PAKISTAN JOURNAL OF EMERGING SCIENCE AND TECHNOLOGIES (PJEST)

December, 2022, 3(2) ISSN 2788-8630 (On-Line)

RESOLVING SMART HEALTH SECURITY ISSUES USING ONTOLOGIES AND BLOCKCHAIN SERVICES

ZAHIRA ILYAS[1], MUHAMMAD IMRAN TARIQ[1], SYED KHURRAM SHAHZAD[2], RUKHSANA ABDUL KARIM[1]

[1] Department of Computer Science, Superior University Lahore 54000 Pakistan,

[2] Department of Computer Science, University of Management Technology Lahore 54000 Pakistan,

*Correspondence: rukhue@gmail.com

ARTICLE INFORMATION

Crossref DOI:

https://doi.org/10.56819/pjest.v3i2.74

Received: 30th Nov-2022

Revised and Accepted:

25-December-2022

Published On-Line

21st -January-2023

***Corresponding Author:**

Rukhsana Abdul Karim

rukhue@gmail.com

Original Research Article

ABSTRACT

IoT is one of the most commonly used and emerging technology. It has been used for resolving many issues in daily life. In this paper, we are going to address the security issues in smart health and how we can resolve them by using blockchain technology. Blockchain is evolving rapidly which deals in blocks of data. By using this attribute, we can partially grant access to data to a specific user by identifying their roles in that certain activity. Although there are already many derived solutions by other researchers we will follow the combination of RFID and EHR techniques of blockchain to propose a better solution to solve this security challenge.

Keywords: IoT, Smart Health, Blockchain, Security Issues, Internet of Things, RFID, EHR, Ethereum

Introduction:

The development of the Internet of Things [IoT] has been driven mainly by the needs of large enterprises. Large enterprises will greatly benefit from the anticipation and predictability that comes from the ability to track all objects through the commodity chains to which they are anchored. Mark Weiser said in a critical article in Scientific American (1991) with the advent of IT and his IoT know-how, people's daily lives and working circumstances in organizations have changed a lot. This idea has multiple uses, making it a well-known idea in many horizontal and vertical markets, including the daily lives of ordinary people in society [1]. The ability to encode and track substances has allowed organizations to become more active, speed up methods, reduce errors, prevent theft, and integrate complex and flexible organizational systems through the IoT [2]. The Internet of Things is a technological disruption that represents the future of production and telecommunications, and its development relies on dynamic innovation in many key areas, from wireless sensors to nanotechnology [2].

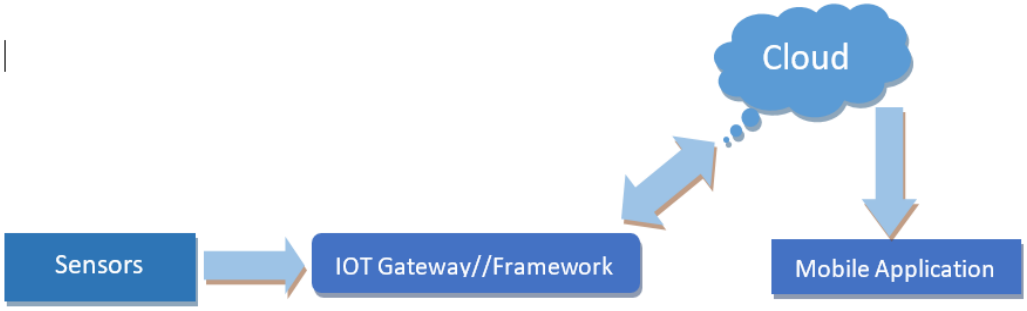

Fig. 1: IoT architecture adapted from [3]

The diagram above shows how data is sent through a gateway using sensors and stored in cloud storage. The user can use sensors to update doctors, check their health status, and store this data in her Smart Health Services in cloud storage. In this modern age, intelligent health is an integral part of our lives. Unfortunately, our rapidly growing population is one of the most alarming conditions that can lead to chronic health problems and illnesses that can overwhelm modern healthcare systems. Similarly, the demand for qualified doctors, beds, and nurses is also very high [8]. In this particular scenario, IoT is widely recognized as a potential solution to reduce pressure on the healthcare system, so further advances in this technology are being researched. Advances in information technology have benefited many fields such as medicine, logistics, transportation, and agriculture. With ongoing data segmentation, real-time analytical processes, and efficient decision-making, this technology has the potential to improve everyday life around the world in many ways [9]. The most important element of IoT is the ability to place sensors anywhere to collect data from patients. But the main problem after collecting patient data is protecting it from unauthorized access. Advances in home health care are also due to the application of ambient intelligence and artificial intelligence [10]. The combination of modern sensor equipment and advances in data processing technology and wireless networks are leading to the development of a digital. An environment that evolves our daily lives.

