information

Article

Enabling Blockchain with IoMT Devices for Healthcare

Jameel Almalki [1,†], Waleed Al Shehri [1,†], Rashid Mehmood [2,†], Khalid Alsaif [3,†], Saeed M. Alshahrani [4,*], Najlaa Jannah [1] and Nayyar Ahmed Khan [4,*,†]

[1] Department of Computer Science, College of Computer in Al-Lith, Umm Al-Qura University, Makkah 24382, Saudi Arabia
[2] High Performance Computing Centre, King Abdulaziz University, Jeddah 22254, Saudi Arabia
[3] Department of Computer Science, King Abdulaziz University, Jeddah 22254, Saudi Arabia
[4] Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra 11961, Saudi Arabia
* Correspondence: salshahrani@su.edu.sa (S.M.A.); nayyar@su.edu.sa (N.A.K.)
† These authors contributed equally to this work.

Abstract: Significant modifications have been seen in healthcare facilities over the past two decades. With the use of IoT-enabled devices, the monitoring and analysis of patient diagnostic parameters is made considerably easy. The new technology shift for medical field is IoMT. However, the problem of privacy for patient data and the security of information still a point to ponder. This research proposed a prototype model to integrate the blockchain and IoMT for providing better analysis of patient health factors. The authors suggested IoMT data to be collected over Edge Computing gateway devices and forward to Cloud Gateway. The three-layered decision making structure ensures the integrity of the data. The further analysis of information collected over sensor-based devices is done in the Cloud IoT Central Hub service. To ensure the secrecy and compliance of the patient data, Smart Contracts are integrated. After the exchange of smart contracts, a block of information is broadcast over the health blockchain. The P2P network makes it viable to retain all health statistics and further processing of information. The paper describes the scenario and experimental setup for a COVID-19 data-set analyzed in the proposed prototype mode. After the collection of information and decision making, the block of data is sent across all peer nodes. Thus, the power of IoMT and blockchain makes it easy for the healthcare worker to diagnose and handle patient data with privacy. The IoMT is integrated with artificial intelligence to enable decision making based on the classification of data. The results are saved as transactions in the blockchain hyperledger. This study demonstrates the prototype model with test data in a testing network with two peer nodes.

Keywords: IoMT; blockchain; bog; bdge; bloud; computing; hyperledger; healthcare

Citation: Almalki, J.; Al Shehri, W.; Mehmood, R.; Alsaif, K.; Alshahrani, S.M.; Jannah, N.; Khan, N.A. Enabling Blockchain with IoMT Devices for Healthcare. *Information* **2022**, *13*, 448. https://doi.org/10.3390/info13100448

Academic Editors: Inam Ullah Khan, Mariya Ouaissa, Tarandeep Kaur Bhatia and Syed Bilal Hussain Shah

Received: 13 August 2022
Accepted: 21 September 2022
Published: 25 September 2022

1. Introduction

In the present era, the Internet of Things (IoT) and blockchain technologies are in great demand across all sectors of lifestyle and living. The Internet of Things is typically a group of services that are decentralized in nature and the capability of the services are a result of the server performance and utilization factors. Thus, it becomes a typical task for the performance enhancement of IoT devices to connect and collaborate seamlessly with computing resources. To overcome these issues, blockchain technology provides decentralization with high reliability and security. Thus, IoT based on blockchain technology may become an effective option for building a secure IoT system. With technology advancements, many healthcare devices have been used to help patients stay in touch with their physicians and track their health during day-to-day activities. Most wearable devices use IoT technologies, which ultimately forms several networks of various sizes that aim to process patient data to provide a helpful decision about patient health. The Internet of Things (IoT) networks are intelligent networks that could connect billions of objects that communicate digitally to

share information and integrate devices through standard protocols. IoT is a commonly used term that means locating, tracking, monitoring, and managing things. IoT healthcare applications implement the latest communication technologies to connect healthcare providers and patients through value-added services, such as remote monitoring the health status of patients and providing data analysis applications from sensors to help doctors and patients. Therefore, IoT has an important role towards the medical and healthcare information realm and transcription process.

While healthcare systems utilize the benefits of IoT networks to monitor and track patients, several pre-processing issues remain open, including handling extensive stream data and the real-time tracking of patient's records. Such a problem is a common issue for people who suffer from chronic diseases affecting people's quality of life [1]. Often, IoT applications are used to collect various human body symptoms and factors such as blood pressure or temperature. Often various wearable devices operated by sensors are used to measure the vital signs and some applications can be used to help patients with their living activities. Therefore, the main issue is how data are gathered, processed, and saved, given the different types of data: textual, video, and continuous data.Researchers showed that implementing an Internet of Things platform based on a centralized approach to enhance data transfer from these sensors is a significant challenge [2]. According to [3], the main challenges in connecting traditional and Internet of Things applications in healthcare are dealing with big data at very high speed as well as the need to solidify the basic infrastructure involved in this process. Therefore, the cost of analytic data platforms, the ever-increasing number of Internet devices, and standardized standards for collecting data from IoT devices are driving the further adoption of this technology, which requires computerizing huge amounts of data collected from sensors as well as ensuring the security and privacy of these data [3].

The traditional model of the IoT that generates large amounts of data sent to the information center to process and store is no longer efficient for healthcare systems. Therefore, with limited computation at IoT networks (edge computing), alternative options are sought to deal with the computation challenge. In this era, and add-on layer called fog computing, in association with the cloud layer, aims to drive the sensor's data processing and storage features close to the data source to ensure a rapid and reliable response to emergency monitoring applications and the safe handling of privacy-sensitive data [4]. In the meantime, the fog computing model of IoT healthcare applications is increasingly being investigated as a means to conduct complex computing and time-sensitive processing locally [5]. Furthermore, above fog computing, when processing Big data, such as providing data to various subscribers, cloud computing becomes an alternative, where data could be collected from different providers and shared across hospitals, physicians, and insurance companies with restricted privacy and sharing policies.

The manuscript is divided into five sections. The background comprises information about block chain technology and its allied components such as security, the Ledger, sharing and distribution. Further, the discussion over Internet of Medical Things devices and their applicability in healthcare is discussed. The data collected from these IoMT devices is sent over the Internet with the help of fog, edge and cloud gateways. The issues related to fog and edge gateways are discussed sequentially. Section 3 contains the research. The motivations under which some of the Allied architectures fall are discussed. A variety of designs and implementations, submitted by various authors, are expressed in this section. Section 4 contains the system design and the methodology. The proposed a system architecture comprising of the three stages of processing is explained in this section. Various layers at which the data are accumulated and submitted to the cloud computing environment for further processing are explained. Furthermore, after the data acquisition is over, data analytics is expressed for decision-making module. In the next Section 5, the experiment and observations are represented. The prototype model created for test networks is explained in the experiment portion. This section also expresses some of the hardware specifications along with analysis of results for the data-set collected from an

open source repository. The analysis is also depicted in the form of graphs and tables. At the end of the section, a block chain network is deployed in the test network to demonstrate the exchange of smart contracts between two peer nodes. Each and every section contains a detailed description of all the points mentioned.

2. Background

2.1. Blockchain

blockchain technology has emerged as the most secure decentralized platform, offering many significant features without dealing with a third party and limiting tampering to ensure data confidentiality and privacy. The use of blockchain can help to reduce the problems associated with the security and management of the IoT platform to a larger extent [6]. blockchain technology offers many benefits to medical researchers, healthcare providers, and individuals and is a means that can be used in medical research to create a website to store health data, track personal data and allow accurate data access [7]. Data sharing within various stakeholders in healthcare collaborations is indeed one of the most important tasks that was required during the outbreak of the global COVID-19 pandemic. The global connectivity and data availability ensure that the research needed to handle the pros and cons of the pandemic can accelerate at a higher pace. The powerful data sets that result from the global data collection can turn up as very high-level inputs to study and resolve various issues related to COVID-19 research. The data sharing must be as per the global rules and international regulations to avoid any misconduct of the data sharing policies. The privacy of the patient's information is indeed one of the key factors at the top end of the data share spectrum. The medical data for an individual should be shared as per the standards in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and global data policies. As per [8–33] the electronic regulations of data sharing presented in the article reveal the difficulty of keeping track of who has had access to the data and how the data may have changed over its lifetime; while providing a secure and easy-to-use mechanism to share the data between different users.

The use of various medical-oriented IoT devices is becoming more popular to measure the medical conditions of the patients. These devices are capable of identifying the blood pressure, temperature of the body, oxygen level and heart beats of a human with ease. The decentralized nature of the blockchain in combination with these Internet of Medical Things (IoMT) devices can be very helpful for patients in terms of privacy and usability. The eradication of the centralized server or agencies from the patient and data access makes it easier and more natural to share information over global platforms and increase control of the human being involved in the process. In general, the use of blockchain empowers the hospitals and patients to communicate over the data and information in a very convenient and decentralized manner. The global sharing of the IoMT powered devices in accordance with the patient's medical transformation history is made very easy with the help of the blockchain and IoT integration. Sending the IoMT data to the blockchain under secure smart contract mechanism makes it really easy for the system to reduce data forgery as well as the mutation of the information. The trust between the stakeholders is achieved with the help of the blockchain security policies. The system for data collection, sharing, storing and maintenance becomes really simple and transparent with the use of the blockchain decentralized storage concept. It also results in a proper control of the patient privacy policy.

2.2. Blockchain Components

In the past, enabling blockchain directly on resource-constrained IoT devices was inadvisable due to the following three reasons: lack of computational resources, lack of sufficient bandwidth and the need to preserve power. Therefore, fog and cloud technologies have emerged to overcome these limitations for enabling a blockchain in IoT systems. With the advent of smartphone technologies, computational resources are becoming an alternative solution for edge computing to act as fog instead, thus overcoming resource constraints in computation and bandwidth issues.

