keywords Healthcare 4.0 · Message scheduling · Wireless sensor networks

1 Introduction

Recently, the IT sector has appeared to be vibrant with several new fields, e.g., healthcare 4.0 [1], interconnected industries, smart factories, industry 4.0 [2], and embedded Internet of Things (IoT). Today, we are on the edge of a technological insurgency that has radically transformed the way we live and work [3]. This change will be unprecedented in terms of both complexity and efficiency in human history. Internet-connected devices are increasingly being used in a wide range of industries to make manufacturing smarter, as well as health care smarter, cities smarter and homes smarter. Because of the huge volumes of data generated every second by smart machines and systems, decision-making has become extremely relevant. It is becoming increasingly common for researchers to focus on developing physical systems and embedded smart appliances as a research and development focus. Hardware and software systems in real-time embedded systems [4] are subjugated to many limitations, and pervasive computing must react within given time restrictions or deadlines. The message scheduler of embedded devices [5] should be equipped with smart decision-making capabilities so that it can make the best use of available resources and the order in which messages are run.

Advanced networking and rapidly advancing digital processing technology have aided in the expansion of a variety of digital services [6]. Numerous services use the IoT as a way to communicate with processes and objects, enhancing social interaction among people. Technologists and researchers have been forced to move from a centralized to a decentralized framework by these microservices. As a result, smart homes, smart cities, smart transportation systems, smart wearables, and smart health care are all developing [7]. Therefore, it is clear that data technology has been added to modern internet technology to support the growth of smart devices, which generate a significant amount of data. A group of major information technology (IT) organizations, including Amazon, Google, Microsoft, Apple, and many others, have already set up cloud data centers (DCs) [8] to process and store data produced by a range of applications and solutions on a pay-per-use basis. Despite the fact that the method actually works effectively, it is more appropriate for latency-tolerant devices than for real-time applications. The construction of a fog computing (FC) [9] management plane near end devices to promote portability and data localization has been prompted by the expectation that the current rate of data generation would result in a 92% data workload in the coming years.

Due to a strong push and deployment of all services by healthcare experts, suppliers, patients, and governments, e-healthcare facilities play a crucial part in people's health. In the conventional medical model, patients must be hospitalized in order to have their health issues examined and tracked locally. We explore the development of smart technologies and the security requirements for applying them in the medical industry. The advantages of distributed ledger technology are covered, as well as potential applications for healthcare organizations [10]. Since the beginning of healthcare services in the 1970s, the development of adaptable IT platforms has been observed. This period is referred to as healthcare 1.0. The Healthcare 2.0 era was defined as the period from 1991 to 2005 [11] when medical systems were insufficient and not associated with digital systems, which caused a lack of resources. The development of contemporary healthcare systems took place during this time as healthcare and information systems were merged. The development of advanced tracking during this time period gave doctors access to scanning technologies for assessing patients' conditions. New user-enabled technologies began to arrive in the healthcare sector at the same time that social media started to take off. Healthcare practitioners are beginning to create online communities where expertise can be shared, data are stored on cloud storage, and patient records are accessible on mobile devices. This makes it possible for the patient and the doctor to have easy accessibility. Critics emphasized their concern with the erroneous information given and the violation of patients' privacy during this period. Healthcare 3.0, which allowed users to choose how patient healthcare information was delivered, developed simultaneously as Web 3.0 [12].

Interfaces have grown more streamlined and adaptable, enabling more individualized and optimized experiences. The introduction of wearable and embedded technologies, as well as electronic healthcare records (EHRs) [13], made it possible to track patients' medical conditions everywhere, in real time. In a similar vein, EHR systems started to appear that used standalone, non-networked technology like social networks to store patient data. The process has been simplified by the sharing of health data through networked channels, such online networking, between practitioners using EHR systems. The interaction and communication between medical staff and patients have also improved. The healthcare 4.0 approach has been our way of living since 2016. This era was motivated by the idea of Industry 4.0, where strong and high-touch systems are implemented and blockchains are developed to enable real-time access to patient clinical data using cloud services, fog and computing capabilities, big data analytics, artificial intelligence, and deep learning. The primary objective of this phase is to advance virtualization, enabling real-time customized health care. With the potential to improve health care's predictability and specialization, collaboration, coherence, and convergence are currently in the spotlight.

Information about healthcare necessitates an exceptionally high level of confidentiality and security. Personal privacy is the ability to permit or disclose personal information to third parties. Collaboration between authorities and healthcare experts is required for this, as well as the creation of accepted policies and procedures. To protect their healthcare data, many countries have passed legislation and security regulations. Since the start of the 4.0 healthcare era, smart technologies have become more and more important to medical practitioners. These technologies provide the transmission, receiving, and collecting of patient records for health recordkeeping, as well as the cure and diagnostics of certain diseases. To be successful, a healthcare provider must have high-quality data stored in EHR systems. As a result, data must always secure and risk-free. The technologies used might not function properly or be regarded as reliable if these requirements are not met.

The specific tasks that fog computing accomplishes depend on the application and domain. Filtering, aggregating, analyzing, and swiftly storing data are common activities [14]. Fog computing can be done by a single node or by a group of nodes working together. As a result, there are more adaptability, scalability, and redundancy control because new fog nodes can be added as more computational power is required. Fog computing is influenced by many of the same ideas as cloud computing. Using a decentralized network and blockchain technology, data are saved in tamper-resistant formats. Because blockchain transactions may only be amended or added by generating new hash values, prior transactions cannot be changed. To comprehend it, the prospective use of distributed ledger technology must be compared to all of the characteristics that distinguish the blockchain from others: [15]

- Distributed ledger: By eradicating a single point of failure, transactions are scattered over a network, ensuring system recovery.
- Consensus tactic: Transactions are only recorded when the terms of the transaction are accepted by all authorized network users.
- Provenance: The entire history of data stored on the blockchain network.
- Integrity: Network record cannot be manipulated or tampered with, ensuring the security and trustworthiness of all data.
- Finality: When a transaction is added to a blockchain and confirmed, it can no longer be changed or undone.
- Smart contract: Codes are written on simply on blockchain network and are mostly executed by computers and nodes when an event occurs. The programs automatically run within the specified time period or condition.

1.1 Contributions

Our research focuses on the key contributions of fog brokering, such as the segregation of messages at the fog broker into critical and non-critical patient conditions for quick response to critical symptoms of patients, obtaining cloud services for data mining to reduce operating costs, and access point add the priority with comparing received value to the predefined threshold values.

