Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

Softwarization of the Infrastructure of Internet of Things for Secure and Smart Healthcare

Mayur Mistry[0000-0001-9419-8369], Riya Pandey, Akshit Kalita

Computer Science Dept, Ganpat University, India

Corresponding author email:mayur.mtechbda1703@ict.gnu.ac.in

Abstract- Smart Healthcare is a very important application in the field of Internet of Things. It is going to revolutionize the Healthcare sector and help the Healthcare providers in decreasing their expenditure along with utilizing new technologies. The crucial step in this process is the acquisition, aggregation and the analysis of the data obtained through the various sensors present in the various devices which produce huge amounts of varied data which include text, audio, and video. Since the growth in technologies, various new kinds of sensors have been made to measure different types of data for the healthcare sector. Generation of these large amounts of data will necessitate some type of processing to take place which can stand in the way as a big challenge along with the security concerns for the data. Thus, to address these challenges, a scalable, cost-effective, stable, and secure implementation is suggested in this chapter using an infrastructure which has been Softwarized that includes cloud and fog computing, Blockchain and Tor. The suggested system is a machine-to-machine messaging, rule-based beacon for seamless data management, and uses two types of data processing techniques, to facilitate smart-healthcare applications, which are explained further. Along with the proposed system various other terminologies like fog computing, Blockchain and Tor are explained which will make the idea of the system clearer.

Keywords:Cloud Computing, Smart Healthcare, Fog Computing, Internet of Things, Blockchain, Tor

I. Introduction

With the growing technologies in the field of smart healthcare, it is very essential to introduce a system which will enhance the quality and efficiency of the equipment that provide the health analysis and perform various other tasks like alarming the doctors in case of an emergency, tracking the patients' health and reports regularly along with reducing the amount of latency and risks of privacy of the systems. Usage of real time data has increased in the field of smart healthcare and thus calls for real time analysis. Various IoT devices and sensors can be used for the purpose of collecting the data relating to the patient. The collected data must be transmitted to the devices which will perform the analysis on the data to produce the results.This task can be taken care of by Wi-Fi, Zigbee, a wired connection or Mobile networks like 3G/4G/LTE [1-5]. The next step is the analysis of data which can be done on the cloud, but this process introduces latency, thus fog computing can be used to help reduce that. Furthermore, various methods [1]can also be used for providing anonymity of the user and security of the healthcare information that can otherwise be misused. [2]

[1]The corresponding author Mayur Mistry is with Computer Science dept, Ganpat University, Riya Pandey and Akshit Kalita is with SIT, India.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

Some methods for protection of the data explained in the chapter are Blockchain and Tor. The system proposed aims to softwarize the infrastructure of Internet of Things for Smart

Healthcare which will help meet all the requirements discussed so far with the highest level of efficiency[6-8].

II. System's Architecture

The architecture of the system includes smart sensors of different types and sizes that track and monitor raw sensor data as well as patients' health-related metrics[9-10]. The sensors' transceivers use a wireless interface to communicate with the base stations and the most powerful base station acts as the data aggregator. The IOT gateways operate with a variety of devices and network protocols, allowing for widespread communication.

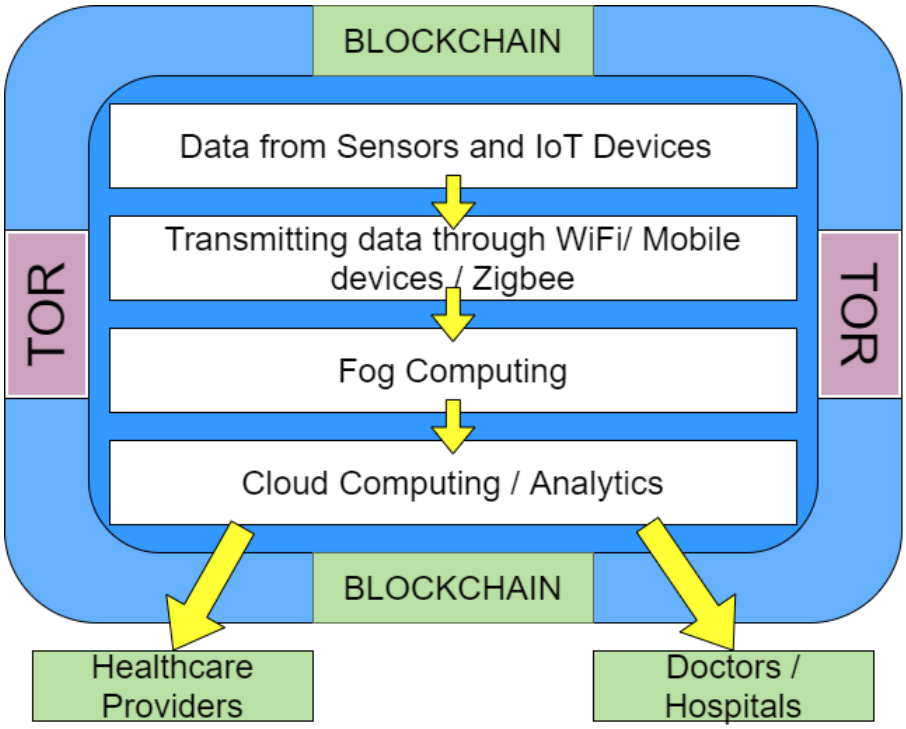

Figure 1: System Architecture

Now let us discuss the system architecture in detail along with all the aspects involved in it which are:1) Data sensors 2) Data Transmission3) Fog Computing4) Cloud computing5) Security and privacy (Blockchain, Tor)

A. Sensors and IoT Devices

Softwarization of sensor networks will allow them to be dynamically configurable which is not possible in the usual sensors which are mostly application specific[11-23]. Software-defined networking (SDN) will also be more economical along with improving the sensor networks' agility and flexibility and allows management of data-forwarding rules. This will also allow the user to easilymake commercially available off-the-shelf hardware SDN compliant and improve interoperability among communication protocols thus

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

also lowering the cost of network deployment and configuration. All the sensors that can be utilized for various activities in the domain of Health Sciences like diagnosis, treatment or monitoring are called medical sensors[24-35]. Based on the risk potential all the devices in the Healthcare sector are divided into 4 categories, Class 1 being the devices with lowest potential risk and Class 4 with highest potential risk. Sensors in the medical domain need to follow some standards and specifications which are discussed below:

- IEC 60601-1 provides standards of safety to be followed by the medical equipment.
- They must satisfy the legal specifications that include various quality management standards, management of risk. The sensor must also ensure that it is effective in producing accurate response to the provided input. Safety during the operation of the device must also be considered.
- It should provide a measurement that is very stable and quick along with fast response time.
- Measurement of the sensors should be highly precise and accurate
- They should give outputs as digital so that it can be directly connected to the microcontrollers/microprocessors.