2.2.1. Ledger

The entire history of the communication and the transactions that have taken place in the blockchain are governed by a Ledger. This is a piece of software which is able to hold all the transaction and database entries which are responsible for any transaction in the P2P network. It is also very efficient and quick in terms of database commitments. Unlike the traditional databases, the Ledger tries to update the blocks based on the concept of no overriding. This empowers the integrity of the system information which is broadcasted to all the nodes in the blockchain.

In the case of our prototype, we try to make use of hyperledger fabric as the backbone of the blockchain network. The hyperledger fabric is a standalone framework, which is responsible for handling all the blockchain transactions and record all the information. The data that flow from the analytics model of the cloud service provider reach the hyperledger with the help of registered devices, and cloud gateway. The use of edge computing and fog computing makes it easier to make decisions based on the information. Once the decision is made, the final commit with the help of a smart contract will be completed at the blockchain hyperledger level across the P2P network. The decentralized information assures the security and privacy of the patient information in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other federal laws of individual information.

2.2.2. Secure

All the information that is stored in the blockchain network is encrypted with the help of secure cryptography algorithms. These algorithms are a variety of computational procedures which are governed with the help of spatial mathematical operations and hash functions. All the data that are stored in the Ledger are encrypted with the help of these security algorithms. These data cannot be tampered with or monitored. The alteration of the information that is made available in the data is not possible without the help of the hash value. The security of the blockchain depends mainly upon the function that is used to encrypt the data. One more exciting feature of blockchain security is its ability to append the hash value of the present block with the previous and the next connected block. All the peers in the network are checked for the integrity of this hash value. Just in case the value is tampered with or not as per the real, the data block is considered to be vulnerable and information tampering or forgery is detected. This makes the privacy concern of the blockchain very effective and powerful.

2.2.3. Shared

The Ledger, which is responsible for holding the information across the P2P network in the blockchain, contains various actors and stakeholders. The transparency across the nodes is maintained with the help of secure hash algorithms. All the participants carry equal privileges and functions that can be helpful to maintain the integrity of the data. Forgery or tampering in the shared model becomes very difficult due to the decentralization of data across global nodes.

2.2.4. Distributed

A distributed blockchain is also possible. The scaling of the nodes which are indeed a part of the blockchain can be controlled in order to make it more efficient and resilient towards attack piety and ethical access. As a general observation, a larger number of network nodes enhances the chance for ethical access. This can result in a bad impact on the consensus protocol which is used for the safety measures of the blockchain [20].

2.2.5. Private

At this point the use of private blockchain is very useful. All the information between the patient and the health-related information monitoring application, and at the further levels, will be shared using a private blockchain.

2.3. IoMT

The IoMT devices works with smart , low-energy, wireless-enabled media which are very efficient and safe [8]. Generally, these are used to find the values, manipulate, collect, analyze and secure the bio-metric data of a patient. The information collected by these small sensors generally comprises the position of the patient, their body weight, dimensions, sleep times, oxygen level, temperature, heart beats, rate of respiration, fatigue level and blood pressure. IoT has resulted in the advent of the Internet of Medical Things (IoMT) [9], such as beds and wheelchairs embedded with sensors, which are what is meant by "medical things". The hospital staff, including the nurses and doctors, have the access to the patient bio-metric information which is very valuable at the run time diagnosis of the patient. The handheld devices or the sensor-based IoMT devices will be very helpful for the handling of the information that is available in this situation. The decisions made by the doctors in this case will be more accurate and eligible for diagnosis of proper medicine and actions in the hospital to save a patient from ailments. Multiple sources of information are available from various IoMT devices and their resulting readings [10]. The correlation between these readings are indeed very helpful for the doctors and the stakeholders to provide a quality treatment to the patients. The information which is given by the devices and experience of the doctors makes it easy to handle the patient health. Any specific potential situation can be handled and some emergency situations can be averted with the help of the sensor-based devices as well.

2.4. Fog, Edge and Cloud-Computing

The power of blockchain lies in the fact that it does not require a centralized database or computational unit. To enhance the working capability of this blockchain unit. The ideology of edge computing, fog computing and cloud computing can be applied thoroughly. As per [10], Cloud computing is indeed one of the most powerful computational technologies that enhances the functionality of applications. The devices that are connected to any healthcare unit are called as edge gateways. Edge computing makes it easier to process the raw information collected by the sensor devices into meaningful data packets. The further processing of these devices takes place at the fog layer. It contains various analytic engines powered by the artificial intelligence algorithms. Tools such as TensorFlow and Keras have emerged as powerful techniques to analyze the information collected at the fog layer. Finally, the information can be analyzed with the help of various cloud-based service routines provided by the cloud service providers. These analytics input the information passed from the edge gateways or fog layer. This information is dressed and modified as per the cloud service provider analytic engine. It is the duty of the data admin to handle this piece of information. Once the information reaches the cloud network and is analyzed, it is further propagated to the blockchain network for final P2P sharing across the decentralized nodes.

As per [31], there is a significant problem associated with the fog computing paradigms. The devices in the fog computing environment are more likely to be attacked by various type of threats. Issues and problems associated with forgery, tampering, spamming, jamming, eavesdropping, denial of services, man in the middle, collusion, impersonation, virtual machine attack, side channel attack and session hijacking are some of the well-known threats to for computing devices. The issues of privacy, for a user, their identity, data, usage and location are also one of the prime problems associated with fog computing. Similar kinds of issues have been reported in edge computing nodes in which a large amount of data were stored. Compared to the cloud computing environment, the resources available in edge computing are fewer. Thus, it becomes easier for the attackers to perform any type of security breach, especially eavesdropping, denial of service, data tampering, distributed denial of service, rogue gateway and physical attacks. Reference [32] suggested that there has been a significant emphasis on security and privacy protection in the blockchain environment as compared to fog and edge computing. Up to certain extent, the cloud computing environment is more suitable for security. However, the decentralized data

in the blockchain along with the secure hash algorithms are more safe. In general, this proposed architecture uses all three computing paradigms. However, the final result is synchronized and sent to the block chain notes in the P2P network.

3. Research Motivation

Massive amounts of data are streamed on the IoT platforms by various sensor-based devices and circuits. The connection of these devices via the internet makes it possible to stream the data over the wires or wireless medium to intended centralized servers for further processing. Various concerns arise when the data are streamed on the internet and they are indeed very important consider. The security of the data, privacy matters and congestion of the network transfers are some very strong issues that still require much attention. The server efficiency, performance and its latency are indeed more important factors that should be studied before information floats on the internet-based computational units. However, blockchain technology has resolved these issues up to a larger extent. The use of such information in a secure decentralized environment makes it suitable to handle the biggest issue of data privacy and security. Therefore, to improve connectivity in the IoT environment, edge–fog–cloud computing has been adopted to overcome scalability, latency and computing efficiency issues, and blockchain technology is capable of handling and dealing with security issues. Therefore, the result of this work is an Edge–IoT-enabled framework based on the blockchain.

Cloud platforms are typically hosted in centric and large-scale data located at the edge of the Internet backbone [11]. IoT devices interact with each other in surrounding environments, which leads to the generation of a massive amount of data and, hence, processes, storing the data at a central server [12]. However, the storage of data at a single central server can be exposed to privacy leakage, if there are no appropriate defensive mechanisms adopted [12]. The centralization of the data in various data centers raises the probability of the data to be located at a distance from the user and all the services that are available for the user vary as per the demography of the region in which the data center is located. The concern for larger bandwidth as well as the data center management is another concern in this regard. The limitations that are specified in this study can be leveraged with the help of fog and edge computing. These technologies have emerged as a great means for providing low latency as well as guaranteeing higher bandwidth for the handling of the system. The approach that we are proposing in this study leads us to bring the next generation of data processing with the help of edge resource layers that are used for the real-time decision making.

Reference [13] presented a very comprehensive comparison of existing surveys on the research gaps of secure communication among devices connected in the IoT networks. The authors proposed that the convergence of blockchain at different levels can help in improving the security but they also commented that this will not eliminate the use of existing security approaches. They proposed a security and blockchain model for healthcare which provides authentication, privacy and trust in the devices that are deployed in the healthcare system. The proposed model has not been deployed; therefore, the actual impact is unknown. The collection of data from IoMT is a challenge [14], as most of the devices consume low power and transmitting huge amounts of data is very limited. This limitation can be handled by the help of 5G and Low-Power Wide-Area Network (LP-WAN), which is currently in the deployment phase, at a very rapid pace [15].

Reference [16] proposed a framework of blockchain-enabled Internet of Medical Things (IoMT) named BCeMT. They have also provided some that are efficient during the pandemic situation. The proposed framework by the authors was used for prevention of the disease including contract tracing as well as the management of the injectable medicine supply chain. The proposed framework BCeMT improves interoperability and preserves privacy. It also assures security by using cryptography-based hash function and bit-wise XOR operation. Reference [29] also presented a very robust architecture for the use of blockchain

in healthcare units. The framework suggested by [30] made use of artificial intelligence and IoT devices for a sustainable city healthcare unit.