2 Related work

Integrating blockchain and cloud technologies, Badr et al. [16] provide a multitier framework for implementing IoT into EHR systems. The suggested method employs elliptic curve cryptography (ECC) that has the potential to provide greater security than existing cryptographic systems. The approach, however, does not enable access to health records on a local level. They are instead accessed through some kind of blockchain cloud service, which is not discussed in this paper. The fastened and smart healthcare system is proposed by Tripathi et al. [17] in [1] to ensure privacy and security in healthcare systems. The project collects EHR data from IoT wearable technology to use a smart sensor network (WSN) architecture. Before putting data in the cloud, a blockchain is used to encrypt and standardize it. To prevent data fragmentation and also provide people with better access to their personal information, shen et al. [18] propose a clinical data sharing method. The architecture has a dual-network structure for mutable and immutable data. Silva et al. [19] describe a fog approach for managing medical records using blockchain as well as the cloud. The main goal of the solution is to give patients control over their personal data. To build a decentralized blockchain permission layer and make data available to applications, fog nodes are placed strategically close to sensors. The paper offers a case study that examines the performance, transparency, and accessibility of suggested architecture in different scenarios, including residential health care. Tuli et al. [20] introduce a methodology for connecting IoT devices, fog, and cloud platforms. The proposal comprises of numerous fog nodes located near sensors that provide computing and data processing capacity. Whenever fog nodes become congested, the infrastructure as a service serves as a back-end. Furthermore, blockchain is used to protect the integrity of secret data in the fog layer. The study did not rely on EHR in specifically. The authors, on the other hand, use sleep paralysis as a research study.

To store and manage electronic health records, Vora et al. [21] suggest a blockchain-based architecture. This strategy employs many smart contracts to isolate various sorts of data. Giving patients privacy and revealing confidential information are the main goal of this research. Akkaoui et al. [22] provide the EdgeMediChain architecture, which merges edge and blockchain technologies to simplify the exchange of medical data. It is a system that incorporates identification and authorization for gathering patient data via IoT medical devices. The architecture's main contribution is its capacity to utilize edge-mining pools to handle data from numerous sensors concurrently. Numerous edge nodes in each mining pool evaluate data from sensors placed in a specific area. [5] The goal of Amir Latif et al. [23] is to emphasize data sharing while also attempting to communicate patient information among other hospitals. The research suggests using smart contracts to store historical patient records in a blockchain-based architecture. Deep learning (DL) was proposed by Almaiah et al. [24] as a lightweight authentication mechanism and preservation technique for IoT-based CPS to enable decentralized authentication across legal devices. Authors have reduced the validation time among coupling devices with decentralized authentication, which was followed by better communication statistics. To enable a secure searching and keyword-based access to the database, Ali et al. [25] presented a distributed database using a homomorphic encryption approach. A secure key revoking mechanism is also offered by the suggested solution, and various policies are updated accordingly. To address the efficiency and security difficulties in the existing schemes for exchanging both forms of digital healthcare data, a robust patient healthcare information access scheme has been developed that merges blockchain and trust chain. The solution presented by Rahmadika et al. [26] makes use of privacy preserving bidirectional long short-term memory (BiLSTM) while enhancing security by incorporating blockchain technology built on the Ethereum smart contract setting. Further, the efficacy of the suggested model is empirically tested for exhaustiveness, commensurate incentive schemes with an untrace ability characteristic, and compact findings from a different neural network technique.

Hannah et al. [27] examined the usage of deep neural networks built on a blockchain to transmit healthcare data more quickly and efficiently. The study displays real-time health surveillance for classification and evaluates the speed and accuracy of the responses. The model of deep learning divides brain conditions into benign and malignant categories. The study considers three separate classes—including AD, moderate cognitive deficits, and normal cognitive level—to predict whether a brain disease is benign or malignant. The majority of the data used in the study is used to train these classifiers in an ensemble model, and a metaclassifier is used to categorize the final resultant class. Hannah et al. [28] examined the usage of deep neural networks built on a blockchain to transmit healthcare data more quickly and efficiently. The study displays real-time health surveillance for classification and evaluates the speed and accuracy of the responses. The model of deep learning divides brain conditions into benign and malignant categories. The study considers three separate classes—including AD, moderate cognitive deficits, and normal cognitive level to predict whether a brain disease is benign or malignant. The majority of the data used in the study is used to train these classifiers in an ensemble model, and a metaclassifier is used to categorize the final resultant class.

Das et al. [29] investigated the potential and advantages of combining cloud computing with fog as well as edge-based computing to offer people urgent healthcare services. Using interconnected IoT-edge-fog-cloud computing environments, RESCUE (enabling green healthcare services) is an end-to-end framework that includes an effective spatial–temporal data and analytics module for effective information sharing and spatial–temporal data processing to predict the path for users to take to get to their destination (a hospital or relief camps) with the least amount of delay during an emergency (say, natural disaster). The proprietary blockchain-assisted EHR management was proposed by Ray et al. [30] exploits IoT usage in healthcare. In order to enable secure and trustworthy data transfer and prompt analysis of data sent over IoT networks, innovative blockchain integrated swarm exchange architectures were specifically suggested as the backbone of the suggested method. To deploy EHR transmission securely, a dynamic and modular server support technology is used with an autonomous encryption–decryption technique. Additionally, a number of swarm listen, announcement, peer open, and peer closure algorithms are included in order to take advantage of the true potential of pervasive EHR transmission for improved delivery of e-healthcare services. In order to diagnose the COVID-19 disease, Golec et al. [31] propose the security- and privacy-based lightweight framework known as iFaaSBus. This framework uses the idea of the Internet of Things (IoT), machine learning and Fnction as a Service (FaaS) or serverless computing. It also controls resources automatically to enable dynamic scalability. To secure the patient's health data, iFaaSBus uses OAuth-2.0 Authentication protocol-based transparency and JSON Web Token and Transport Layer Socket protocol-based security.

The protocol presented by Premkumar et al. [32] was contrasted with the traditional approach, the cognitive radio-based heterogeneous wireless sensor area network. The test bed results demonstrate also that EEFCR protocol have significantly improved upon the sum goodput in comparison with a number of other radio users, average likelihood of bit error, computing time in comparison with sensor nodes, and latency in comparison to sensing time. The D-SCN model, which Madhu et al. [33] proposed, comprises of the two critical steps of feature selection and feature discrimination. In order to capture feature invariances during the feature extraction phase, they suggested an end-to-end learned capsule network with such an imperative routing (IR) mechanism. Finally, Lorentz, L1 and L2 probabilistic models were suggested for the assimilation of features during the feature discrimination stage.