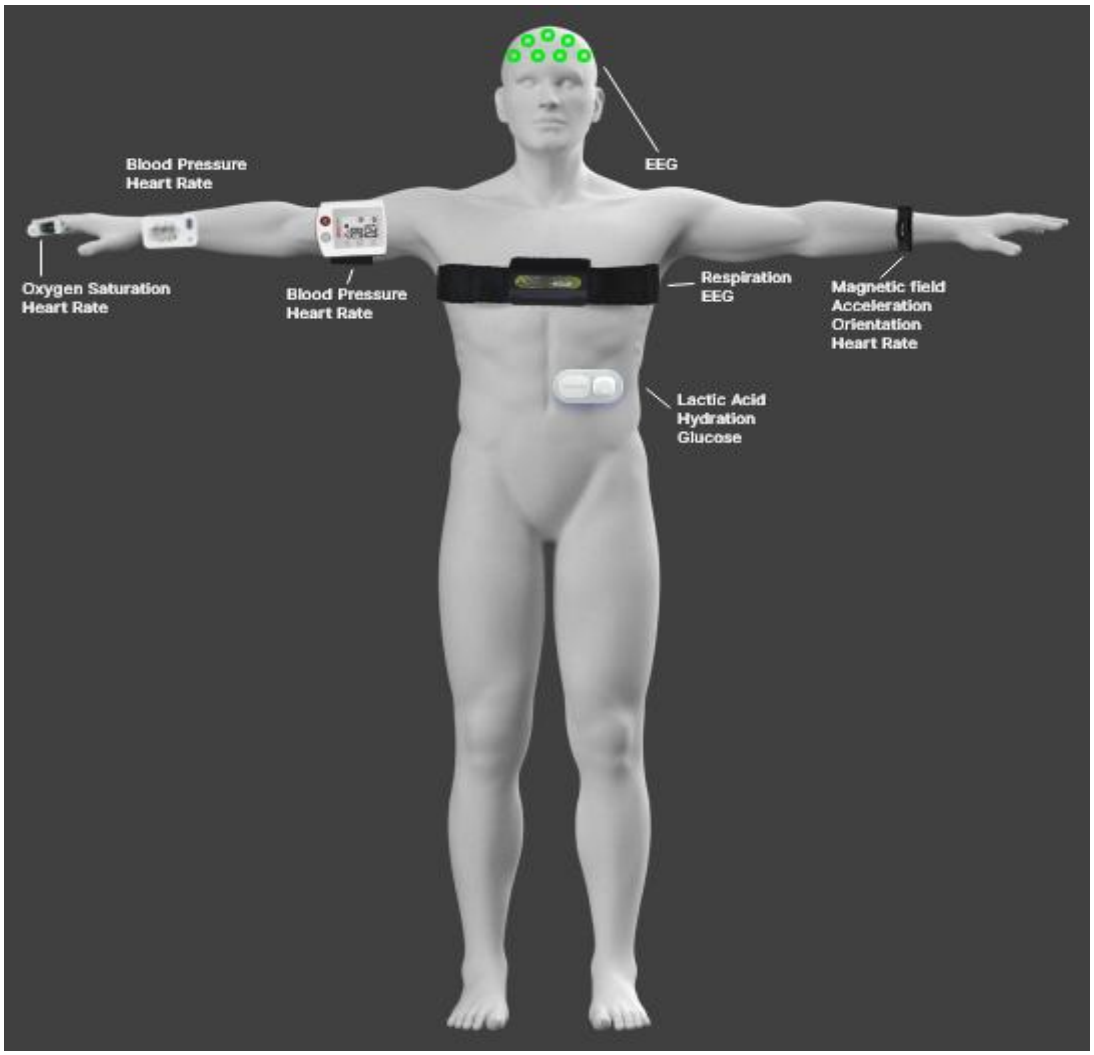

Figure 2: Medical Sensor

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

There are many types of medical sensors that perform different kinds of functions and measurements. Here, let us discuss some of the sensors which we can use in our system for getting the data along with their applications[36-43].

- Temperature sensors (Thermometers): These are very commonly used sensors for the measurement of body temperature.
- Airflow sensors: These are used to measure the flow of air or oxygen and thus these can be used in anesthesia machines, heart pumps etc.
- Pressure sensors: These are used in medical diagnosis or for monitoring the blood pressure and in infusion pumps. These sensors are mostly integrated with embedded systems.
- Implantable pacemaker: This is an embedded sensor system which is used to maintain the rhythm of the heart in real time. It delivers a synchronized rhythmic electric stimulus to the heart muscle to perform its task.
- Oximeter: This sensor measures the ratio of hemoglobin that is saturated by oxygen to the total amount of hemoglobin in the person's blood.
- Glucometer: It measures the concentration of glucose in blood.
- Magnetometer: This sensor examines the magnetic field of the earth around the person and thus tells which direction he is standing in.
- Electrocardiogram sensor (ECG sensor) : This sensor measures the heart's electrical activity.
- Heart rate sensor: It keeps a count of heart contractions occurring in a minute.
- EEG sensor (electro encephalo gram): This sensor is used for measuring the electrical activity of the brain.
- Respiration rate sensing device: It measure the number of times a person's chest rises per minute.

So, the sensors discussed are some of the sensors that are used for the live analysis of the patient's health by the system proposed.

B. Data Transmission

Now that we have the data from the sensors, it is going to be analyzed on the cloud after which the analyzed data will be sent to the healthcare doctors or nurses [44-49]. For these processes data needs to be transmitted in some way. So, the following are some ways which are used for data transmission:

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

1) **Ethernet**

The sensing device is integrated with a processor which analyzes the data which is then uploaded to the cloud. In this way of data transmission wired Internet is required through which the Ethernet connection is attached. But there are a few problems with this method:

- Wired Internet is not present at all places.
- There is no radio link involved in this type of data transmission.

2) **Cellular Technology**

Cellular technologies have very high scalability and reliability and are thus preferable. The Cellular Internet of Things is popularly known as CIOT uses the already existing infrastructure and provides very good coverage. The hardware of CIOT has SIM cards and can thus connect to networks via 2G, 3G, or LTE connectivity[50-62]. Benefits of the Cellular technologies are:

Coverage: Nowadays Cellular technologies have very high coverage and can also reach to rural areas and underground spaces.

Security: The data while the transmission is kept secure as cellular technologies provide End-to-end security by the SIM credentials.

Bandwidth: Cellular technologies like 4G LTE have great bandwidths and a very high speed as fast as 1 Gbps. With the new 5G technology speeds are expected to go up to 10Gbps

3) **ZigBee Data Transmission**

Zigbee devices uses mesh networks of devices to transmit data over larger distances through these device network. Zigbee data packets have two types of transmission namely Unicast and broadcast transmissions. Unicast transmits the data from the source device to one target device. Whereas in broadcast transmissions the data packets are sent to all the devices in the network.

Broadcast transmissions

For all the nodes to receive the data, all the routers receiving the data packets retransmits the packet three times and each time an entry is created in the local broadcast table to make sure that the packets do not keep on getting transmitted for an endless time. The Zigbee stack holds buffer space for every transmission as the packet can be retransmitted by the next node[63-77]. This process takes up a lot of network and causes network congestion. As all the devices in the device network transmits the data packets 3 times, broadcast transmissions are used only in few scenarios to avoid the network traffic.

Unicast transmissions

In this type of transmission, the data is sent from one device to another device directly. If the target device is a neighbour of the source device, then the data is directly sent. But if the destination device is not a neighbour of the source, then the data needs to be sent along a multiple hop path that requires some means to establish the route between the source and target.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

C. Fog Computing

The cloud causes a very high level of latency which cannot be tolerated in healthcare applications. Therefore, Fog computing is sometimes used which decreases the distance between the cloud and the users and brings them closer, thus reducing latency. Fog nodes in our proposed system have lesser resources than the cloud nodes and are smaller than them. But the fog nodes are much more efficient and powerful as compared to IoT devices and gateways. Thus, as the latency is decreased and the performance is improved, the system becomes more efficient and starts to analyze and bundle localized data efficiently while reducing avoidable traffic to the cloud. Fog computing allows short-term analytics at edge devices where data is generated and collected, thereby complementing cloud computing which performs long-term, resource-intensive analytics. Edge devices alone do not have the resources required to perform machine learning and advanced analytics tasks [70-78]. Cloud computing possesses this power but the distance between the data generation and the cloud prevents processing and responding to the data on time. Additionally, connecting all the endpoints to the cloud and sending raw data over the internet can result in negative security, privacy and legal consequences, especially with respect to sensitive data [79-91]. Smart grids, vehicle networks, smart buildings, smart cities and software-defined networks are popular.