The proposed framework [17] has only added an additional layer of blockchain into the IoMT layering architecture. The IoMT has three layers inclusive of the perception layer, followed by a data management layer and finally the medical services layer, which is responsible for taking decisions. The layer which is added in BCeMT is added in parallel to the existing three layers of I0MT in such a way that it serves all the three layers. Thus, it provides a mechanism that all the communication is protected by blockchain technology. The proposed framework is facing some challenges such as resource constraints because the information produced by the medical devices is enormous and the size of the data will grow continuously. Another issue is also related to the size of the chain in blockchain, because all the peers are responsible for duplicating the data, which is done by a participating and broadcasting node. The nodes in this network also have limited processing capability. Therefore, there is a need to have a cloud storage in place that can store huge amounts of data. The data that are not very critical can be placed on the clouds and the critical data can be passed through the blockchain. In this way, the load on the participating nodes can be reduced to a great extent. There are also some governance issues, as the healthcare data are very sensitive and there are multiple medical institutes and hospitals involved that are part of one network. Therefore, some legal measures need to be taken. Further areas that can be further explored are (I) the need for policies and privacy concerns related to the medical data; (II) obstacles that arising related to the sharing of the data in the medical realm, for which there is no guarantee that they will be exploited or leaked; (III) scalability will also be challenged as the size of the network can grow exponentially and the data flow will be enormous when the hospitals are overloaded [16].

Reference [17] highlighted some very important research directions which can help in pandemic situations such as COVID-19. In this paper, they presented a comprehensive review of blockchain technology and IoT for smart cities. They have also proposed a decentralized architecture for the IoT devices integrated into smart cities. The proposed architecture [18] is divided into three layers: the Energy Generation and Distribution Layer, the Communication Layer and the Consumer–Producer Layer. The first is responsible for the management of the energy requirements of the network. The second is responsible for maintaining a reliable communication link using the 6G communication medium between the network components. The third is uses the Ethereum client, which is able to perform a P2P-level trading in the blockchain environment. Each entity in this layer has its own wallet to record all the energy-related transactions. All the transactions are recorded using the framework and are reported back in the decentralized blockchain network. This P2P network results in the duplication of the data across all the nodes in the chain irrespective of the demography of the blockchain.

The authors of [18] summarize three major challenges: (1) The security of the devices that are a part of the IoT realm is not adequate. (2) Privacy: protecting the privacy of the user data. (3) Centralization: centralized methods for IoT and bringing out some challenges such as failure of the node in between, traffic issues during broadcasting and the reduction in the scalability of the entire solution.

Methodology

The proposed methodology that is used in this manuscript is the structured analysis and design technique. The hierarchy design is explained step-by-step in an incremental fashion. The initial stage for designing the system begin from the collection of data from healthcare workers or hospitals and trees with the help of IoMT devices. Once the data are retrieved, that information is flown from the devices to the internet with the help of edge and fog Gateway devices. This devices at the second stage sends some information to the cloud network. The second stage of processing in the proposed methodology comprises yet another system function that relates to decision making based on cloud analytics. The third step , which is responsible for the blockchain and smart contract, is also designed.

The methodology used in this is case helpful for the upgrade of a system and identifying its shortcomings.

4. System Design

The main part for this study is to design a prototype model for creating a blockchain network with the help of IoMT devices, as depicted in Figure 1 below. These devices will be connected to a centralized cloud of that will be responsible for storing huge amounts of data. The data, once they reach the cloud, are analyzed with the help of adaptive engines at the cloud service provider. Once the adaptive engine analyzes the data of a patient's medical history and present condition, including all the other bio-metric factors, it will try to analyze and predict the nature of the issue or problem associated with the patient. Once the information is obtained and finalized, the result will be sent over the blockchain. With the help of a smart contracts, the specialized devices that are enrolled to work in the blockchain network will be able to submit the information. The smart contracts assure the security and privacy of the information at a node. This node can be a hospital, doctor, nurse, or it can be any federal agency responsible for uploading the information on the blockchain. The availability of information will be replicated at decentralized blockchain network across the P2P connection. This connection will be helpful for identification of patient information whenever it is required.

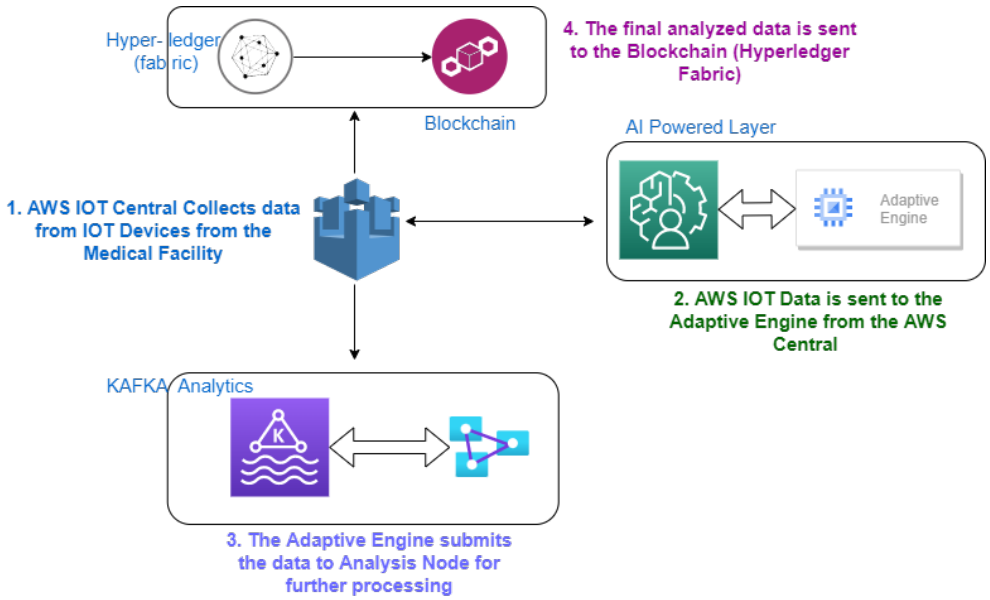

Figure 1. Proposed System Design for the IoMT based Blockchain in Healthcare.

It is highly expected that the data traffic generated by these devices would be enormous and will require mechanisms to extract useful information [16,19]. One of the main areas of concern is the data generated by the Internet of Medical Things (IoMT). This data contains very valuable information about the patients and the types of diseases that are affecting them. In the present circumstances, where COVID-19 has struck the whole world with severe on-going and long-lasting effects, the time has come that rigorous research needs to be conducted regarding the cause of the spread and aiming to minimize the impact of such diseases. It is highly expected that, in the future, humankind will have to face diseases like this that can be more devastating. Several research projects are proposed that show the importance of the use of blockchain for IoMT. In [27], the architecture that was proposed by the authors was very powerful, using blockchain and LoRa Network for Personal Health Care Data Monitoring. Some of them are discussed in the given below sections. Blockchain technology is very useful for the Internet of Medical Things in terms of security. Blockchain multi-layer can combine the features of the blockchain along with the IoMT, which can provide solutions to problems that cannot be solved by just one technology. By combining

these two technologies, a multi-layered blockchain provides a next-generation platform for IoT devices based on blockchain technology as shown in Figure 2 below. The main advantage of this structure is to solve the problems that current mass chains face due to lack of scalability. IoT devices can be the nodes in their own blockchain, and some are also part of the next layer of public blockchain.

Figure 2. Generic Blockchain, Smart Contract and IoT Collaboration.

4.1. Device Registration

4.1.1. IoT Device Registration Process at Edge Layer

The initial layer comprises all the devices that are supposed to be registered inside the blockchain network. Whenever a device registers itself inside the network, the identification number of the device, hash value, critical hash value of the data comprising of the information are updated in the blockchain Ledger. When the sensor data are analyzed and processed inside the Ledger unit, the information is upgraded, and finally sent, with the help of a smart gateway, to all the peer nodes. The decentralized information passes as a broadcasted node with the help of the smart contract. This is the smart contract price to verify the identification number of the device that has sent the data from the propagating node.

As is clear from the schema above in Figure 3, any IoMT device which is responsible for capturing the information of a patient in a specified format will be able to send information to a node. This information will propagate further depending upon the smart contract between the device and the blockchain network. It must be noted that the edge layer computation takes place and the decision for accepting the information is done at the first primary level in this transaction. Just in case the information supplied by the device is not clear or in a proper format, it is rejected immediately at the edge level. In this case, edge computing helps us to reduce the need for high computation power and large memory storage. Thus, it makes the information flow very easy and effective. Without the need for any specialized server or centralized database mechanism, the information roots to a simple node once the smart gateway data is approved.

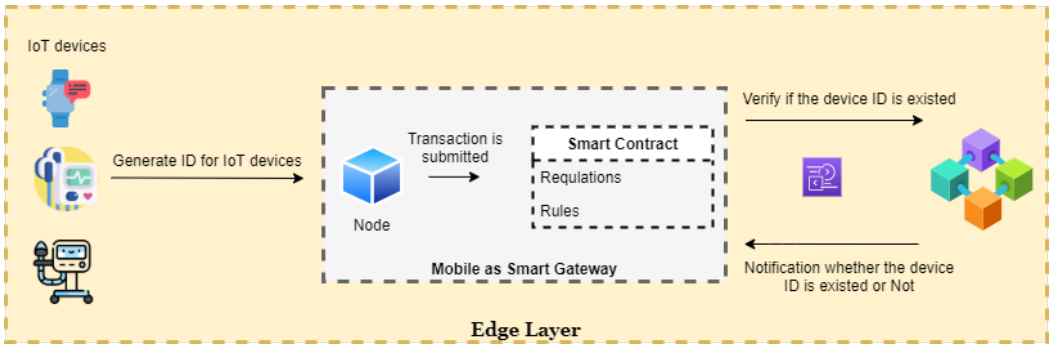

Figure 3. IoT device registration process at Edge layer.

The registration of the device is executed and processed further. Once the process of device registration is executed and the transaction for this execution is noted inside the Ledger, a new block is generated with the help of the blockchain that comprises the device identification along with the hash value. The sensors, which are registered with this network, are also provided unique identification numbers. Once these identification numbers are propagated in the blockchain, the complete system across the decentralized

P2P network is notified. A representation of the registration process at the edge layer is depicted in the Figure 3 above.