3 Proposed framework

Due to many pandemics in the last 10 years, such as COVID-19, SARS-CoV-2, and MERS-CoV, improvements in the healthcare sector [34] now demand a high level of importance and concentration from academia and business. The diagnosis of the patient is made using symptoms, some of which may be life-threatening, such as high temperature, lack of oxygen saturation, and abnormal heart rate. If these signs are identified as soon as possible, the patient may recover earlier. In this study, we identified a patient's three primary symptoms as well as any important symptoms. This subject is not new in this sector; there has already been extensive research on it. The critical messages are handled when their time comes, because all the data from the patient's sensors is treated in a FIFO queued manner [35]. Processing the critical message could take some time, and it might take a long time. In order to address this issue, we developed a framework, and when compared to the present frameworks, it provides quicker access to critical messages. Non-critical messages, such as patient health records, are stored in blockchain after processing, providing safeguards to a patient's medical history to prevent tampering.

The proposed method is based on the cloud layer, fog layer and device layers of the IoT ecosystem's three-layered architecture. Data collection and creation are the responsibilities of the device layer. On the body of the patient, sensor nodes generate data, and an Access Point (AP) in our structure collects it and assign priority according QoS. The fog layer is composed of a Fog Broker (FB), a Critical Fog Cluster

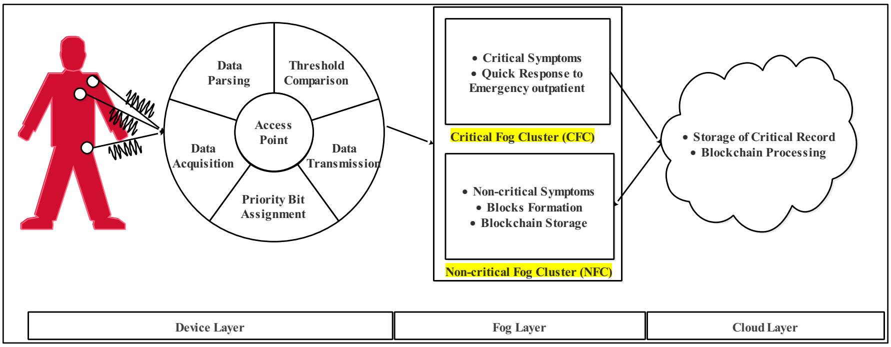

Fig. 1 System architecture

(CFC), and a Non-critical Fog Cluster (NFC). Messages to the CFC or NFC are scheduled by the fog broker according to the priority set by the AP. If the condition of the patient is critical, the CFC receives the notification right away. When non-critical messages are received, FB generates a block that is mined using a cloud service as shown in Fig. 1.

3.1 Device layer

Oxygen saturation, heart rate and temperature were the three sensors that we used with the patient in our framework. Some sensors output data in digital form, while others do in analogue. Analogue temperature has a range of values within a temporal domain. These sensors' values must first be parsed prior processing. Digital oxygen saturation and heart rate sensor data were available, but because they only offer patterns, these are challenging to process. In order to make them meaningful, we parse these using the provided formulas.

3.2 Access point (Arduino)

Data are sent from each sensor to AP (Arduino). GPIO pins are available for Arduino to connect. GPIO can be digital or analogue. Wires connect sensors to the access point. Here, we additionally address the potential synchronizing issue brought on by millisecond-based sensor readings. The NODE MCU conducted segregation and added additional priority bits after receiving these data from the Arduino. For further processing, these data are transferred to Fog in JSON format.

3.3 Fog layer

The FB, CFC, and NFC are the three main elements of the fog layer in this suggested system. At the edge of the fog, FB receives all incoming messages and passes them to either CFC or NFC based on the QoS specifications of each. All incoming messages are held in the FB's memory storage collection until they are forwarded to CFC or NFC. C critical and non-critical messages are considered and handled by this proposed technique. The CFC is informed of the patient's abnormal condition as a life-threatening situation and is then notified to immediately for rescuers. In the case of a normal occurrence, messages will be sent to NFC. The data are compressed into a block and transferred to the cloud for data mining. The emergency response layer, or CFC, where all relevant services are activated, receives the critical data immediately. We also compared the results after taking this queue's forming at the access level into consideration. We provided analysis of this framework using a human-curated methodology and computed the system precision, accuracy, and F-score.

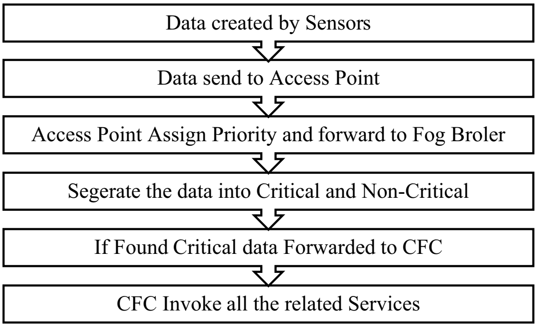
Data created by Sensors
Data send to Access Point
Access Point Assign Priority and forward to Fog Broler
Segerate the data into Critical and Non-Critical
If Found Critical data Forwarded to CFC
CFC Invoke all the related Services

Fig. 2 Flowchart of emergency patients

3.4 Working configuration of the fog layer

The suggested design employs two configurations. In this part, the internal organization of each configuration is examined. The first setting is for critical requests, and the other one is for non-critical messages.

3.4.1 Scenario for patient critical condition

The CFC is responsible for responding instantly to critical signals because a delay could cause significant loss. There might be a slight delay because of some key decisions or transmission issues, but the only thing that matters is that the necessary action is completed as quickly as possible. Assume a patient's heartbeat mechanism is disrupted. It needs to act immediately; otherwise, a catastrophe could happen. When a risk happens, the sensors send a signal to the AP as shown in Fig. 2. The AP intercepts the message from the signal and assigns a priority using predefined criteria and forwards the message to the fog broker. CFC receives the message and takes appropriate action. I might activate an alarm to inform the interested party and the appropriate department.