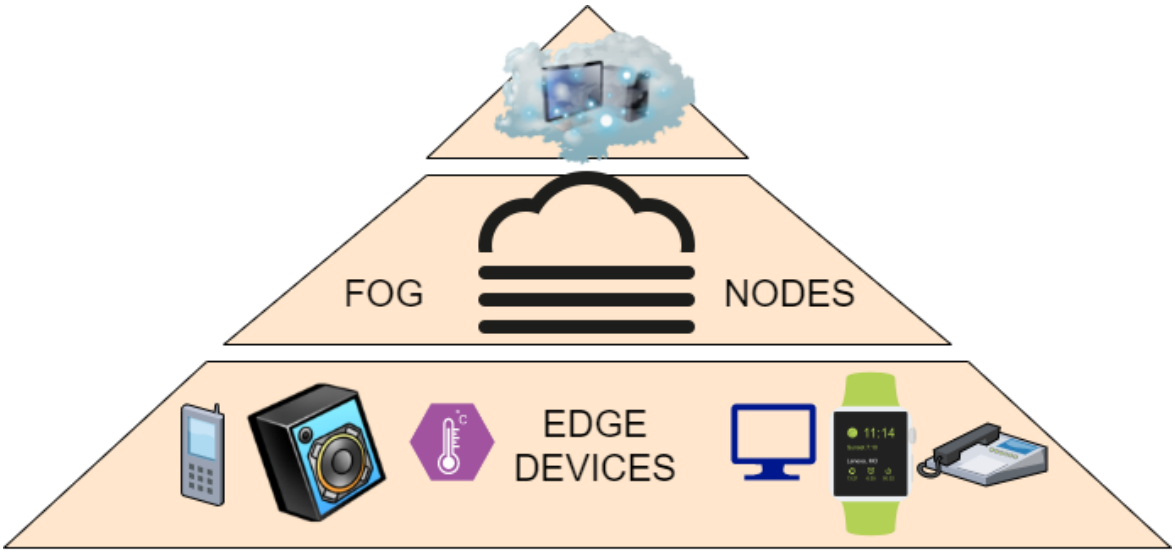

Figure 3: Applications of Fog Computing

Benefits of Fog computing

Fog computing has various benefits and thus we have used it in our proposed system also as it reduces latency and is thus very ideal to use for real time applications. Following are some of its' advantages:

- **Bandwidth conservation:** Bandwidth consumption and related costs are reduced since Fog Computing leads to a reduced volume of data being sent to the cloud [92-94].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

- **Improvement in response time:** since preliminary data processing takes place near the source of the data, there is a reduction in latency and an improvement in overall responsiveness. The aim is to achieve almost real time responsiveness [95-97].
- **Network independent:** The network that is used for Fog Computing can either be wired or wireless and thus it is not network dependent [98-99].

Drawbacks of Fog Computing

Fog computing has some disadvantages too, some of which are stated below:

- **Location Restriction:** Since it is restricted to a physical location, Fog Computing does not provide the anytime/ anywhere flexibility associated with Cloud Computing.
- **Security risks:** Fog Computing is susceptible to IP Spoofing and Man in the middle attacks.
- **Expensive:** Since this technology requires both cloud and edge resources, the hardware costs can prove to be expensive.
- **Ambiguity:** Despite having existed for years, this technology is ambiguous as its definition differs from vendor to vendor.

Fog Computing Workflow based on time sensitivity of Data

Category	Nearest Fog Nodes to IOT Devices	Aggregating Fog Nodes	Cloud
Time taken to Respond[101-102]	Milliseconds	Seconds or a few minutes	Minutes, days or even weeks
Examples of Application[103-110]	M2M communication Haptics, including telemedicine and training	Visualization Simple Analytics	Analysis of Big data Displaying dashboards graphically
Duration of IOT Data[106-109] storage	Momentary	Hours, days or a few weeks	Months or years
Area Coverage	Maximum one city block	Comparatively more	Worldwide

Table 1: Fog computing workflow

The data that is most sensitive to time is analysed on the node nearest to the source. For example, verifying protection and control loops is most time sensitive in a Smart Grid Distribution network. Thus, the closest fog nodes to the grid sensor are able to detect dysfunctionalities and avoid them by transmitting instructions to the actuators. Data which does notrequire real time analysis and can wait a few minutes is transmitted to a node which performs aggregation for analysis. Less time sensitive data is transmitted for analysis and storage to the cloud [110-121].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

D. Cloud Computing

Cloud Computing is the delivery of different IT resources such as data storage, computing power, servers, databases, networks and other services through the internet. By opting to keep files on a cloud-based storage rather than a local storage device, the user has remote access to the data as long as he has an electronic device which has access to the web. Few types of Cloud Computing are - 1. Software as a Service (SaaS) 2. Infrastructure as a service (IaaS) 3. Platform as a Service (PaaS) 4. Functions as a Service (FaaS)5. Integration Platform as a service (IPaaS) definition 6. Private Cloud Definition 7.Hybrid Cloud Definition [122-127].

Cloud Computing Benefits and Drawbacks:

Some advantages of Cloud Computing are -

Agility - Cloud Computing makes deploying technological services possible in a matter of minutes given the broad range of technologies it gives you access to. It gives the user the freedom to test and experiment with new ideas to transform their business.

Elasticity - Cloud Computing allows you to provision only those resources which you need and avoids over-provisioning of resources. These provisions can be scaled up or down depending on the user's requirements.

Saving Costs - Since the user only accesses the resources he/she requires, the cost of unnecessary resources are eliminated, thereby reducing overall costs.

Some Drawbacks of Cloud Computing are -

Data confidentiality risks - Without cloud protection, users' data is susceptible to access by individuals with malicious intent.

Connection dependent - Cloud Computing mandatorily requires a stable internet connection to function. In places with spotty or irregular connection, the access to cloud resources is essentially cut off and the services are rendered unusable.

Reliance on Technical Support- If users encounter problems using Cloud services, they have no choice but to contact customer support who may not be available 24/7. Users do not have the freedom to troubleshoot all problems themselves as they would in their local machines.

E. Security & Privacy

The ability to protect sensitive data and information about personally identifiable health care information is called Privacy. The primary areas of focus with respect to privacy are establishing authorization requirements and formulating policies ensuring that patient's personal details are gathered, exchanged and employed in the correct ways. On the other hand, Security deals with the protection of data from malicious attacks and theft [128-133]. A few methods that fall under the umbrella of Privacy and Security are as follows –

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

i. Tor

Tor is an open-source software which enables users to anonymously communicate by bouncing internet users' and websites' traffic through more than seven thousand relays operated by volunteers globally, making identifying and locating the source of the information extremely difficult. This counters network surveillance threats. Tor can be utilized between the cloud and the fog nodes since it introduces unpredictability and communication delays. The trade-off is the increase in latency which can pose problems for applications that require real time analysis [2][134].

Tor provides data encryption and transmits data via a virtual circuit consisting of several Tor Relays which are randomly selected. Each relay decrypts an encryption layer, revealing the next relay the data has to be passed on to. This method is known as 'Onion Routing'. The innermost layer contains the main data and the address it has to be sent to which the final relay decrypts. This method prevents any single point of communication being susceptible to network surveillance since surveillances relies upon having the knowledge of the source and destination. One must keep in mind, however, that Tor does not wipe out tracks completely but merely reduces the chances of data and actions being traced back to the operator [135].

ii. Blockchain Technology

Blockchain technology secures the records of the patients as it tracks and maintains authorization to all the records and confidential information. A Blockchain is a system that makes it impossible to hack or cheat the system as it stores all transactions together in groups, it is available to participants who have access or authentications to the system. As all the participants can see all the transactions, it makes it impossible to manipulate or change the transactions without being noticed.Blockchain technology validates all the blocks and ensure that each transaction happening is legit and true. The data produced by blockchain has very high security as it is based on the principles of cryptography, decentralization, and consensus. Each block of the blockchain can contain one or more than one transaction [135-137].