4.1.2. Patient EHR/EMR Registration

This is a restrictive type of network where only the users that are from one organization under centralized control can join. The Electronic Medical Record (EMR) is created in this stage. The internal structure in Figure 4 below is very similar to the public blockchain as all the users from this network can have access to it but only the authorized users can have access to the past and on-going transaction records and only few users can validate the transactions. The size of this type is small compared to the public blockchain. Therefore, the performance is much better but, due to the limited size of this type of network, it is easily forged when a few of the participating nodes are compromised [21].

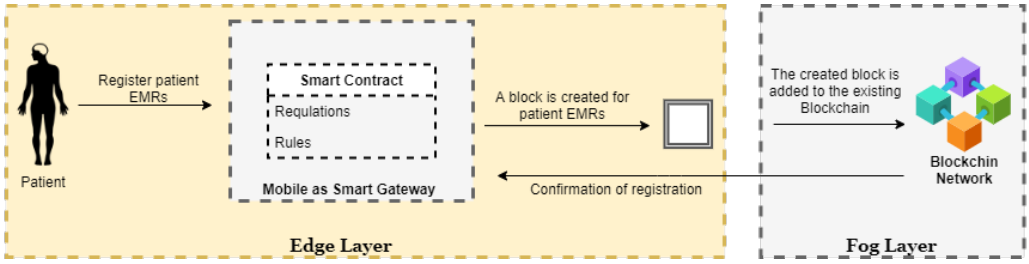

Figure 4. Patient ID registration process.

4.1.3. Lightweight Block Generation of Patient Data

The information which is read by the censors and other devices connected on the patient's body is captured in a predefined format. The cloud service provider across the world can practically connected to any type of IoT device without any problems. Once the device is connected to the IoT Central cloud, information from the devices starts flowing to this particular hub. It should be noted that as soon as the information goes to the hub, it is collected by the analytics service engine. The analytics service tries to identify the captured piece of information and data. After the complete processing and analysis of the information, a result is generated, depending upon the factors and features. The final evaluation and analysis is supplied back to the smart gateway. Similar pieces of data are forwarded to the blockchain network with the help of smart contracts. The block of data generated for a patient information, is transferred and broadcasted to all the P2P network nodes. These nodes are responsible for identifying and finding the information related to patient health. It must be noted that the information follows all copyright issues and compliance policies as per the federal law.

4.2. IoT System

Any healthcare IoT system has some basic system requirements, including a sensor-integrated hardware platform that can reliably coordinate with back-end processing systems. The resulting system is an end-to-end healthcare system that is scalable, remotely accessible, and secure. Further, the system requirements may include cost constraints, measurement of specific health parameters and applications targeted at specific diseases or users. The three essential components of the system architecture of any IoT-based healthcare system are as follows:

1. Data Collection Layer: This layer primarily includes sensors and devices that collect data from the patient and can forward it using a wireless communication protocol such as WiFi, Bluetooth, ANT, Zigbee, NFC. A few examples are heart rate monitoring devices, health bands, and fitness trackers.
2. Data Storage Layer: This layer includes various types of data storage, including physical storage or cloud storage. The data storage must have negligible latency in data retrieval due to the critical nature of healthcare applications. It is also crucial that the data stored has sufficient redundancy and backup to be securely recovered.

3. Data Processing Layer: This layer concerns the analysis of stored data for decision making and insights. The processing could be done entirely in the cloud or distributed between the edge and the cloud. Artificial intelligence, as well as other optimization techniques, are frequently used in this layer.

If we look further into the system requirements for IoT-based healthcare systems, multiple requirements are more application-specific. For example, if the system is being designed for patients, the notifications will be required to be informative and straightforward, whereas if the system is being designed for healthcare professionals, they may need more technical information regarding the patient. Similarly, some applications require monitoring of critical parameters of a patient and hence the data processing and dissemination must be in real-time to avoid fatality. Therefore, the system requirements may change based on the user or application, but the basic requirements will need a robust sensing layer, reliable data storage and a low latency data-processing layer to ensure the system is efficient and secure.

4.2.1. IoT System Components

The system model which is proposed as a part of this study works at three different layers. The framework, which is proposed, is composed of a sensor layer. All the elements and devices which are at this level are termed as edge layers. The main task of this layer is to make sure that the information which is flowing from different sensors and IoMT devices is in the proper format as required by the analytics engine. Usually the bio-metric information of a human patient is collected with the help of such devices and is collectively sent across the Internet to the cloud provider. The next level of working in this prescribed model comprises the fog layer. The information which is received from the edge devices is submitted to the fog layer. This layer tries to identify and analyze the possible issues associated with the outputs. An artificial intelligent analytics system such as KAFKA or data-bricks, etc., executes the routines related to the data. All the information is cached and buffered with the help of these intelligent analytics routines and the final result is supplied back to the data fusion system. The final layer is the cloud gateway layer. The processed data from the edge and the four players are submitted. Finally, too, the IoT Central hub is found by the cloud service provider. This harbor is practically capable of identifying any IoT device connected across the network, sending information to the Central location. The data from the edge layer are processed at the cloud gateway and further analysis is done in accordance with the fog layer. Once the analysis is completed, the information flows through a smart contract towards the blockchain network. All the stakeholders receive a copy of their information on a local node. This information is also replicated across all the P2P network nodes in the blockchain hyperledger. Finally, the information is committed and saved permanently in this decentralized network. A similar approach can be applied to various other diseases and diagnostics required in various healthcare facilities. Figure 5 below represents a schematic representation of the model represented in this study.

The following functionalities take place in the proposed architecture at various levels of computing:

1. Edge Layer: Edge layers are directly related to data collected through the “patient”, having a two-tiered structure, where all the information which is collected with the help of sensor-based IoMT devices travels via a smart gateway. Usually these gateways are smartphones or smart devices connected to the wireless network for streaming data. The main function of IoMT devices is to establish an effective sensing technology to collect various types of patient health data. All IoT devices collect the patient’s medical information or any other type of information that is specific to the patient. These devices are small electronic circuits with specific functionality and therefore they lack computing power and storage. The availability of less computation, speed, memory and more latency results in the poor performance of data streaming and cryptography calculations [22]. Thus, data processing requires a higher level with the central node in blockchain, a high-performance computer that acts as an intelligent

gateway to blockchain in the upper layer. Each patient will have a blockchain to integrate all the patient's IoT data into the patient's blockchain.

The measurement of various physiological parameters requires multiple on-body and implantable sensors. All these sensor nodes are standalone, as well as being capable of communicating with the rest of the system. Each one has its wireless trans-receiver, a computing unit in the form of a micro-controller or microprocessor and energy supply in the form of a battery with an optional energy harvesting unit to charge this battery. Various physiological parameters are sensed, collected, processed and then forwarded to an access point using the wireless interface. Some of the standard sensor nodes used are Accelerators, Gyroscope, Magnetometer, Temperature sensors, ECG Sensor, EEG Sensor, EMG, EOG and pulse oxy-meter. Accelerators, Gyroscopes and Magnetometers are used for motion detection, monitoring and fall detection. In addition, ECG, EEG, EMG and EOG are used to record physiological parameters used in conjunction with other vital signs to detect various chronic diseases such as heart conditions, respiratory diseases and neurological diseases. It is important that the sensed parameters met the standards of Quality of Information (QoI) standards to ensure that the underlying decisions made using this data regarding the patient's health are reliable, fast and useful.

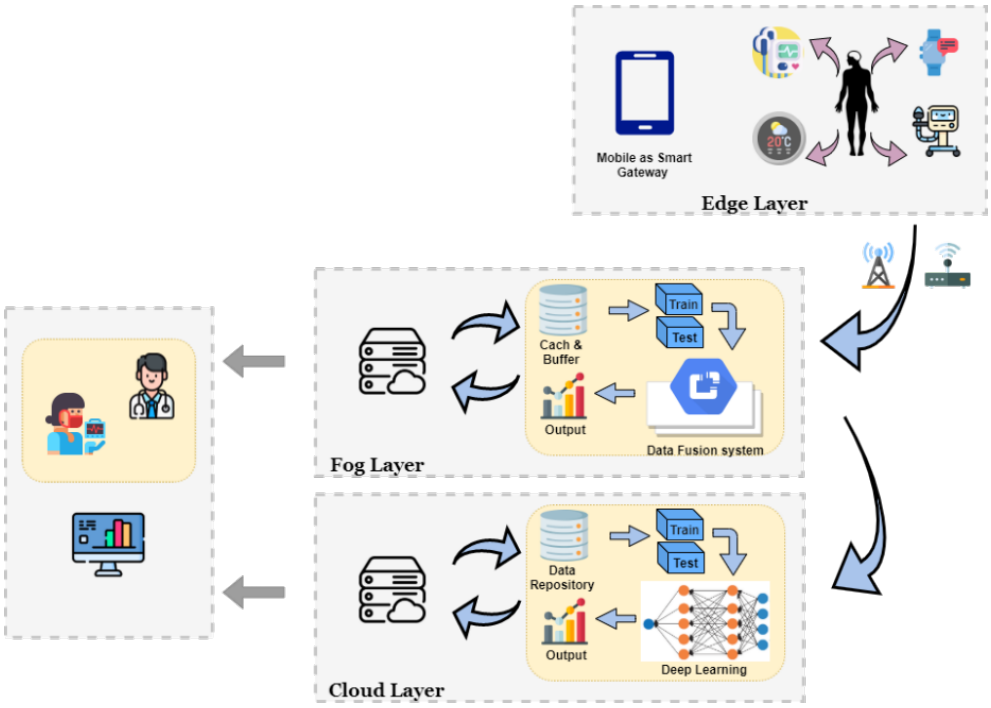

Figure 5. Layered Decision-driven system for healthcare.