3.4.2 Scenario for patient normal condition

The non-critical fog cluster uses configuration 2 with an illustration. Due to the processing time of the system, applications that can tolerate delays are the best

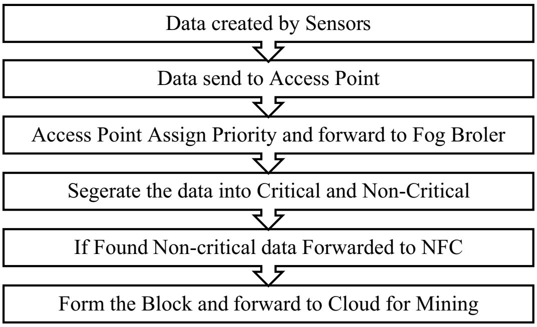
Data created by Sensors
Data send to Access Point
Access Point Assign Priority and forward to Fog Broler
Segerate the data into Critical and Non-Critical
If Found Non-critical data Forwarded to NFC
Form the Block and forward to Cloud for Mining

Fig. 3 Flowchart of delay-tolerant messages

candidates for blockchain. Think about a patient's condition, for instance. The message request is generated by an authorized sensor, and when the parameters are checked, it is sent to the access point. The fog broker places these messages in a non-critical message queue and holds them there until the block length limit has been reached. The block is broadcast to all cluster members, including CH as shown in Fig. 3. This block is forwarded by the NFC cluster to the cloud for blockchain processing via mining services. After determining the nonce value, the cloud server sends the correct nonce back to the cluster head and it is broadcast to all members of the cluster.

4 Simulation setup

The technicalities of implementing the suggested technique and framework into operation are covered in this section. We have discussed the simulation used for this analysis as well as the problems that emerged during the framework's development. We started working with electronics simulators early on in this project, using Packet Tracer, Proteus, and LABView. The previously mentioned package excluded network modules and solely supported the simulation of electronics. Despite having network modules, some networking simulation software was lacking of IoT sensors. To make our system simpler to understand and enhance in the future, we divided it into layers. We took considerable pains to cover every conceivable subsystem.

4.1 Tools used in research

The following resources are employed in the execution of this framework: We downloaded these open-source programs from the internet. The software configuration, if necessary, is covered in the paragraph that follows.

4.1.1 Library and boards

For the same purpose, engineers from all around the world have worked to shape up the libraries. The most of libraries are open access. We have added the following libraries of a certain designer: The following design must be conFig.d in order to view the firmware (Arduino, Node MCU) output [36] on the chronic screen. Set up the board that contains the ESP8266 [37] and Arduino UNO first. We imported the relevant board's libraries as shown in (Table 1).

Table 1 Baud rate of hardware

Board	Baud rate
Serial output [Arduino]	115,000 bps
Serial output [ESP8266-node MCU]	115,000 bps
Serial communication [Arduino]	4820 bps
Serial communication [node MCU]	4820 bps

4.2 Data acquisition

It is obvious that the sensor layer collects the sense data from the patient's body. The sensor nodes have limited resources, so these cannot apply further operations on data. Due to easy availability, for example, sensors are used to get the sensed value and forward it for further processing.

4.2.1 Temperature sensor

We chose the LM35 temperature sensor [38] out of all the options available. The LM35 sensor works on the basic idea of a diode, where the voltage across a diode grows at a known proportion as the temperature increases. By carefully magnifying the voltage change, it is simple to create an analogue signal that is directly related to temperature.

4.2.2 SPO2 and heart rate sensor

Max30102 [39] provides both SPO2 and heart rate, making it a dual-functional device. Its typical value is from 96 to 100%. After stating, it is imperative to follow some parameters for reasons of precision. The sensor is set up using the default configuration. The IR LED kills the mood because the red LED is dim to even consider revealing that the sensor is operating. Small light beams that flow through your finger's blood to measure the level of oxygen are used in pulse oximetry. Pulse oximeters measure variations in optical emission in oxygenated or deoxyhemoglobin blood, according to British Lung Foundation.

4.3 Queueing models for proposed solution

In this section, we provide some key explanations of the models employed in our framework technique.

4.3.1 Model M/M/1 [40]

This queue is a part of an end-to-end IoT connection that represents the smooth message delivery (collection, processing or transmission). It is comparable to the traditional M/M/1 queue in which a single server manages Poisson arrivals across an exponentially spaced service time. One way to describe an M/M/1 queue is as follows:

$$Qm/m/1 = (\lambda, \mu) \tag{1}$$

where the rates at which messages enter the queue is λ, and the rate at which they are handled is μ. Let $D = 1/\ \mu$ be the service requirement for the processing delay of a message (service time). Queuing time plus service time, often known as mean responsiveness, is how long a message remains in an M/M/1 system.

$$\Delta^{m/m/1} = \frac{D}{(1 - \lambda D)} \tag{2}$$

4.3.2 Multiclass model [41]

This queue architecture offers continuous service for messages from different classes, like critical and non-critical messages, in terms of transmission, receipt, or processing.

IoT communication is divided into two classes based on its many qualities. Critical and non-critical messaging represents emergency and delay-tolerant services respectively, demand different transmission and processing resources. The multiclass queue is composed of several M/M/1 queues because each class relates to a common M/M/1 queue with Poisson arrivals and an exponential service rate.

5 Results

5.1 Threshold values of symptoms

Values are compared to and placed against common attributes. The next task, "emergencyAlert()," is conducted in the unlikely event that anything of value is found. At this capacity, all desirable boundaries are exceeded. We recorded the values from clinical sources. The normal and edge values are displayed in Table 2.

5.2 Reading and parsing of sensors values

We have approximately 1200 individuals with varied signs, including temperature, heart rate, and SPO2, available for examination. These characteristics are acquired using sensors and stored in a data base. We evaluate the framework's presentation in the context of gathering attributes and afterward parsing them into a useful outcome for managing. With the assistance of Expert Identification, we assess the effectiveness of our framework and estimate the quantity of correctness, accuracy, reviews, and F-scores that we acquired. If the framework fails to account for a patient's qualities, its performance will be poor and shaky. We demonstrated a delay of 1 S between each stretch, with an adjustment time of about ten milliseconds. We also demonstrate that this always has 3600 s. Therefore, 1200 quality can be obtained

Table 2 Threshold values of symptoms

Vital sign	Normal value	Above range	Below range
Beats per min	Different in different age groups, but an average is 50–150 bpm	> 150	< 50
Temperature	97–100	> 102	< 96
SPO2	95–100	> 100	< 95

Table 3 Reading and parsing of sensors values (confusion matrix)

Reading and parsing of sensors values (confusion matrix)			
Expert identification ↓	IoT hospital		Total
	Acquired values	Not acquired values	
Acquired values	1155 (TP)	45 (FN)	1200
Not acquired values	0 (FP)	0 (TN)	0
Total	1155	45	1200

Table 4 After tune-up—reading sensor values

After tune-up—reading and parsing of sensors values (confusion matrix)			
Expert identification ↓	IoT hospital		Total
	Acquired values	Not acquired values	
Acquired values	1165 (TP)	35 (FN)	1200
Not acquired values	0 (FP)	0 (TN)	0
Total	1165	35	1200

in 20 min. The disarray grid for evaluating the presentation is displayed in Table 5. We concentrated on the four main activities in the setup of our framework for easy understanding of the disarray matrix. An outcome when the model incorrectly predictions the positive class is known as a false positive. Furthermore, a false negative is an outcome where the model forecasts the negative class incorrectly.