The three main principles of Blockchain are:

1. **Cryptography:** This is a method to secure the data by converting it into a form that can only be understood by the sender and the receiver like encryption which is discussed further in the chapter.

2. **Decentralization:** Blockchain has participants from a distribute network which enables decentralization. A single point of failure cannot be found in this kind of a network. A single user does not have the right to change the record of transactions.

3. **Consensus:** This is a decision-making process which takes place between a group. In Blockchain, this mechanism is used to make all the participants come to a single conclusion for making the decisions regarding approval of a transaction or any other required decision.

However, different blockchain networks can have different security aspects defining who participates in the network and who cannot access the data. Networks are categorised as two types depending on this labelled as either private or public,describing who can participate in the network, if the network requires specific permissions or not to add new participants and how new participants can enter the network.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

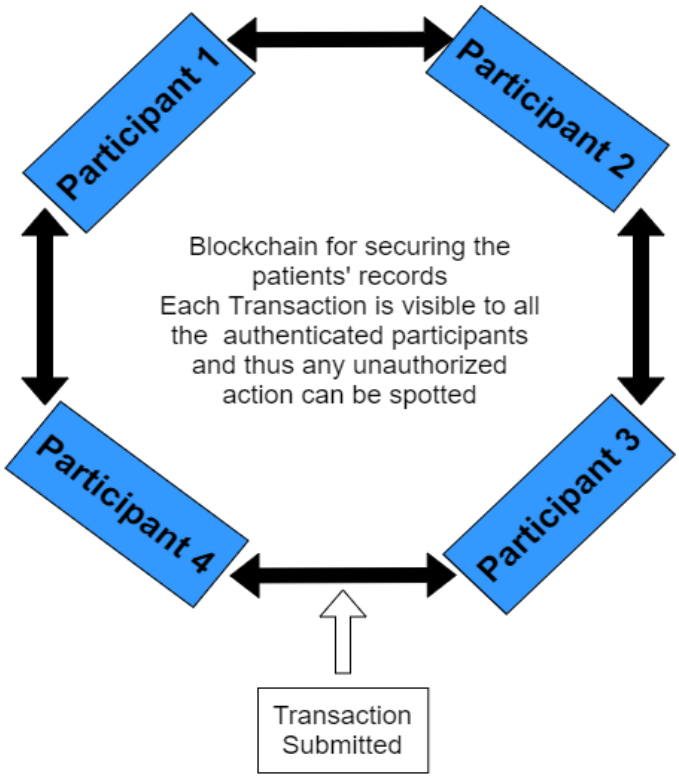

Figure 4: Blockchain Healthcare Technology

Public blockchains

In Public blockchain networks anyone can join and become a participant and be anonymous as well. To achieve consensus and validate transactions in public blockchain computers with internet connections are used.Bitcoin is the most prevalent example of a public blockchain and consensus in bitcoin is achieved through bitcoin mining. In the bitcoin network, the computers, also known as the miners, perform tasks to solve the cryptographic problem and then validates the transactions.

Private blockchains

In Private blockchains participants have to disclose their identity which is then used to validate the individual and only then can he become the participant. This type of network typically allows only known organizations to become participants. This network achieves consensus through a process called selective endorsement. In this process only the known users verify the transactions. Members who have special permissions and access can maintain the transaction ledger. This network type is more secure and has greater access controls.According to one's business goals, the type of network is decided. Private blockchains are mostly used when tight control and regulations are required. Whereas Public networks are used when high level of decentralization needs to be achieved.While establishing a private network, a secure infrastructure and good technology choices are very important because lack of these can lead to security risks.

Understanding blockchain network risks and managing them is very crucial for the Blockchain Technology. Thus, a blockchain security model is implemented which is just a plan to implement security

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

to the network. For developing the security model, administrators create another model which contain all types of risks like business, technology, process, and governance risks. This is known as a risk model. Next, they make a threat model which contains all the threats to the network. And finally, they specify the security controls that should reduce the threats and risks, which were stated in the models.

iii. Data Encryption

Data Encryption is the process of using an algorithm to convert data into ciphertext which is undecipherable by the everyday user. This is a popular method that adds an added level of security incase an attacker were to gain access to data. In order to decrypt the data and view it in its original form, a decryption key is required which is basically a number. Cryptography can be symmetric or asymmetric in nature. Symmetric-key algorithms use the same key for encrypting or decrypting a file. This method is much faster than its asymmetric counterpart but requires the sender to exchange the key with the receiver once the data has been delivered. Asymmetric cryptography uses a public key to encrypt files and a private key to decrypt them. As the names suggest, the public key may be accessible to everyone whereas the private key must be protected.

One of the most popular public key cryptosystems is the Rivest Sharmir-Adleman (RSA) algorithm. The user using the RSA approach generates and releases a public key which is done on the basis of two large, protected prime numbers as well as an additional value. Anyone can encrypt these messages using the public key but they can only be decrypted using the aforementioned prime numbers. No approaches to defeat this system have been published if the key is big enough in size. Since it is a slow algorithm, data is not directly encrypted with it, rather it is used to send the keys for symmetric cryptography which can later be utilized for encryption-decryption in bulk.

One method of decrypting an encrypted file is to use the brute force method of trying all possible combinations of keys until one works. This method usually requires the attacker to have huge access to huge amounts of computational power and is therefore very inefficient. The length of the key determines the possible number of keys and hence a lengthy key may render the success of this kind of attack implausible. Most encryption software use asymmetric algorithms to exchange these secret keys after using a symmetric algorithm to encrypt the data.

II. Data Aggregation

For analytics, applications, and services, users must collect and process data from the IoT sensor network in the field of medicine and healthcare. For example, considering an application like a health monitoring system for a person. The sensor network can be large, and it contains various sensors including sensors for body temperature, pulse rate, room temperature, and humidity. This application requires data to be logged into the system in real time to the cloud so that analysis can take place and quick alerts can be generated if health problems are detected. Thus, the monitoring system requires collaboration among all the sensors.

Processing of Data

Two main approaches of data processing are:

1. **Data fusion:** The final decision, for example indicating the health parameters of a patient, is made by a gateway of sensor-network or a base station that acquires data from each sensor, analyses it and then

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

makes the decision. This base station then forwards its decision to the IoT gateway for reporting or taking necessary actions.

2. **Decision fusion:** Smart sensors are used in this kind of approach. The sensors locally process their data and make decisions about the health of the patient. The individual sensors then pass on its decision to the sensor's gateway which is further connected to the IoT gateway. The Internet of Things gateway receives the individual decisions, aggregates them, then makes a final decision about the patient.

Advantages and disadvantages of the two approaches of data processing:

1. The first approach that is data fusion gives out high volume of raw data and thus takes up higher power and bandwidth.

2. The second approach that is Decision fusion is usually less accurate as the sensors locally process the data which may not show very accurate processing capabilities whereas in Data fusion, the computations are executed on the sensor network gateways that have higher power capability by the system.

Agile IoT Platform

A platform which uses a gate array that can be programmed along with hardware and software parts which allow personalized patient care by transmitting location and other services with the help of M2M communication is proposed. Advantages of the platform:

- Very flexible. It can work with various types of hardware, thus almost all types of actuators or sensors can be used. This is a very useful attribute as it helps the user configure the system as per their requirement and provides access to remote control services.
- Enables seamless data aggregation and analytics. It also lets the user control the application as well as the devices.
- Reduced Latency and improved data collection and aggregation because of the use of M2M communication and FPGA hardware.
- Reduced cost of providing softwarized IoT for smart healthcare. The platform also offers efficient management and no loss of accuracy.