2. Fog Layer: All the sensors that are connected in the gateway layer route the data with the help of an IoT gateway. Any type of abnormal sensor data is identified and managed with the help of these gateways. They have the power to identify the format in which the data is transferred across the gateway. They are responsible because any irrelevant piece of data should not travel across the blockchain network at the time of a smart contract in the network layer. Failure of which can result in no, wait for the data in the blockchain. The rejection rate will be very hard for all the information that is not in the prescribed format as required. The network layer connects to all the P2P nodes across the entire blockchain. These nodes are exclusively responsible for providing a backbone towards all the transactions that happens in the Ledger. From the gateway or smart phone application, the sensor data travels with the help of these central nodes and any kind of conflicts are resolved at this level. Once the data is

found, clean and as per the format, the network layer routes the data towards further processing in the Ledger.

3. Cloud Layer: The cloud layer is where IoT is supplemented by the processing and storage capabilities of the cloud. Cloud-level blockchain is necessary to control the interaction. This work aims to design a cloud fog-based model for detecting and monitoring patients of COVID-19 efficiently and in real-time using cloud fog computing. The information of the patient after their constant monitoring and detection of the disease is replicated and broadcasted over the P2P network in the blockchain. This ensures that the correct piece of information goes global and the analytics and research which are required to be done for any specific disease are executed without any hindrances. It must be noted that all three layers execute at different level in the P2P network to provide a properly processed block of data. This framework consists of three levels: sensing level, fog level and cloud layer. Regarding the sensing level, it consists of a variety of sensors, such as sensors/medical devices on/inside the body, that can measure health-related data (measure vital signs) and carry out the acquisition, analysis and forwarding of essential data to highly computerized, dedicated servers (fog and cloud servers).

4.2.2. Bottom-Up Decision-Making Approach

Fog and edge computing have been introduced to mainly deal with the problem of latency in IoT systems [23]. Latency becomes highly critical in terms of healthcare application. This higher latency value can result in various effects such as improper reporting of health status, high value of latency for faults, and improper analysis of the data collected by the sensors and smart gateways; such problems associative with latency can be fatal for patients [24]. Hence, achieving low latency for IoT healthcare systems is an important focus area of research that must be addressed. One of the main reasons for high data latency is the time taken by the cloud layer to process the data. Healthcare systems need on-time or near-real-time transmission and not being able to achieve this can directly affect the healthcare system. The introduction of fog layer that is closer to the sensor nodes results in faster and greater accuracy in data processing and, hence, low latency.

Figure 6, below, shows a three-layered architecture in which the decision making becomes really simple and effective. At the edge level, smartphones or smart gateways are responsible for identifying the information and keeping track of all the sensor data collected from various IoMT devices. At the second layer the decision making is done with the help of fog computing based on the analytics engine. The information received from the edge devices is accumulated and analyzed. This becomes the middle layer for making a decision towards diagnosing a patient's disease. The last and final layer is a cloud-based service provided by the cloud service provider in its IoT hub. The analytics service, which are regulated by the cloud and IoT Central, tends to identify and analyze the information coming via Internet from the edge devices and the process to fog layer. The three level hierarchy assures that an accurate result is predicted for the patient illness and proper diagnostic is provided. Once the results are identified and the information is calibrated, the output is sent to the stakeholders, such as the hospital or a doctor and a copy of the same is propagated further in the form of a block. The smart contract registers the information into the blockchain network and broadcasts the data block over the P2P network. This reduces the probability of a fault occurring at any level.

Apart from that, the sensor nodes are usually bandwidth- and resource-constrained and sending the data directly to the cloud is a power intensive process. Fog and edge computing address this problem by serving as intermediate layers close to the sensor nodes and with greater bandwidth and resources which are better suited to interacting with the cloud layer. The objective of this work is to design a cloud fog-based model for decision-making efficiently and in real-time using a smartphone as smart edge for IoT devices, fog computing and cloud computing. This framework consists of three levels in

which decision-making takes place: Reception/Sensing level in edge level, Fog level and Cloud/Data-center level, as shown in Figure 6 above.

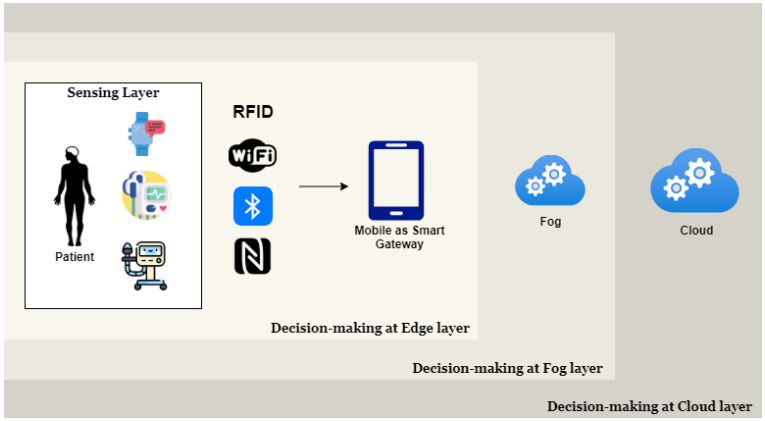

Figure 6. Bottom Up Decision Making.

4.2.3. Decision Making at Edge Layer

Decision making at the edge layer works as per the Figure 7 below in the proposed model. The advanced smartphones are well-established as they have multiple built-in sensors, such as WiFi, Bluetooth, RFID, NFC, etc. Given the power of smartphones, they can play a vital role as a smart gateway (smart edge computing) for IoT systems. All IoT devices collect the patient's medical information or any other type of information that is specific to the patient and it is pushed to the smart gateway (smart phone) acting as the edge layer.

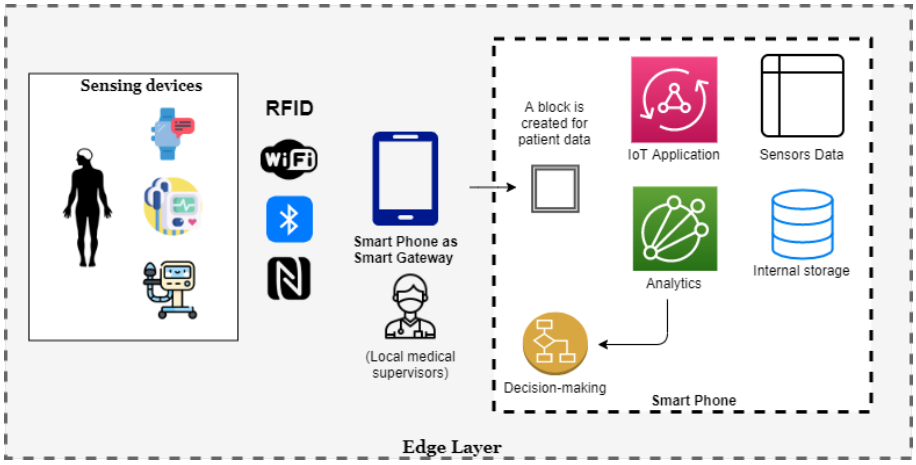

Figure 7. Components for Edge Layer decision making.

4.2.4. Decision Making at Fog Layer

For the bigger data that need more computation, which cannot be processed at the edge layer, the decision-making will move up to the Fog layer as data processing requires a higher level, a high-performance computer that acts as a smart gateway to blockchain in the upper layer. We have already discussed above that, due to the small size and limited functionality of the sensor-based IoT devices, their computational power, along with memory storage, is limited [22]. Thus, each patient will have a blockchain so that all the patient's IoT data will be integrated into the patient's own blockchain. The gateway in the fog layer is responsible for access to part of the sensors as per Figure 8 below. The network layer is responsible for storing all the transactions that take place in the blockchain. The selection of the main node and the broadcasting of information to all the peer nodes

in the P2P network is handled with the help of the network layer to provide the complete functionality in the Ledger.

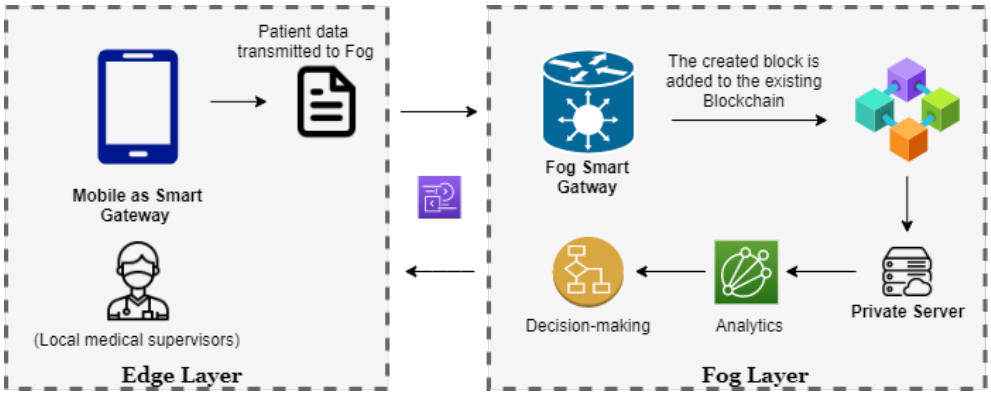

Figure 8. Components for Fog Layer decision making.