To further clarify, we stated that true positive denotes the existence of patient worth in actuality and our framework's acceptance of it, while true negative denotes the absence of patient worth in reality and our framework's failure to provide any worth in the framework. False positive denotes the absence of patient value whereas our framework provides the value to the framework. False negative indicates that patient worth is present in reality but was ignored by our framework. We are now filling the confusion matrix using the rules given in Table 3.

In our framework, there's many problems with precision. These characteristics differ due to the following factors: disengagement of the patient sensor arrangement, actual sensor execution, sequential correspondence, patient improvement, framework hang with other program (hence the requirement of a dedicated server that is not delegated to some other task), and our attempts to tune the framework and note the response once more.

5.3 After tune-up: patient values reading and parsing

Then, using the previously shown similarity, we recalculated the result (Table 4).

It is adjusted and will work better for a specific sensor, but if we apply it to another sensor, we risk ridicule. The evaluations both prior to and after making

Table 5 Average value of reading sensors

Performance actors	A/B	Value%	Average
Accuracy	Before	96.3	96.61%
	After	97	
Precision	Before	100	100%
	After	100	
Recall	Before	96.3	96.7%
	After	97	
F-Score	Before	98.1	98.3%
	After	98.4	

Table 6 Coined the abnormal values

Found out of range values (confusion matrix)			
Expert Identification ↓	IoT hospital		Total
	Out of range value found	Out of range value not found	
Out of range value found	656 (TP)	6 (FN)	662
Out of range value not found	0 (FP)	542 (TN)	541
Total	655	545	1203

Table 7 Blockchain mining

Blockchain mining (confusion matrix)			
Expert Identification ↓	IoT hospital		Total
	Blockchain success	Blockchain not success	
Eqpt found	647 (TP)	7 (FN)	654
Eqpt not found	1 (FP)	0 (TN)	1
Total	648	7	655

adjustments are averaged. The performance actors' average values for the gathering of sensor values are shown in Table 5 and 6.

5.4 Found abnormal values

We compute the display of our approach for finding the peculiar traits using Table 8. Our framework must be changed in order to value the unexpected or miss it. We continue to use the same collection of 1200 quality characteristics that were used in earlier execution evaluation Table 6.

Table 8 Overall system accuracy

IoT hospital	Accuracy	Precision	Recall	F-score
Reading and parsing of sensor values	96.2%	100%	96.7%	98.3%
Found out of range values	99.6%	100%	99.3%	99.7%
Blockchain mining	98.5%	99.8%	98.8%	99.3%
Overall IoT hospital	**97.7%**	**99.5%**	**97.9%**	**98.7%**

5.5 Blockchain mining

In our system, blocks of blockchain are mined from cloud services. It provides a low-cost solution for blockchain implementation (Table 7).

5.6 Overall system accuracy

We now summarize the findings and determine the overall system performance. starting with the first step (Table 8):

IoT Hospital performed over 98% for almost all phases in terms of its overall performance.

5.7 Result comparisons

The results of the suggested solution are compared with [38] in terms of accuracy, precision, recall, and F-Score. Figure 4 compares the receiving and parsing of sensor data for the suggested system and [38], and it is clear that our proposed technique produces better results than the alternative.