III. Challenges

A. IoT Softwarization:

For providing ultra-low latency and for allowing the users to communicate with the system via their mobile devices, Softwarized IoT devices would need to seamlessly integrate with 5G wireless technology. On comparing the current technologies with 5G systems, a lot of challenges come up including an absence of a standard 5G definition.

Some other issues that Softwarization technologies must address, include:

1. Managing transmission control, bandwidth, and other resources.

2. Connecting network computers, transceivers, and physical elements in the most efficient way possible.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

3. The key indicators for assessing the efficiency of softwarized components and applications must be established.

4. To guarantee the scalability, designing and managing distributed controllers and network functions.

5. Organizing network functions and resources autonomously through the softwarized middleware

B. Privacy & Security:

Since any blockchain member can see all transactions, it is critical to use established communication protocols with the IoT devices. Homomorphic encryption or zero knowledge proofs can also be used for the security purpose depending on the technical capabilities of the devices.Blocked Transactions that usually occurs because of an absence of agreement among blockchain members to have a requested transaction can be minimized using proper logical blockchain implementations based on enforceable smart contracts. Further including legalities in the smart contracts can enforce various required laws or regulations and control misconduct which necessitates procedures that produce a hash of the smart contract's legal component ensuring its confidentiality.

IV. Conclusion

Applications in the sector of Smart Healthcare are enormous, and it will help the mankind with a lot of applications in the field of healthcare some of which include real time patient monitoring, medical-device actuation, improving healthcare quality using data analytics, improving patient experience and lower the cost. The system proposed in the chapter offers an economical, secure, private, and flexible solution. In the future, a new FPGA platform for high efficiency, reduced latency, and the local implementation of user defined flow rules can be proposed. In addition, an M2M transmitter-receiver and microcontroller can be envisioned for data integration and agile deployment of smart healthcare applications and services. Through this system we learnt all about the medical sensors, their important features, their types, devices which can be used for data transmission, fog computing, how it works and its types, cloud computing, its types and various challenges and advantages of the same. As we move to the era where data is becoming enormous and is increasing at a very high rate, the privacy concerns come into picture which were discussed in the chapter and some ways which can be used to overcome those concerns. Next, we saw data aggregation and various types of methods for data processing. Lastly, we defined some of the challenges present in the field of IoT.

References

1. Ghassan Karame, Srdjan Capkun, Blockchain Security and Privacy, IEEE Security & Privacy, July/August 2018, pp. 11-12, vol. 16. DOI Bookmark: 10.1109/MSP.2018.3111241
2. Mishra, N. and Pandya, S., Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review, IEEE Access, April 2021, IEEE.
3. F. Dai, Y. Shi, N. Meng, L. Wei and Z. Ye, "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues," 2017 4th International Conference on Systems and Informatics (ICSAI), 2017, pp. 975-979, doi: 10.1109/ICSAI.2017.8248427.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

4. Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2018, May 28). Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare. arXiv.org. https://arxiv.org/abs/1805.11011v1.
5. Data transmission: What is it? Everything you need to know. (2021, April 9). https://www.cdnetworks.com/enterprise-applications-blog/everything-you-need-to-know-about-data-transmission/.
6. Burgess, L., & Connect. (2015, October 13). How does sensor data go from device to cloud? Retrieved May 20, 2021, from https://readwrite.com/2015/10/13/sensor-data-device-to-cloud/
7. L. Catarinucci et al., "An IoT-Aware Architecture for Smart Healthcare Systems," in IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, Dec. 2015, doi: 10.1109/JIOT.2015.2417684.
8. S. B. Baker, W. Xiang and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," in IEEE Access, vol. 5, pp. 26521-26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
9. S. Pavithra, S. Ramya and S. Prathibha, "A Survey On Cloud Security Issues and Blockchain," 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), 2019, pp. 136-140, doi: 10.1109/ICCCT2.2019.8824891.
10. Nallapaneni Manoj Kumar, Pradeep Kumar Mallick, Blockchain technology for security issues and challenges in IoT, Procedia Computer Science, ELSEVIER, Volume 132, 2018, Pages 1815-1823.
11. H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain," 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017, pp. 1-3, doi: 10.1109/EuroSPW.2017.43.
12. Pandya, S. and Ghayvat, H., Ambient acoustic event assistive framework for identification, detection, and recognition of unknown acoustic events of a residence. Advanced Engineering Informatics, 47, p.1012, 2021, Elsevier.
13. Ghayvat, H., Awais, M., Gope, P., Pandya, S. and Majumdar, S., 2021. ReCognizing SUspect and PredictiNg ThE SpRead of Contagion Based on Mobile Phone LoCation DaTa (COUNTERACT): A System of identifying COVID-19 infectious and hazardous sites, detecting disease outbreaks based on the internet of things, edge computing, and artificial intelligence. Sustainable Cities and Society, p.102798, Elsevier.
14. Ghayvat, H.; Awais, M.; Pandya, S.; Ren, H.; Akbarzadeh, S.; Chandra Mukhopadhyay, S.; Chen, C.; Gope, P.; Chouhan, A.; Chen, W. Smart Aging System: Uncovering the Hidden Wellness Parameter for Well-Being Monitoring and Anomaly Detection. Sensors, 19, 766, MDPI.
15. P. Karthikeyyan, S. Velliangiri and M. I. T. Joseph. S, "Review of Blockchain based IoT application and its security issues," 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2019, pp. 6-11, doi: 10.1109/ICICICT46008.2019.8993124.
16. Y. Yu, Y. Li, J. Tian and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," in IEEE Wireless Communications, vol. 25, no. 6, pp. 12-18, December 2018, doi: 10.1109/MWC.2017.1800116.
17. B. Li, R. Liang, W. Zhou, H. Yin, H. Gao and K. Cai, "LBS Meets Blockchain:an Efficient Method with Security Preserving Trust in SAGIN," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3064357.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

18. H. Zhu et al., "Smart Healthcare in the Era of Internet-of-Things," in IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 26-30, 1 Sept. 2019, doi: 10.1109/MCE.2019.2923929.

19. Tian, S., Yang, W., Grange, J. M. L., Wang, P., Huang, W., & Ye, Z. (2019, October 14). Smart healthcare: Making medical care more intelligent. https://www.sciencedirect.com/science/article/pii/S2414644719300508.
20. Srivastava, A., Jain, S., Miranda, R., Patil, S., Pandya, S., Kotecha K. 2021. Deep learning-based respiratory sound analysis for detection of chronic obstructive pulmonary disease. PeerJ Computer Science 7:e369.
21. Burgess, L., & Connect. (2015, October 13). How does sensor data go from device to cloud? https://readwrite.com/2015/10/13/sensor-data-device-to-cloud/.
22. M. M. E. Mahmoud et al., "Enabling Technologies on Cloud of Things for Smart Healthcare," in IEEE Access, vol. 6, pp. 31950-31967, 2018, doi: 10.1109/ACCESS.2018.2845399.
23. D. C. Nguyen et al., "Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3072611.
24. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things. Sensors 2021, 21, 772. https://doi.org/10.3390/s21030772
25. N. Weerasinghe, T. Hewa, M. Liyanage, S. S. Kanhere and M. Ylianttila, "A Novel Blockchain-as-a-Service (BaaS) Platform for Local 5G Operators," in IEEE Open Journal of the Communications Society, vol. 2, pp. 575-601, 2021, doi: 10.1109/OJCOMS.2021.3066284.
26. S. Singh, A. S. M. S. Hosen and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," in IEEE Access, vol. 9, pp. 13938-13959, 2021, doi: 10.1109/ACCESS.2021.3051602.
27. C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," in IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.
28. Z. Lv, L. Qiao, M. S. Hossain and B. J. Choi, "Analysis of Using Blockchain to Protect the Privacy of Drone Big Data," in IEEE Network, vol. 35, no. 1, pp. 44-49, January/February 2021, doi: 10.1109/MNET.011.2000154.
29. KH Wandra, S Pandya - A Survey on Various Issues in Wireless Sensor Networks, International Journal of Scientific & Engineering, 2012.
30. Mishra, N. and Pandya, S., Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review, IEEE Access, April 2021, IEEE.
31. P. Lin, Q. Song, F. R. Yu, D. Wang and L. Guo, "Task Offloading for Wireless VR-Enabled Medical Treatment with Blockchain Security Using Collective Reinforcement Learning," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3051419.
32. S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand and A. H. Gandomi, "Authentication and Key Management in Distributed IoT using Blockchain Technology," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3063806.
33. Bhushan, B., Sahoo, C., Sinha, P. et al. Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wireless Netw 27, 55–90 (2021). https://doi.org/10.1007/s11276-020-02445-6
34. Tanweer Alam. Mohamed Benaida. "Blockchain, Fog and IoT Integrated Framework: Review, Architecture and Evaluation.", Technology Reports of Kansai University. Vol 62(2). 2020.