4.2.5. Decision Making at Cloud Layer

This is the upper layer, where the Internet of Things is supplemented by the processing and storage capabilities of the cloud. Figure 9 above represents the scheme in which decision making is done at Cloud Level. Reference [26] suggested a novel algorithm for the decision making with neural network and deep learning. Reference [28] suggested the design of a Smart and Secured Healthcare Service blockchain with the use of Deep Learning. Similar algorithm can be applied the module here as well. In the model proposed, the cloud central IoT is responsible for receiving the data from the edge gateway devices. These devices convert the data from sensors and IoMT devices from a raw format to the cloud central hub generic data format. The database of the information resides in the cloud where the information is processed for the decision making. The artificial intelligence service for image processing or data analytics in the smart cloud gateway assured that the data is analyzed and the final commit at the server takes place. This database receives all the information from the fog gateway devices and, after the decision making is completed, then the final data-block is synchronized at the blockchain level.

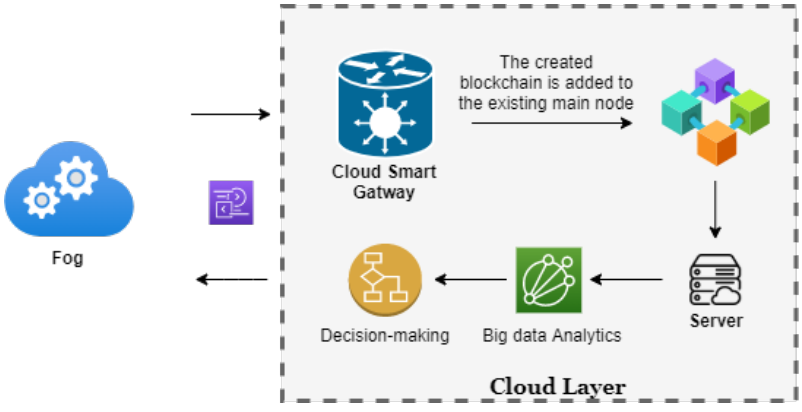

Figure 9. Components for Cloud layer decision making.

5. Experiment and Observations

The experimental setup for this study makes use of IoMT devices, IoT Hub, Cloud Service Provider, Field Gateway devices, Edge Gateway Devices, Analytic Services, and blockchain network formation with smart contracts.

IoMT Devices: the main emphasis in this study is on the detection of COVID-19. In order to identify the virus and verify whether the patient is suffering from this chronic disease, X-ray data-sets were taken from smart gateway devices. The result, which is given

by these data-sets, was analyzed with the help of deep learning algorithms and TensorFlow analysis using Keras framework.

Azure IoT Hub: Azure IoT Hub is a service which can be used to enable the communication between millions of IoT devices. It is a managed service that provides access of the bidirectional flow of information with the help of protocols such as HTTP, AMQP and MQTT. It is very effective to practically monitor and maintain the use of any type of IoT device connected across the network. It also available as easy to use SDK in various languages such as C#, C, Node.JS, etc. In the simplest case of cloud-based IoT solution, the IoT devices send data directly to the cloud and the IoT data persists there. However, it is not possible to manage the IoT data all the time in the cloud. Sometimes there is a requirement for a quicker response, possibly a near-real-time response, especially for critical applications. For these applications, the high latency of the cloud applications can prove to be highly detrimental for the end users as it results in increased response times. Edge computing helps move the computing capability closer to the data source. This results in the movement of workloads from the cloud to the edge which in turn resolves the problem of latency and response times.

Apart from offloading the computing, edge devices also provide the advantage of deploying artificial intelligence near to the data source. Machine learning models can be trained in the cloud and then deployed in the edge. IoT Edge also enables offline operations and enhanced security for IoT applications. Any IoT application implemented using the cloud has three major parts. All the devices which collect data from sensors are plugged inside the network directly or indirectly with the help of a field gateway. The edge intelligence is imparted to these devices that are connected to the gateway. The transportation of the data packets which are not in proper format is restricted at the back-end of the device and local-level decision-making is done at the edge level. The four key concepts that are available in edge computing relative to the connectivity and transportation of the information from the sensor devices to the central hub are:

1. For all the devices having a valid device ID and IP address, direct connectivity is provided to the cloud gateway.
2. For the devices that follow certain industry standards and are used for transferring information from a range of existing technologies such as BLE or ZigBee [25], the connectivity is provided with the help of a field gateway. These devices need to be registered once before they are enrolled in the transaction processing system at Ledger level in the blockchain.
3. Some devices require the installation of specific device drivers or consensus protocols translations that empowers them to be used in the communication network. These devices, after proper installation of the protocol, can be used with the help of a customized cloud gateway to send the transaction or information from one point to another.
4. The connectivity to other devices is approved and provided with the help of a field gateway or any other custom cloud gateway. This enables the manual installation and approval system to handle all such devices inside the broadcasting network.

5.1. Field Gateway

An edge device, sometimes also termed as Field Gateway, is a special type of device which is used to act as a medium responsible for communicating from a local control system to a centralized data processing hub. These devices are usually capable of processing a small amount of data with a limited computation capability and submitting the desired format of the data to a centralized cloud store or a data hub. One of the most important features for these devices concerns the processing of the data which is recorded by the censors in a prescribed format, which is required to be processed at higher end. All the devices that are connected to such a field gateway are usually well defined with the protocol suit and the data headers, which is required for transaction processing at the Ledger. The management of access and the information flow at this level is not the same as it used to be

in a traffic router. The provisioning of the devices, filtering of the information and the data, batch processing, aggregation, buffering of the information, resolution of the protocol for communication and transport, and final processing at various event levels are some of the functions that are associated with these field gateways. Azure IoT Edge is recommended to be used as one of the field gateways for processing all the transactions and collecting the information from various sensor-level devices from the edge layer.

5.2. Cloud Gateway

The communication between various edge devices which are available at different potential locations is accomplished with the help of cloud gateway. The information that flows from various edge devices is transferred over the Internet or a network virtualization overlay to these cloud gateway devices. All the attached edge-level devices can send information processed at their end to the cloud gateway for further processing and analytics. The communication between the devices, connection management, protocol variations, data protection at communication level, device authentication and identity access management is done at cloud gateway level. The data which comes from various edge level devices to the cloud gateway are finally processed with the help of computational services available at the cloud gateway.

5.3. AI Powering the Edge Computing

Edge computing is now being reinvented with technologies such as IoT and AI, which bring added value to healthcare outcomes, thus reducing workloads and optimizing networks and services to improve health outcomes. In the new data era, the dependence on internet-connected medical devices will be increasing, hence making edge computing a key technology for healthcare systems. Figure 10 below represents various departments in the hospital/healthcare unit comprising their own edge gateways. These devices are small computational units, which are capable of performing a certain specific task and streaming the information on the Internet. They can be called IoMT devices at the edge gateway. From various departments, information goes to the hospital cloud or data centre. This information is analyzed with the power of artificial intelligence to give the edge-level inferences and results. This accounts for the first layer of execution in the proposed model in this study. There can be several other departments as well, which can share the information related to a patient disease or analysis. All the information collectively comprising of a registered patient ID is submitted from registered devices. It becomes the duty of the edge gateway to assure that the information submitted from each and every machine for a particular patient ID is in a proper format and ready to be analyzed with the help of the adaptive artificial intelligent analysis engine.

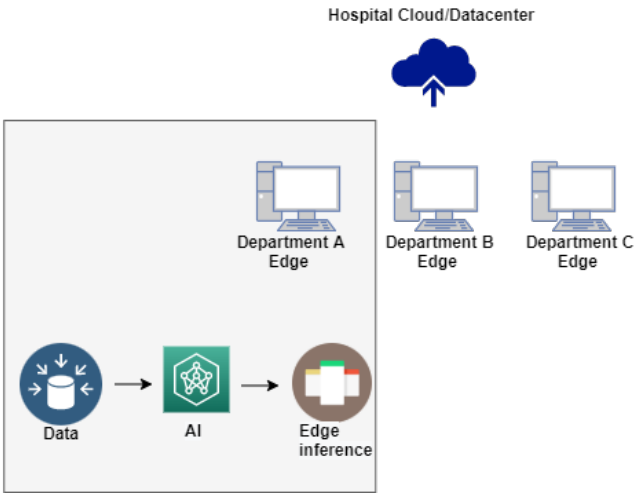

Figure 10. Healthcare Facility using AI for Decision Making.

5.4. Hardware and Software

During the development of techniques for the analysis and detection of COVID-19, we used deep learning approaches and TensorFlow and Keras libraries for the X-ray data-set, but, as we know, it required a large amount of the data-set for the training of models, so we used Image Data Generator techniques, which helps to increase the data volume and is sufficient to train the deep learning models. We used CNN and Dark-net Algorithms for the large amount of data. When we used the "Image Data Generator" approaches, which has a few features such as re-scaling the images, sheering images, zooming in on or out of images and horizontally flipping the images. It gives a very large volume of images. We used TensorFlow and Keras libraries for the deep learning model executions. In this technique, we used the few images for the testing and used already-trained models for the same data-set. Due to the small data-set, we did not require any high-specification system, we used our laptop to execute the whole code and test the model as well.

1. Hardware: PC (RAM 32 GB, SSD 1 TB), Intel(R) Core (TM) i9-9900k CPU, Dual NVIDIA Ge-Force RTX 2070 SUPER;
2. Software: Anaconda using Jupiter Notebook. Lighter libraries to use deep learning concepts.

As per the experimental setup, the analysis of information was done with the help of software programs performing deep learning analysis. The power of artificial intelligence is to help to predict the nature of the disease which a patient might be suffering.

Figure 11 below shows the graphical representation of the training accuracy and test accuracy, which are high and prove that it is a good model. We set 100 epochs and obtained very low values against training loss and test loss. The analysis is done for four different types of parameter and the findings are identified as below.