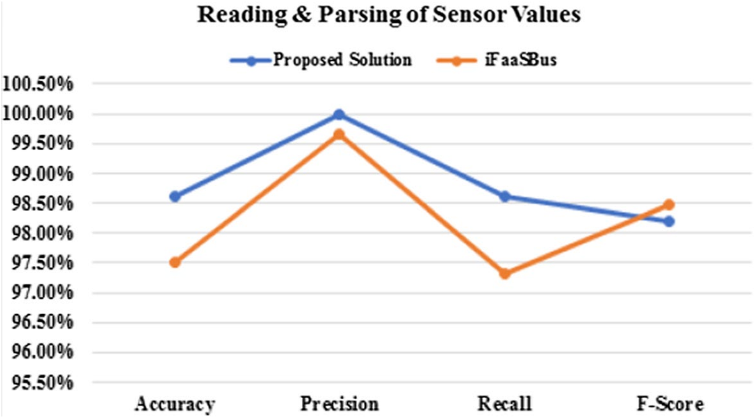

Fig. 4 Reading and parsing of sensor values

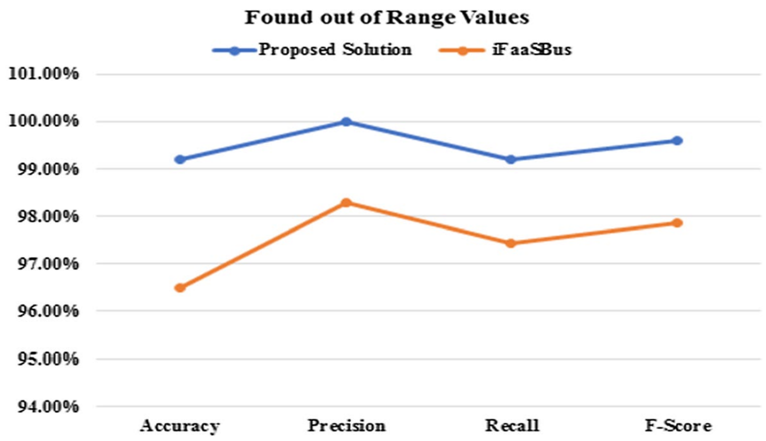

Fig. 5 Found out range of values

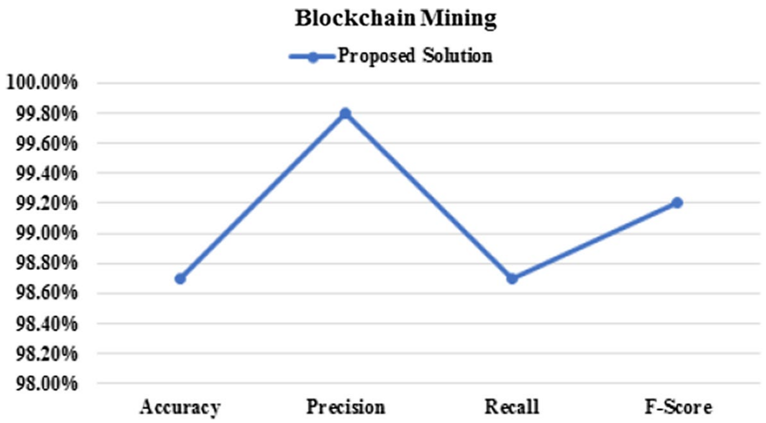

Fig. 6 Blockchain mining

Figure 5 compares the performance of the suggested solution and article [38] across a range of values.

The performance of the proposed solution is observed between 99 and 100%, according to this graph, while the competing methods is between 96 and 98%. Figure 6 depicts the mining efficiency of blockchain, which ranges from 98.60 to 99.80%, but [38] has not incorporated blockchain in his approach.

The total performance of both strategies is compared in Fig. 7.

When the critical message rate is 80% or above, as shown in simulation 4, Fig. 8 system response time clearly reveals that the suggested system is considerably faster than benchmark approach. The system performs noticeably better than benchmark. Packet drop rate and throughput of the system are shown in Figs. 9 and 10, respectively. Figure 11 compares how benchmark and the suggested solution use