35. J. Leng, M. Zhou, J. L. Zhao, Y. Huang and Y. Bian, "Blockchain Security: A Survey of Techniques and Research Directions," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2020.3038641.
36. B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 881-888, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008906.
37. K. Dinesh Kumar, Venkata Rathnam T., Venkata Ramana R., M. Sudhakara, Ravi Kumar Poluru, Towards the Integration of Blockchain and IoT for Security Challenges in IoT: A Review, Transforming Businesses With Bitcoin Mining and Blockchain Applications, Copyright: © 2020 |Pages: 23. DOI: 10.4018/978-1-7998-0186-3.ch003
38. M. Du et al., "Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security," in IEEE Wireless Communications, vol. 27, no. 3, pp. 38-45, June 2020, doi: 10.1109/MWC.001.1900466.
39. H. Huang, J. Lin, B. Zheng, Z. Zheng and J. Bian, "When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues," in IEEE Access, vol. 8, pp. 50574-50586, 2020, doi: 10.1109/ACCESS.2020.2979881.
40. H. Ghayvat, Pandya, S., and A. Patel, "Deep Learning Model for Acoustics Signal Based Preventive Healthcare Monitoring and Activity of Daily Living," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-7, doi: 10.1109/IDEA49133.2020.9170666
41. Pandya, S., Shah, J., Joshi, N., Ghayvat, H., Mukhopadhyay, S.C. and Yap, M.H., 2016, November. A novel hybrid based recommendation system based on clustering and association mining. In Sensing Technology (ICST), 2016 10th International Conference on (pp. 1-6). IEEE.
42. Bhabendu Kumar Mohanta, Debasish Jena, Utkalika Satapathy, Srikanta Patnaik, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,Internet of Things, Volume 11, 2020, 100227, ISSN 2542-6605. https://doi.org/10.1016/j.iot.2020.100227.
43. D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad and J. Wang, "Blockchain-Enabled Distributed Security Framework for Next-Generation IoT: An Edge Cloud and Software-Defined Network-Integrated Approach," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6143-6149, July 2020, doi: 10.1109/JIOT.2020.2977196.
44. Liang, W., Ji, N. Privacy challenges of IoT-based blockchain: a systematic review. Cluster Comput (2021). https://doi.org/10.1007/s10586-021-03260-0
45. Liu, T., Yuan, Y. & Yu, Z. The service architecture of Internet of things terminal connection based on blockchain technology. J Supercomput (2021). https://doi.org/10.1007/s11227-021-03774-9
46. Jain A., Singh T., Jain N. (2021) Framework for Securing IoT Ecosystem Using Blockchain: Use Cases Suggesting Theoretical Architecture. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1270. Springer, Singapore. https://doi.org/10.1007/978-981-15-8289-9_21
47. Namasudra, S., Deka, G.C., Johri, P. et al. The Revolution of Blockchain: State-of-the-Art and Research Challenges. Arch Computat Methods Eng 28, 1497–1515 (2021). https://doi.org/10.1007/s11831-020-09426-0

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

48. Khalaf, O.I., Abdulsahib, G.M. Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. Peer-to-Peer Netw. Appl. (2021). https://doi.org/10.1007/s12083-021-01115-4
49. Banotra A., Gupta S., Gupta S.K., Rashid M. (2021) Asset Security in Data of Internet of Things Using Blockchain Technology. In: Giri K.J., Parah S.A., Bashir R., Muhammad K. (eds) Multimedia Security. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-8711-5_14
50. Hemalatha , et. al., Monitoring and Securing the Healthcare Data Harnessing IOT and Blockchain Technology, Turkish Journal of Computer and Mathematics Education (TURCOMAT), Vol. 12 No. 2 (2021), DOI: https://doi.org/10.17762/turcomat.v12i2.2213
51. Pandya, S., Sur, A. and Kotecha, K., "Smart epidemic tunnel: IoT-based sensor-fusion assistive technology for COVID-19 disinfection", International Journal of Pervasive Computing and Communications, Emerald Publishing.
52. Pandya, S., Ghayvat, H.; Kotecha, K.; Awais, M.; Akbarzadeh, S.; Gope, P.; Mukhopadhyay, S.C.; Chen, W. Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol. Appl. Syst. Innov., MDPI.
53. Farhin F., Kaiser M.S., Mahmud M. (2021) Secured Smart Healthcare System: Blockchain and Bayesian Inference Based Approach. In: Kaiser M.S., Bandyopadhyay A., Mahmud M., Ray K. (eds) Proceedings of International Conference on Trends in Computational and Cognitive Engineering. Advances in Intelligent Systems and Computing, vol 1309. Springer, Singapore. https://doi.org/10.1007/978-981-33-4673-4_36
54. Yaqoob, I., Salah, K., Jayaraman, R. et al. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput & Applic (2021). https://doi.org/10.1007/s00521-020-05519-w
55. D. He, R. Ye, S. Chan, M. Guizani and Y. Xu, "Privacy in the Internet of Things for Smart Healthcare," in IEEE Communications Magazine, vol. 56, no. 4, pp. 38-44, April 2018, doi: 10.1109/MCOM.2018.1700809.
56.
57. M. Bansal and B. Gandhi, "IoT & Big Data in Smart Healthcare (ECG Monitoring)," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 390-396, doi: 10.1109/COMITCon.2019.8862197.
58.
59. Mehta P, Pandya S., Kotecha K. 2021. Harvesting social media sentiment analysis to enhance stock market prediction using deep learning, PeerJ Computer Science 7:e369.
60. P. Zhang, M. A. Walker, J. White, D. C. Schmidt and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), 2017, pp. 1-4, doi: 10.1109/HealthCom.2017.8210842.
61. Snader, R., & Borisov, N. (2008, February). A Tune-up for Tor: Improving Security and Performance in the Tor Network. In ndss (Vol. 8, p. 127).
62. Pandya, S., W. Patel, H. Ghayvat, “NXTGeUH: Ubiquitous Healthcare System for Vital Signs Monitoring & Falls Detection”, IEEE International Conference, Symbiosis International University, December 2018.