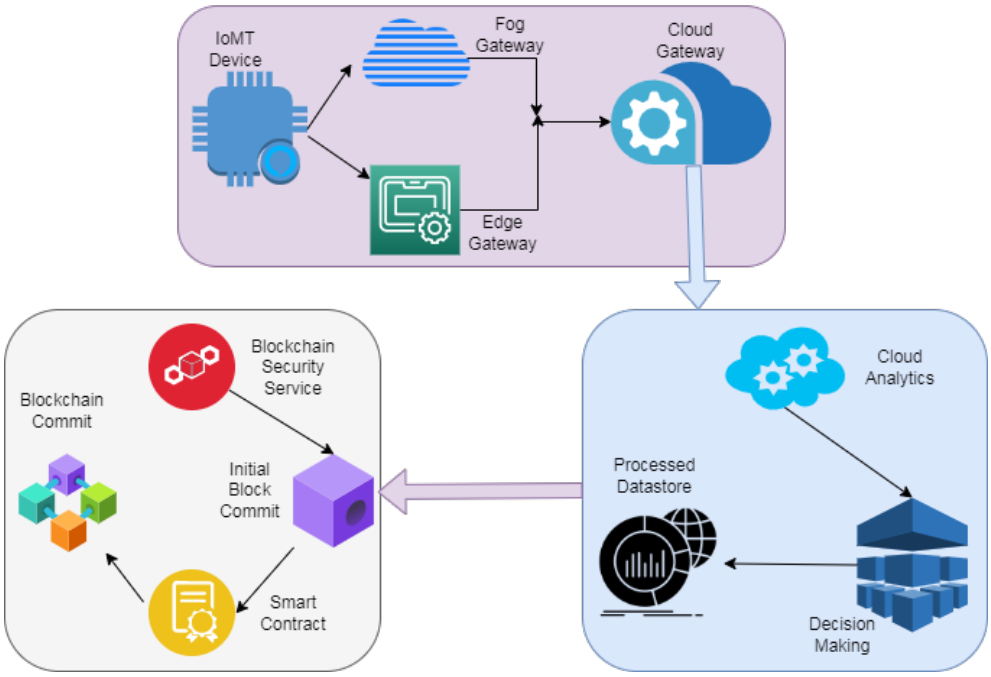

Figure 11. Proposed System Flow Design.

This metrics in Figure 12 below show the evaluation values to train the model for 100-image data, which show the best values. These images are taken from IoMT devices. The analysis of the image values was done with the help of AI-powered algorithms. Keras and Anaconda were used to analyze the data-set.

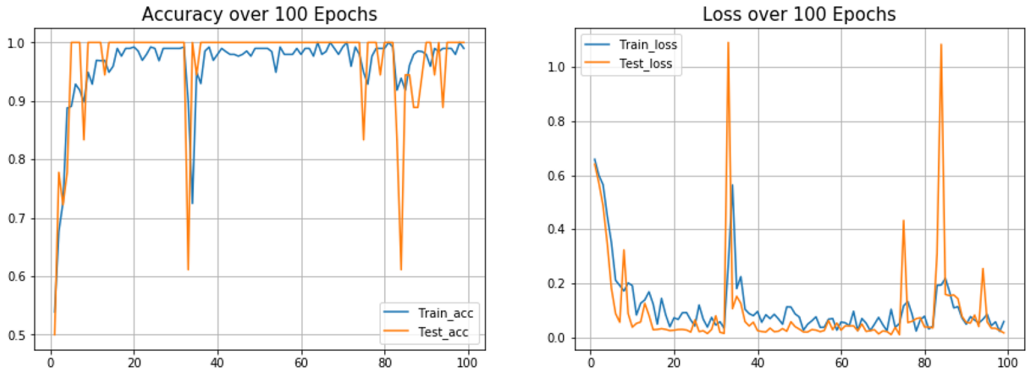

Figure 12. TensorFlow Analysis results for X-ray data-sets.

After the analysis is completed for all the images in the data-set (Figure 13), it is identified that 10 and 30 images give the maximum evaluation metrics values. This observation is important, as it can predict the nature of a disease that a patient might be suffering from. In this case, the accuracy increases after 30 images in the analysis engine. There is no 'Image Generator or Augmentation' applied because we have only a few images' data. The model is already trained and we used the previously trained models during the testing of models, such that when we pass any image for the testing, first it calculates the feature vector and then compares it with the trained models. We used the CNN model including the VGG16 flavor with deep learning libraries such as TensorFlow and Keras. We did not use the Fastai.vision library here because it takes a very large number of computations and it is useful for large amounts of data, and for training purposes only. Figure 14 below shows that larger data-set or observations from the IoMT devices results in better accuracy.

	precision	recall	f1-score	support
Covid-19	1.00	0.88	0.93	24
No_findings	0.97	1.00	0.99	101
micro avg	0.98	0.98	0.98	125
macro avg	0.99	0.94	0.96	125
weighted avg	0.98	0.98	0.98	125

Figure 13. Best Evaluation value Metrics for data-sets.

	precision	recall	f1-score	support
Covid	1.00	1.00	1.00	20
Normal	1.00	1.00	1.00	20
accuracy			1.00	40
macro avg	1.00	1.00	1.00	40
weighted avg	1.00	1.00	1.00	40

Figure 14. Maximum Evaluation value Metrics for data-sets.

We set parameters such as only using 10 epochs, and used dropout libraries to shorten the execution time.

Figure 15 is a graphical representation that aims to provide the detail about the three trained data-sets. Time elapsed is measured in minutes. Once we have completed the analysis at the edge level and cloud level, the information which is finally analyzed is

reported back to the main stakeholder. In the proposed model, the first organization comprises of the healthcare unit and the second organization belongs to the patient whose diagnostics reports are generated. The IoT Central hub, after the final analysis of the information, sends the processed data to the blockchain network.

Figure 15. Accuracy for decision making increase with data-set size.

In the experimental setup, we have deployed our own hyperledger fabric at the local network. The docker images from the Figure 16 below shows that, inside the test network, two organizations are trying to communicate with each other. These organizations can vary depending upon the nature of blockchain established between them. The hyperledger fabric makes it possible for the two peers to accept smart contract between them. When the analyzed data block is finally ready to be deployed in the blockchain network, smart contract is floated in the docker images for both organizations to accept. As soon as the organization accepts the smart contract, the data block comprising the final analytic of the patient history and information is submitted on the blockchain network to all the nodes.

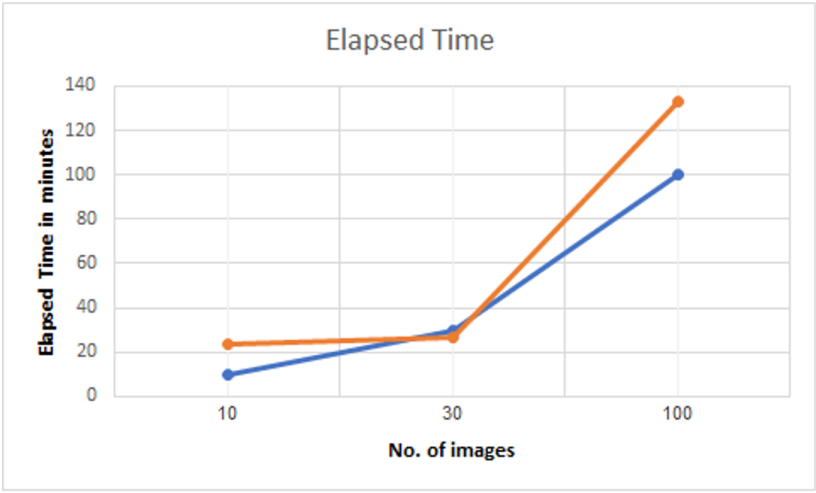

Figure 16. Elapsed time for three trained data-sets.

Figures 17 and 18 below show the console results after the two parties accept the Smart Contract in the prototype model in the test network. This makes it possible for the P2P network to accept the data block for a registered patient ID. The information inside the data block is valid and close across the network from registered IoMT devices. This type of communication makes it very simple for the healthcare unit to make use of valid and authentic information. At the same time. The privacy of the user whose information is propagated across the P2P network is also maintained.