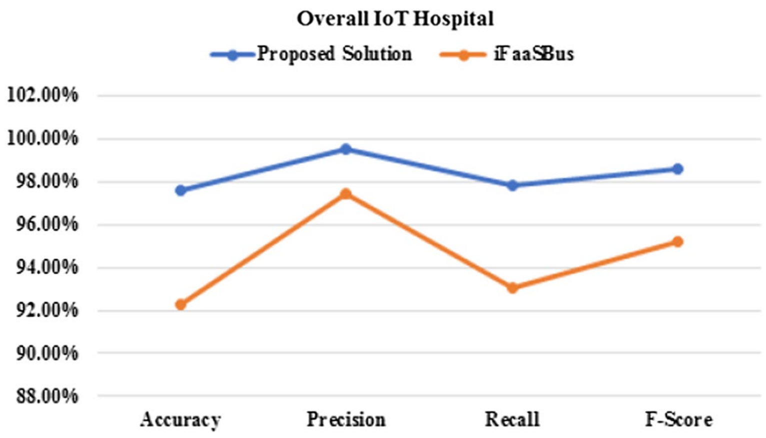

Fig. 7 Overall IoT hospital performance

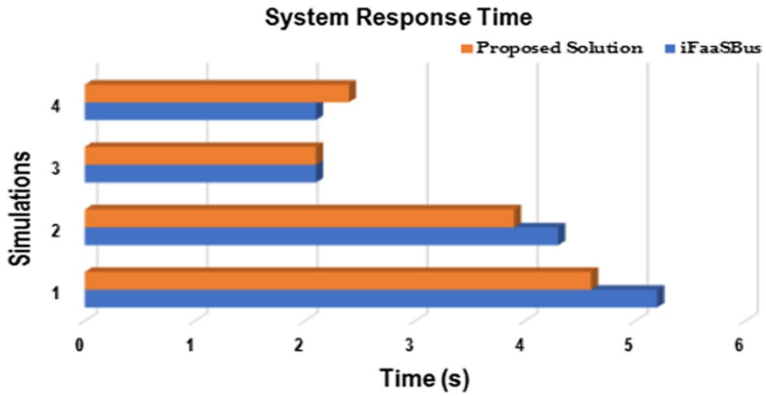

Fig. 8 System response time

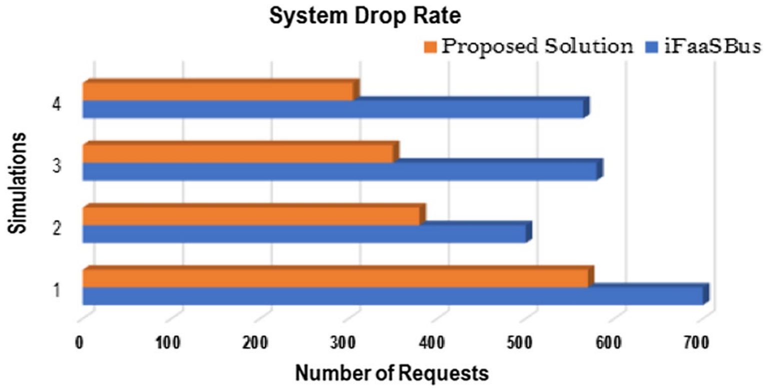

Fig. 9 System drop rate

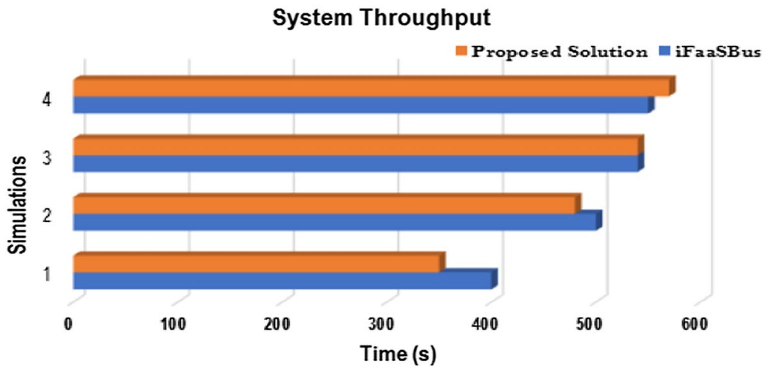

Fig. 10 System throughput

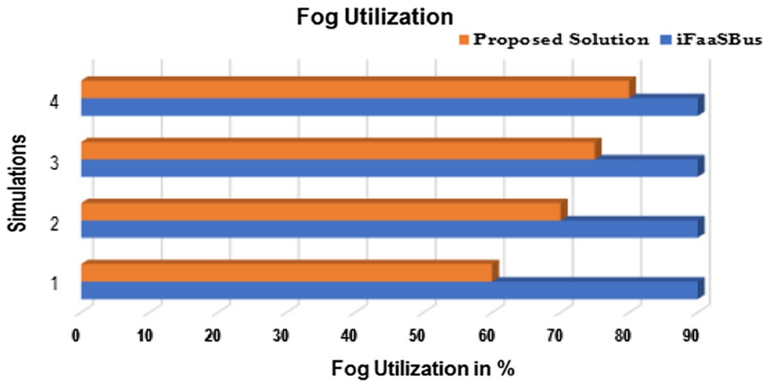

Fig. 11 Fog utilization

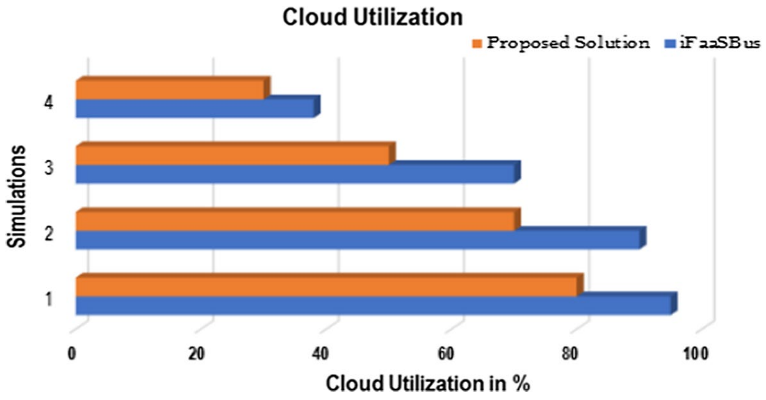

Fig. 12 Cloud utilization

fog. Figure 12 displays cloud usage. Due to the mining operations being obtained from the cloud, the suggested method obtains a little bit extra cloud resources than benchmark.

6 Discussions

All aspects of life are greatly affected by the IoT. Blockchain technology is utilized to make data immutable in order to address the IoT weaknesses of data tampering. IoT devices provide a variety of messages, some of which necessitate immediate action while others can tolerate delay. Splitting data streams and responding appropriately is a difficult task. Clustering at the device layer is challenging due to resource constraints; in addition, cloud deployment may cause delays. At the fog layer, our solution accomplishes message segregation. Authors of similar works [10, 30–40] did not employ blockchain technology, as given in Table 1. The aforementioned issues are intended to be fixed in this solution. Moreover, IFaasBus solution has not used blockchain technology to secure data, and in our solution, we have implement it.

7 Limitations

It should be noted that all received messages through IoT devices follow a Poisson arrival data, which means incoming requests in real systems may fluctuate and follow different patterns. The sources of the content could include businesses, smart phones, sensors, traffic density, etc. The needed service time may not necessarily be exponential for data. However, it is also important to keep in mind that Poisson arrival and exponential service time have been employed in the literature to obtain adequate approximations of real systems. We have got results for a predetermined set pattern. Our solution will perform well when receiving more critical messages compared to non-critical messages. If the system receives more non-critical messages, then response time may increase.

8 Conclusion and future work

Different scholars have proposed various methods to implement blockchain in IoT environment over the last decade in different fields of life, including smart buildings, supply chains, farming, and smart health care. Blockchain incorporation with IoT provide a great research potential. This proposal examines IoT, fog, and blockchain-based implementation in the healthcare industry in depth. The sensors that are affixed to the patient's body produce both critical and non-critical messages. To alert the interested parties to cope with the emergency scenario, important signals are given via the Critical Fog cluster on the fog layer in this system. Non-critical messages are handled through a cloud service but stored in the fog layer. Blockchain processing from cloud service will cause more delay to process blockchain from the cloud. In the case of blockchain processing at the fog layer, it needs a significant amount of additional computing power. In our solution, blockchain processing takes place in the cloud, while storage takes place in the fog layer. Fog storage will cut down on latency, while cloud processing will provide a more affordable option. Second, this approach will permit message scheduling because the demand is distributed over numerous systems. The fog layer is, after all, divided into two halves. For critical communications, the first subsystem will function as a legacy CDC-IoT, and for non-critical messages, the second subsystem will function as a CDC-IoT. This method might be used in the future to exploit both critical and non-critical signals in additional categories. Critical messages are urgent alerts that call for immediate action in a condensed amount of time. Non-critical messages are handled by blockchain and are delay-tolerant. The findings of this study demonstrate that the response time and accuracy outperform previously suggested options.

Acknowledgements The authors acknowledge the referees' insightful feedback. We also like to express our gratitude to Islamia University and the Virtual University of Pakistan for their assistance.

Funding The authors have not received any financial support from any person, institution, or organization for this research work.

Declarations

Conflict of interest This article was submitted without any conflicts of interest, and all of the authors gave their approval.

Ethics approval This article does not contain any studies with human participants or animals performed by any of the authors. Results are gotten through simulation and tested number of times to take final value.

References

1. Akkaoui R, Hei X, Cheng W (2020) Edgemedichain: a hybrid edge blockchain-based framework for health data exchange. IEEE Access 8(1):113467–113486
2. Al-Haija QA, Ishtaiwi A (2022). Multiclass classification of firewall log files using shallow neural network for network security applications. In: Soft computing for security applications, Springer, pp 27–41
3. Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, Teo J, Zakarya M (2022) An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors 22(2):572–593
4. Almaiah MA, Hajjej F, Ali A, Pasha MF, Almomani O (2022) A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT Based CPS. Sensors 22(4):1448–1460
5. Alreshidi EJ (2022) Introducing fog computing (FC) technology to internet of things (IoT) cloud-based anti-theft vehicles solutions. Int J Syst Dyn Appl (IJSDA) 11(3):1–21
6. Amir Latif RM, Hussain K, Jhanjhi NZ, Nayyar A, Rizwan O (2020) A remix IDE: smart contract-based framework for the healthcare sector by using blockchain technology. Multimed Tools Appl 1–24
7. Badr S, Gomaa I, Abd-Elrahman E (2018) Multi-tier blockchain framework for IoT-EHRs systems. Procedia Comput Sci 141(1):159–166