63. Ghayvat, H., Pandya, S., “Wellness Sensor Network for modeling Activity of Daily Livings–Proposal and Off-Line Preliminary Analysis” IEEE International Conference, Galgotias University, New Delhi, December 2018.
64. A. B. Haque, A. Muniat, P. R. Ullah and S. Mushsharat, "An Automated Approach towards Smart Healthcare with Blockchain and Smart Contracts," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021, pp. 250-255, doi: 10.1109/ICCCIS51004.2021.9397158.
65. Pandya, S., Wakchaure MA, Shankar R, Annam JR. Analysis of NOMA-OFDM 5G wireless system using deep neural network. The Journal of Defense Modeling and Simulation. Sage.
66. Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir, Self-sovereign identity for healthcare using blockchain, Materials Today: Proceedings, 2021, ISSN 2214-7853,https://doi.org/10.1016/j.matpr.2021.03.083.
67. Raja Wasim Ahmad, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Samer Ellahham, Mohammed Omar,
68. The role of blockchain technology in telehealth and telemedicine, International Journal of Medical Informatics, Volume 148, 2021, 104399, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2021.104399.
69. Shadab Alam, F. A. R. , S. M. Z. H. K. K. R. (2021). Towards Trustworthiness of Electronic Health Record system using Blockchain. Annals of the Romanian Society for Cell Biology, 25(6), 2425–2434. Retrieved from https://www.annalsofrscb.ro/index.php/journal/article/view/5858
70. K. Azbeg, O. Ouchetto, S.J. Andaloussi, L. Fetjah, A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications, IRBM, 2021, ISSN 1959-0318, https://doi.org/10.1016/j.irbm.2021.05.003.
71. Pandya, S., Ghayvat, H., Shah, J., Joshi, N., A Novel Hybrid based Recommendation System based on Clustering and Association Mining, 10th IEEE International Conference on Sensing technology and Machine Intelligence (ICST-2016), Nanjing, China, November 2016.
72. Patel, C.I., Labana, D., Pandya, S., Modi, K., Ghayvat, H. and Awais, M., 2020. Histogram of Oriented Gradient-Based Fusion of Features for Human Action Recognition in Action Video Sequences. Sensors, 20(24), p.7299, MDPI.
73. Kumar, R., Tripathi, R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. J Supercomput (2021). https://doi.org/10.1007/s11227-020-03570-x
74. Xiaomin Du, Beibei Chen, Ming Ma, Yanjiao Zhang, "Research on the Application of Blockchain in Smart Healthcare: Constructing a Hierarchical Framework", Journal of Healthcare Engineering, vol. 2021, Article
ID 6698122, 13 pages, 2021. https://doi.org/10.1155/2021/6698122
75. D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "BEdgeHealth: A Decentralized Architecture for Edge-based IoMT Networks Using Blockchain," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3058953.
76. Boyi Xu, Li Da Xu, Yuxiao Wang & Hongming Cai (2021) A distributed dynamic authorisation method for Internet+ medical & healthcare data access based on consortium blockchain, Enterprise Information Systems, DOI: 10.1080/17517575.2021.1922757

77. Vahdati M., Gholizadeh HamlAbadi K., Saghiri A.M. (2021) IoT-Based Healthcare Monitoring Using Blockchain. In: Namasudra S., Deka G.C. (eds) Applications of Blockchain in Healthcare. Studies in Big Data, vol 83. Springer, Singapore. https://doi.org/10.1007/978-981-15-9547-9_6
78. Awais, M., Ghayvat, H., Krishnan Pandarathodiyil, A., Nabillah Ghani, W.M., Ramanathan, A., Pandya, S., Walter, N., Saad, M.N., Zain, R.B., Faye, I. Healthcare Professional in the Loop (HPIL): Classification of Standard and Oral Cancer-Causing Anomalous Regions of Oral Cavity Using Textural Analysis Technique in Autofluorescence Imaging. Sensors, 2020, 20, 5780, MDPI.
79. B. S. Egala, A. K. Pradhan, V. R. Badarla and S. P. Mohanty, "Fortified-Chain: A Blockchain Based Framework for Security and Privacy Assured Internet of Medical Things with Effective Access Control," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3058946.
80. P. P. Ray, B. Chowhan, N. Kumar and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3050703.
81. Sharma P., Jindal R., Borah M.D. (2021) Healthify: A Blockchain-Based Distributed Application for Health care. In: Namasudra S., Deka G.C. (eds) Applications of Blockchain in Healthcare. Studies in Big Data, vol 83. Springer, Singapore. https://doi.org/10.1007/978-981-15-9547-9_7
82. Pandya, S., W. Patel, An Adaptive Approach towards designing a Smart Health-care Real-Time Monitoring System based on IoT and Data Mining, 3rd IEEE International Conference on Sensing technology and Machine Intelligence (ICST- 2016), Dubai, November 2016.
83. Chelladurai, U., Pandian, S. A novel blockchain based electronic health record automation system for healthcare. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-03163-3
84. I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob and M. Omar, "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," in IEEE Access, vol. 9, pp. 37397-37409, 2021, doi: 10.1109/ACCESS.2021.3062471.
85. Banotra A., Sharma J.S., Gupta S., Gupta S.K., Rashid M. (2021) Use of Blockchain and Internet of Things for Securing Data in Healthcare Systems. In: Giri K.J., Parah S.A., Bashir R., Muhammad K. (eds) Multimedia Security. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-8711-5_13
86. M. Junaid Gul, Barathi Subramanian, Anand Paul, Jeonghong Kim, Blockchain for public health care in smart society, Microprocessors and Microsystems, Volume 80, 2021, 103524, ISSN 0141-9331,https://doi.org/10.1016/j.micpro.2020.103524.
87. Sejal Patel, Narendra Singh, Sharnil Pandya, IoT based smart hospital for secure healthcare system, 2017/5, International Journal on Recent and Innovation Trends in Computing and Communication.
88. Veeramakali, T., Siva, R., Sivakumar, B. et al. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. J Supercomput (2021). https://doi.org/10.1007/s11227-021-03637-3.
89. Garg D., Patel P., Pandya, S., K. Kotecha, "A Deep Learning Approach for Face Detection using YOLO", IEEE International Conference, Symbiosis International university, December 2018.
90. Ziyu Wang, Nanqing Luo, Pan Zhou, GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

Journal of Parallel and Distributed Computing, Volume 142, 2020, Pages 1-12, ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2020.03.004.

91. Pandya, S., Ghayvat, H., Kotecha, K., Wandra, K., Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET, 10th IEEE International Conference on Sensing technology and Machine Intelligence (ICST-2016), Nanjing, China, November 2016.
92. Rashmi G. Shukla, Anuja Agarwal, Shekhar Shukla, Chapter 10 - Blockchain-Powered Smart Healthcare System, Handbook of Research on Blockchain Technology, Academic Press, 2020, Pages 245-270,
93. ISBN 9780128198162, https://doi.org/10.1016/B978-0-12-819816-2.00010-1.
94. Pandya, S. et al., "Smart Aging Wellness Sensor Networks: A near real-time daily activity health monitoring, anomaly detection, and alert system" in Networks and Systems, ed: Springer, 2020.
95. Gautami Tripathi, Mohd Abdul Ahad, Sara Paiva, S2HS- A blockchain based approach for smart healthcare system, Healthcare, Volume 8, Issue 1, 2020, 100391, ISSN 2213-0764, https://doi.org/10.1016/j.hjdsi.2019.100391.
96. Sur, A., Sah, R., Pandya, S., Milk storage system for remote areas using solar thermal energy and adsorption cooling, Materials Today, Volume 28, Part 3, 2020, Elsevier.
97. L. Soltanisehat, R. Alizadeh, H. Hao and K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," in IEEE Transactions on Engineering Management, doi: 10.1109/TEM.2020.3013507.
98. Fakhri Alam Khan, Muhammad Asif, Awais Ahmad, Mafawez Alharbi, Hanan Aljuaid, Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development, Sustainable Cities and Society, Volume 55, 2020, 102018, ISSN 2210-6707,

https://doi.org/10.1016/j.scs.2020.102018.