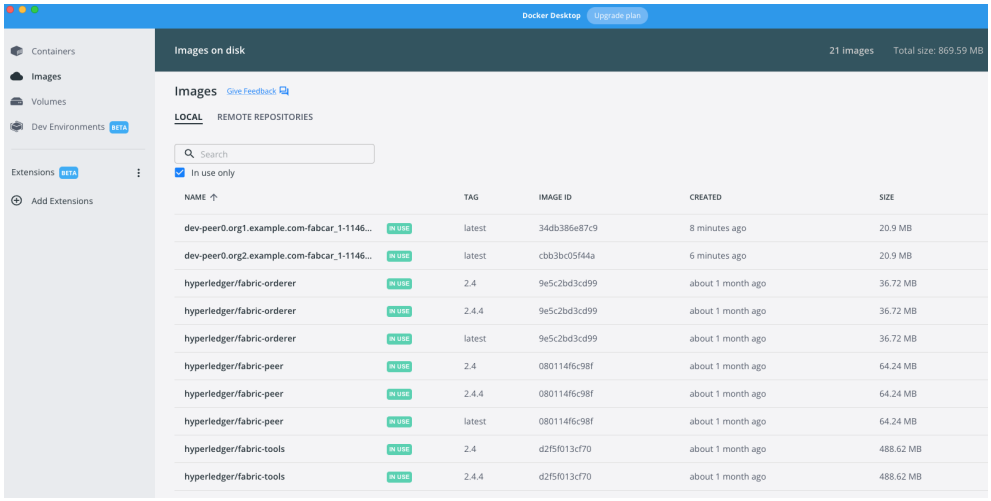

Figure 17. Docker Images for the Hyperledger Fabric running to provide Smart Contracts.

```
Package ID: fabcar_1:1146b4b491871bf18b23dd67dd8cc058655b36cc0e2274f165ed06b796a8f276, Label: fabcar_1
CCITs-iMac:test-network ccit$ $ CC_PACKAGE_ID=fabcar_1:1146b4b491871bf18b23dd67dd8cc058655b36cc0e2274f165ed06b796
a8f276
-bash: $: command not found
CCITs-iMac:test-network ccit$ CC_PACKAGE_ID=fabcar_1:1146b4b491871bf18b23dd67dd8cc058655b36cc0e2274f165ed06b796a8
f276
CCITs-iMac:test-network ccit$ peer lifecycle chaincode approveformyorg -o localhost:7050 --ordererTLSHostnameOver
ride orderer.example.com --channelID mychannel --name fabcar --version 1.0 --package-id $CC_PACKAGE_ID --sequence
 1 --tls true --cafile ${PWD}/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tls
cacerts/tlsca.example.com-cert.pem
2022-07-23 14:11:03.614 +03 0001 INFO [chaincodeCmd] ClientWait -> txid [5a5760c10342b7c86076f73d0006031f80587f94
5dbd6a4e4e4761a39b4b8cee] committed with status (VALID) at localhost:9051
CCITs-iMac:test-network ccit$ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name fabcar -
-version 1.0 --sequence 1 --tls true --cafile ${PWD}/organizations/ordererOrganizations/example.com/orderers/orde
rer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem --output json
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": true
        }
}
```

Figure 18. Acceptance of the Blockchain smart contract for final commit.

6. Conclusions

In the proposed architecture. we have presented a methodology with the help of which we can integrate the power of blockchain to impart security and privacy for patients' data. These data can be collected over various IoMT devices and submitted with the help of fog and edge computing gateways. These devices dress the data to be used by the cloud computing gateway. The information reaches the IoT central hub at the Cloud Service Provider. Finally, when the information is analyzed and predictions are made for the patients' ailments, the data block is received. Once the results are fetched, the data block of the results along with the patient's information is created. The information from this data block is submitted to the blockchain security service to create the hash information and processing of the smart contract takes place. We have created a test network to identify and test smart contract sharing between two peer nodes. Once the smart keys are exchanged between the nodes, the block of data is shared on the P2P network in the form of a decentralized data block. One of the main motivating factors for the creation of this model is to identify and use the power of blockchain towards the security of patient data and managing the privacy of the information. Our test network gave us the results where the smart contracts were exchanged by the two nodes. It is also worth mentioning that we have taken a data set on X-ray images for COVID-19 patients and we tend to analyze them with the help of the cognitive service of the cloud service provider. The decision making is done with the help of machine learning algorithms provided by the cloud services and the final results are also included in the form of graphs in the manuscript. Overall, the model proposes a very strong and Secure Framework that can help to handle the information of a patient in the blockchain, providing security and privacy.

Author Contributions: Conceptualization, W.A.S.; software, R.M.; validation, K.A.; formal analysis, K.A.; investiga-tion, N.J., N.A.K.; resources, J.A.; data curation, S.M.A.; writing—original draft preparation, N.A.K.; writ-ing—review and editing, N.A.K.; visualization, W.A.S.; supervision, S.M.A.; project administration, R.M.; funding acquisition, J.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the Deanship of Scientific Research at Shaqra University for supporting this work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chiuchisan, I.; Costin, H.-N.; Geman, O. Adopting the internet of things technologies in health care systems. In Proceedings of the 2014 IEEE International Conference and Exposition on Electrical and Power Engineering (EPE), Iasi, Romania, 16–18 October 2014.
2. Asghar, M.H.; Negi, A.; Mohammadzadeh, N. Principle application and vision in Internet of Things (IoT). In Proceedings of the 2015 IEEE International Conference on Computing, Communication & Automation, Luxembourg, 8–11 September 2015.
3. Darshan, K.; Anandakumar, K. A comprehensive review on usage of Internet of Things (IoT) in healthcare system. In Proceedings of the 2015 IEEE International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India, 17–19 December 2015.
4. Janbi, N.; Katib, I.; Albeshri, A.; Mehmood, R. Distributed artificial intelligence-as-a-service (DAIaaS) for smarter IoE and 6G environments. *Sensors* **2020**, *20*, 5796. [CrossRef] [PubMed]
5. Verma, P.; Sood, S. Fog assisted-IoT enabled patient health monitoring in smart homes. *IEEE Internet Things J.* **2018**, *5*, 1789–1796. [CrossRef]
6. Kshetri, N. Can blockchain strengthen the internet of things? *IT Profess.* **2017**, *19*, 68–72. [CrossRef]
7. Randall, D.; Goel, P.; Abujamra, R. Blockchain applications and use cases in health information technology. *J. Health Med. Inform.* **2017**, *8*, 8–11. [CrossRef]
8. Dautov, R.; Distefano, S.; Buyya, R. Hierarchical data fusion for smart healthcare. *J. Big Data* **2019**, *6*, 1–23. [CrossRef]
9. Joyia, G.J.; Rao, M.; Liaqat, A.F.; Rehman, S. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* **2017**, *12*, 240–247. [CrossRef]
10. Alshahrani, S.-M.; Jeeva, S.C.; Rajsingh, E.B. URL Phishing Detection Using Particle Swarm Optimization and Data Mining. *CMC J.* **2022**, *73*, 5625–5640.
11. Zhang, B.; Kraska, T. The Cloud is Not Enough: Saving IoT from the Cloud. In Proceedings of the 7th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 15), Santa Clara, CA, USA, 18 May 2015.
12. Zhou, L.; Wang, L.; Sun, Y.; Lv, P. Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation. *IEEE Access* **2018**, *6*, 43472–43488. [CrossRef]
13. Jan, M.A.; Cai, J.; Gao, X.-C.; Khan, F.; Mastorakis, S.; Usman, M.; Alazab, M.; Watters, P. Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *J. Netw. Comput. Appl.* **2021**, *175*, 102918. [CrossRef]
14. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* **2019**, *5*, 1–7. [CrossRef]
15. Schulz, P.; Matthe, M.; Klessig, H.; Simsek, M.; Fettweis, G.; Ansari, J. Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture. *IEEE Commun. Mag.* **2017**, *55*, 70–78. [CrossRef]
16. Bormann, C.; Castellani, A.P.; Shelby, Z. Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67. [CrossRef]
17. Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* **2021**, *172*, 102–118. [CrossRef]
18. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017.
19. Katib, A.F.M.R.; Albogami, I.; Albeshri, N.N.A. Data fusion and IoT for smart ubiquitous environments: A survey. *IEEE Access* **2017**, *5*, 9533–9554.
20. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. *Blockchain Technology Overview*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
21. Niranjanamurthy, M.; Nithya, B.; Jagannatha, S. Analysis of Blockchain technology: Pros, cons and SWOT. *Cluster Comput.* **2019**, *22*, 14743–14757. [CrossRef]
22. Mukhopadhyay, S.; Suryadevara, N. *Internet of Things: Challenges and Opportunities;* Mukhopadhyay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–17.

23. Anawar, M.R.; Wang, S.; Azam, M.Z.; Jadoon, A.K. Fog computing: An overview of big IoT data analytics. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1–22. [CrossRef]
24. Lyu, L.; Jin, J.; Rajasegarar, S.; He, X.; Palaniswani, M. Fog-empowered anomaly detection in IoT using hyperellipsoidal clustering. *IEEE Internet Things J.* **2017**, *4*, 1174–1184. [CrossRef]
25. Alsulami, M.H.; Atkins, A.S.; Alaboudi, A.A. ZigBee Technology to Provide Elderly People with Well-Being at Home. *Int. J. Sens. Wirel. Commun. Control* **2021**, *11*, 921–927. [CrossRef]
26. Aitizaz, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors* **2022**, *22*, 572.
27. Dammak, B.; Turki, M.; Cheikhrouhou, S.; Baklouti, M.; Mars, R.; Dhahbi, A. LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring. *Sensors* **2022**, *22*, 1497. [CrossRef]
28. Mohanty, M.D.; Das, A.; Mohanty, M.N.; Altameem, A.; Nayak, S.R.; Saudagar, A.K.J.; Poonia, R.C. Design of Smart and Secured Healthcare Service Using Deep Learning with Modified SHA-256 Algorithm. *Healthcare* **2022**, *10*, 1275. [CrossRef] [PubMed]
29. Bataineh, M.R.; Mardini, W.; Khamayseh, Y.M.; Yassein, M.M.B. Novel and Secure Blockchain Framework for Health Applications in IoT. *IEEE Access* **2022**, *10*, 14914–14926. [CrossRef]
30. Ahmed, I.; Zhang, Y.; Jeon, G.; Lin, W.; Khosravi, M.R.; Qi, L. A blockchain-and artificial intelligence-enabled smart IoT framework for sustainable city. *Int. J. Intell. Syst.* **2022**, *37*, 6493–6507. [CrossRef]
31. Alwakeel, A.M. An overview of fog computing and edge computing security and privacy issues. *Sensors* **2021**, *21*, 8226. [CrossRef]
32. Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 2088–8708. [CrossRef]
33. Epiphaniou, G.; Pillai, P.; Bottarelli, M.; Al-Khateeb, H.; Hammoudesh, M.; Maple, C. Electronic Regulation of Data Sharing and Processing Using Smart Ledger Technologies for Supply-Chain Security. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1059–1073. [CrossRef]