8. Chithaluru P, Stephan T, Kumar M, Nayyar A (2022) An enhanced energy-efficient fuzzy-based cognitive radio scheme for IoT. Neural Comput Appl 4(1):1–23
9. Chondrogiannis E, Andronikou V, Karanastasis E, Litke A, Varvarigou T (2022) Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. Blockchain Res Appl 3(2):100049–100060
10. Crameri KA, Maher L, Van Dam P, Prior S (2022) Personal electronic healthcare records: what influences consumers to engage with their clinical data online? A literature review. Health Inf Manag J 51(1):3–12
11. Das J, Ghosh S, Mukherjee A, Ghosh SK, Buyya R (2022) RESCUE: enabling green healthcare services using integrated IoT-edge-fog-cloud computing environments. Softw Pract Exp
12. Das S, Namasudra S (2022) A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. Comput Electr Eng 101:107991
13. Famá F, Faria JN, Portugal D (2022) An IoT-based interoperable architecture for wireless biomonitoring of patients with sensor patches. Internet Things 19:100547
14. Ganesh B, Rajakumar T, Malathi M, Manikandan N, Nagaraj J, Santhakumar A, Elangovan A, Malik YS (2021) Epidemiology and pathobiology of SARS-CoV-2 (COVID-19) in comparison with SARS, MERS: An updated overview of current knowledge and future perspectives. Clin Epidemiol Glob Health 10:100694
15. Goel AK, Bakshi R, Agrawal KK (2022) Web 3.0 and decentralized applications. Mater Proc 10(1):8
16. Golec M, Ozturac R, Pooranian Z, Gill SS, Buyya R (2021) iFaaSBus: a security and privacy based lightweight framework for serverless computing using IoT and machine learning. IEEE Trans Ind Inform
17. Hannah S, Deepa AJ, Chooralil VS, BrillySangeetha S, Yuvaraj N, Arshath Raja R, Suresh C, Vignesh R, Srihari K, Alene A (2022) Blockchain-based deep learning to process IoT data acquisition in cognitive data. BioMed Res Int
18. Krishnamoorthy S, Dua A, Gupta, S (2021) Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: A survey, current challenges and future directions. J Ambient Intell Humaniz Comput 1–47
19. Latif A, Arfianto AZ, Poetro JE, Phong TN, Helmy ET (2021) Temperature monitoring system for baby incubator based on visual basic. J Robot Control (JRC) 2(1):47–50
20. Lepore D, Dolui K, Tomashchuk O, Shim H, Puri C, Li Y, Chen N, Spigarelli F (2022) Interdisciplinary research unlocking innovative solutions in healthcare. Technovation 102511–102541.
21. Madhu G, Govardhan A, Ravi V, Kautish S, Srinivas BS, Chaudhary T, Kumar M (2022) DSCN-net: a deep Siamese capsule neural network model for automatic diagnosis of malaria parasites detection. Multimed Tools Appl 12(1):1–23
22. Massey WA, Ekwedike E, Hampshire RC, Pender JJ (2022) A transient symmetry analysis for the M/M/1/k queue. Queueing Syst 1–43
23. Mnif E, Mouakhar K, Jarboui A (2021) Blockchain technology awareness on social media: Insights from twitter analytics. J High Technol Manag Res 32(2):100416–100433
24. Pagano P, Antonelli S, Tardo A (2022) C-ports: a proposal for a comprehensive standardization and implementation plan of digital services offered by the "Port of the Future." Comput Ind 134(1):103556–103576
25. Pitt J (2022) The digital transformation and modern indentured servitude. IEEE Technol Soc Mag 41(2):6–9
26. Rahmadika S, Astillo PV, Choudhary G, Duguma DG, Sharma V, You I (2022) Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices. IEEE J Biomed Health Inform
27. Rajguru K, Tarpe P, Aswar V, Bawane K, Sorte S, Agrawal R (2022) Design and implementation of iot based sleep monitoring system for insomniac people. In: 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), pp 1215–1221
28. Rani S, Kataria A, Chauhan M, Rattan P, Kumar R, Sivaraman AK (2022) Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: state-of-art work. Mater Today Proc
29. Ray PP, Chowhan B, Kumar N, Almogren A (2021) Biothr: electronic health record servicing scheme in IoT-blockchain ecosystem. IEEE Internet Things J 8(13):10857–10872
30. Roy SK, Devaraj R, Sarkar A (2022) SAFLA: scheduling multiple real-time periodic task graphs on heterogeneous systems. IEEE Trans Comput

31. Safari S, Ansari M, Khdr H, Gohari-Nazari P, Yari-Karin S, Yeganeh-Khaksar A, Hessabi S, Ejlali A, Henkel J (2022) A survey of fault-tolerance techniques for embedded systems from the perspective of power, energy, and thermal issues. IEEE Access 10:12229–12251
32. Shen B, Guo J, Yang Y (2019) MedChain: efficient healthcare data sharing via blockchain. Appl Sci 9(6):1207
33. Silva CA, Aquino GS, Melo SRM, Egídio DJB (2019) A fog computing-based architecture for medical records management. Wirel Commun Mob Comput
34. Silva FA, Nguyen TA, Fé I, Brito C, Min D, Lee JW (2021) Performance evaluation of an internet of healthcare things for medical monitoring using M/M/c/K queuing models. IEEE Access 9:55271–55283
35. Singh K, Bura D (2021) Internet-of-Things (IoT): distinct algorithms for sensor connectivity with comparative study between node MCU and arduino UNO. NVEO-Nat Volatiles Essent Oils J NVEO 4313–4324
36. Sutikno T, Purnama HS, Pamungkas A, Fadlil A, Alsofyani IM, Jopri MH (2021) Internet of things-based photovoltaics parameter monitoring system using NodeMCU ESP8266. Int J Electr Comput Eng 11(6):2088–8708
37. Tripathi G, Ahad MA, Paiva S (2020) S2HS-A blockchain based approach for smart healthcare system. Healthcare 8(1):100391
38. Tuli S, Mahmud R, Tuli S, Buyya R (2019) Fogbus: a blockchain-based lightweight framework for edge and fog computing. J Syst Soft 154(1):22–36
39. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJPC (2018) BHEEM: a blockchain-based framework for securing electronic health records. In: 2018 IEEE Globecom Workshops (GC Wkshps)1–6
40. Zhang C, Chen Y (2020) A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics. J Ind Integr Manag 5(01):165–180
41. Zhang Z, Zeng Y, Liu H, Zhao C, Wang F, Chen Y (2022) Smart DC: an AI and digital twin-based energy-saving solution for data centers. In: NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symposium, 1–6

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.