99. Shreshth Tuli, Shikhar Tuli, Gurleen Wander, Praneet Wander, Sukhpal Singh Gill, Schahram Dustdar, Rizos Sakellariou, Omer Rana, Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions, INTERNET TECHNOLOGY LETTER, LETTER, 2019. https://doi.org/10.1002/itl2.145
100. Pandya, S., H. Dandvate ―New Approach for frequent item set generation based on Mirabit Hashing Algorithm‖, IEEE International Conference on Inventive Computation technologies (ICICT), 26 August, India, 2016.
101. Pandya, S., Patel, W., Mistry, V., i-MsRTRM: Developing an IoT based iNTELLIGENT Medicare System for Real-time Remote Health Monitoring, 8th IEEE International Conference on Computational Intelligence and Communications Networks (CICN-2016), Tehari, India, 23-25th December 2016.
102. SJ Swarndeep, S Pandya, Implementation of Extended K-Medoids Algorithm to Increase Efficiency and Scalability using Large Datasets, - International Journal of Computer Applications, 2016.
103. A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," in IEEE Access, vol. 8, pp. 118433-118471, 2020, doi: 10.1109/ACCESS.2020.3004790.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

104. Pandya, S., Shah, J., Joshi, N., Ghayvat, H., Mukhopadhyay, S.C. and Yap, M.H., 2016, November. A novel hybrid based recommendation system based on clustering and association mining. In Sensing Technology (ICST), 2016 10th International Conference on (pp. 1-6). IEEE.
105. Anton Hasselgren, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, Arild Faxvaag, Blockchain in healthcare and health sciences—A scoping review, International Journal of Medical Informatics, Volume 134, 2020, 104040, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2019.104040.
106. Satamraju, K.P.; B, M. Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare. Sensors 2020, 20, 1389. https://doi.org/10.3390/s20051389
107. P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," in IEEE Systems Journal, vol. 15, no. 1, pp. 85-94, March 2021, doi: 10.1109/JSYST.2020.2963840.
108. Cloudscene.Cloudscene.[Internet].2018Availablefrom:https://cloudscene.com/news/2018/05/internet-of- things-iot/.
109. Pandya, S., Vyas, D. and Bhatt, D., A Survey on Various Machine Learning Techniques‖, International Conference on Emerging trends in Scientific Research (ICETSR-2015), ISBN no: 978-81-92346-0-5, 2015.
110. Pflaum A, Gölzer P. The IoT and Digital Transformation: Toward the Data-Driven Enterprise. IEEE Computer Society.2018;18(1536-1268):5.
111. Gupta B, Quamara M. An overview of Internet of Things (IoT): Architectural aspects,challenges, and protocols. John Wiley & Sons. 2018.
112. NAHA R, GARG S, GEORGAKOPOULOS D, JAYARAMAN P, Gao L, XIANG Y, RANJAN R. Fog Computing: Survey of Trends,Architectures, Requirements, and Research Directions. IEEE Access. 2016;4(2169-3536).
113. Pandya, S., Wandra, K., Shah, J., A Hybrid Based Recommendation System to overcome the problem of sparcity‖, International Conference on emerging trends in scientific research, December, 2015.
114. Vyas, S., Pandya, S., A Survey on Various Issues in Wireless Sensor Networks, National Conference on Computer Science& Security (COCSS-2013), ISBN no: 978-81-92346-0-5.
115. Sarker V, Queralta J, Gia T, Tenhunen H, Westerlund T. A Survey on LoRa for IoT: Integrating Edge Computing. In: Fourth International Conference on Fog and Mobile Edge Computing;2019.
116. Elijah O, Rahman A, Orikumhi I, Leow C. An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. IEEE INTERNET OF THINGS JOURNAL.2018;5(2327-4662).
117. Pandya, S. et al., "Precision Agriculture: Methodologies, Practices, and Applications" in Networks and Systems, ed: Springer, 2020.
118. ChangC,Srirama S, Buyya R. Internet of Things(IoT)andNewComputingParadigms.JohnWiley&Sons. 2019.
119. Pandya, S. et al., "A Novel Multicast Secure MQTT Messaging Protocol Framework for IOT Related Issues," in Networks and Systems, ed: Springer, 2020.
120. Carnevale L, Galletta A, Fazio M, Celesti A, Villari M. Designing a FIWARE Cloud Solution for Making your Travel Smoother: the FLIWARE Experience. In: IEEE 4th International Conference on Collaboration and Internet Computing;2018.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 6680 - 6701
Received 25 April 2021; Accepted 08 May 2021.

121. Yu S, Park K, Park Y. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. Sensors. 2019;19(10.3390/s19163598):3598.
122. Mayur Mistry. (2021). Trash Net based Waste Segregation Assistive System for Smart Cities. Annals of the Romanian Society for Cell Biology, 1532–1544. Retrieved from https://www.annalsofrscb.ro/index.php/journal/article/view/2661
123. Sur S., Pandya, S., Ramesh P. Sah, Ketan Kotecha & Swapnil Narkhede, Influence of bed temperature on performance of silica gel/methanol adsorption refrigeration system at adsorption equilibrium, Particulate Science and Technology, Taylor and Francis.
124. Pandya, S., Ghayvat, H., Sur, A., Awais, M., Kotecha, K., Saxena, S., Jassal, N., Pingale, G. Pollution Weather Prediction System: Smart Outdoor Pollution Monitoring and Prediction for Healthy Breathing and Living. Sensors, 2020, 20, 5448, MDPI.
125. Barot, V., Kapadia, V., & Pandya, S., QoS Enabled IoT Based Low Cost Air Quality Monitoring System with Power Consumption Optimization, Cybernetics and Information Technologies, 2020, 20(2), 122-140, Bulgarian Academy of Science.
126. ShiraziS,GouglidisA,FarshadA,Hutchison D. TheExtendedCloud:ReviewandAnalysis of MobileEdge Computing and Fog From a Security and Resilience Perspective. IEEE.2017;35(0733-8716):11.
127. Sarangi S, Naik V, Choudhury S, Jain P, Kosgi V, Sharma R, Bhatt P, Srinivasu P. An Affordable IoT Edge Platform for Digital Farming in Developing Regions. In: IEEE;2019.
128. Satyanarayanan M. The Emergence of Edge Computing. I EEE COMPUTER SOCIETY. 2017;17(0018- 9162).
129. Math A, Ali L, Pruthviraj U. Development of Smart Drip Irrigation System Using IoT. IEEE. 2018;18(978- 1-5386-5323-4).
130. Pandithurai O, Aishwarya S, Aparna B, Kavitha K. AGRO-TECH: A DIGITAL MODEL FOR MONITORING SOIL AND CROPS USING INTERNET OF THINGS (IOT). IEEE. 2017;17(978-1-5090- 4855-7).
131. Aagaard A, Presser M, Andersen T. Applying Iot as a leverage for business model innovation and digital transformation. IEEE.2019;19(978-1-7281-2171-0).
132. Chandra N, Khatri S, Som S. Business Models Leveraging IoT and Cognitive Computing. IEEE. 2019;19(978-1-5386-9346-9).
133. Whitmore A, Agarwal A, Da Xu L. The Internet of Things—A survey of topics and trends. Springer.2014.
134. Lewis, G. (2010). Basics about cloud computing. Software engineering institute carniege mellon university, Pittsburgh.
135. George, A., Dhanasekaran, H., Chittiappa, J. P., Challagundla, L. A., Nikkam, S. S., & Abuzaghleh, O. (2018, May). Internet of Things in health care using fog computing. In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1-6). IEEE.
136. Shnayder, V., Chen, B. R., Lorincz, K., Fulford-Jones, T. R., & Welsh, M. (2005). Sensor networks for medical care.
137. Dama, S., Pasca, T. V., Sathya, V., & Kuchi, K. (2016, April). A novel RACH mechanism for dense cellular-IoT deployments. In 2016 IEEE Wireless Communications and Networking Conference (pp. 1-6). IEEE.