Problem Statement

This white paper presents a solution for keeping patient data confidential so that not any unauthorized person can access this data. In addition to security, medical services must be error-free and complete. Follow well-defined IoT-based rules and regulations for data quality levels [11]. Advances in IoT technology have changed many things. Just as patients with chronic or critical illnesses have implanted or superficial medical nodes that can provide eHealth IoT network services. In this way, complex physiological data is collected via the internet into a gateway to the patient's device. This is how a patient's Electronic Health Record (EHR) is managed [12]. We can elaborate on the internal architecture of health services in the following diagram

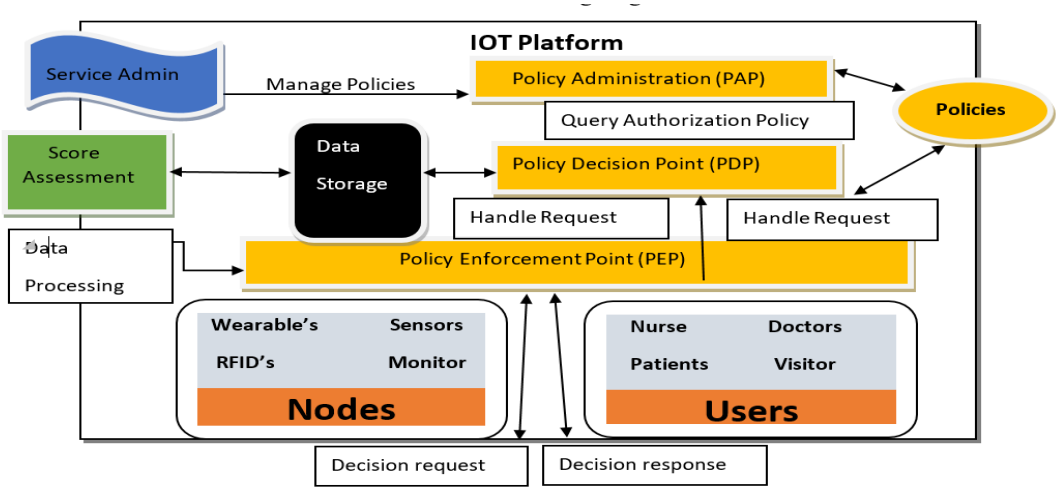

Fig. 1: Architecture of Health services adapted by [11] Problem Statement

In this current scenario, the most common and extensively researched area in the field of IoT is smart health services. But even though a lot of work has been done on this but still there is a need for a lot of improvements and changes. Just like

- Support
- Maintenance
- Lack of Physical Device Security
- Lack of encryption
- Lack of user Level Security

Smart health services deal with most private and confidential data of the patient and there are several security issues regarding that data as everyone wants to prevent that data from the access by an unauthorized person. The most highlighted flaws are

- Lack of data integrity
- Less data security

Blockchain is one of the best services used to solve this problem in smart healthcare infrastructure. This technology adequately solves this problem from a privacy and security perspective. A block is a secure and reliable technology, basically a decentralized, decentralized, shared, constant database that carries vast amounts of data and records assets and transactions in a peer-to-peer network. Store [13]. Blockchain services store all previous data, making it available worldwide without compromising security concerns. There are two types of blockchain services: permissioned and permissionless[2]. Permissioned blocks stored all private data that could be kept more secure using this blockchain feature. Permissionless, on the other hand, is a block that requires no security, and the data it contains is intended for the general public. Elliptic curve cryptography is a technology used in blockchain and SHA-256 hashing that provides strong cryptographic proof of data integrity and security. As we discussed security issues for smart health services, in this particular situation, blockchain technology, and its capabilities can be implemented in smart health systems. This keeps your data more private and away from hackers.

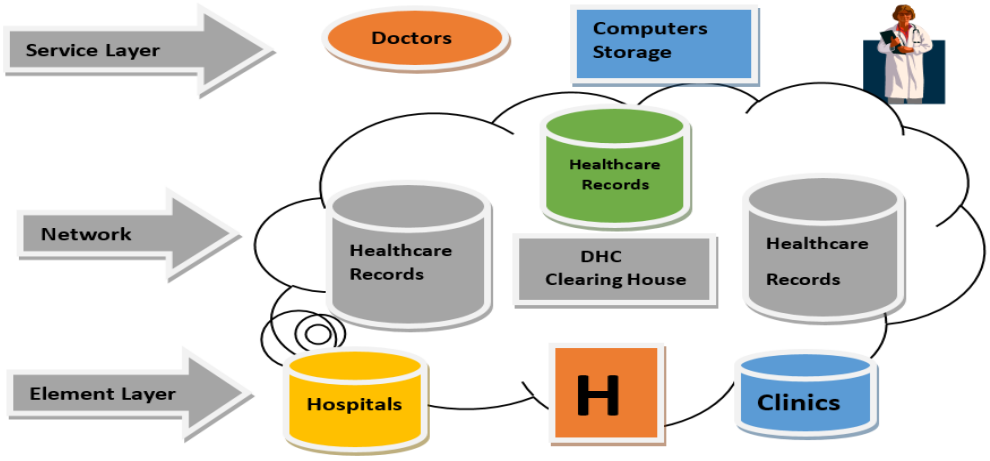

Fig. 2: Smart Healthcare Architecture adapted by [16]

The application architecture of smart health can be defined clearly in terms of a diagram that clarifies the rest of the things about the working of IoT.[15]

Literature Review

In 1991, Mark Weiser outlined a vision for the future of the Internet under the name "ubiquitous computing". Through this vision, he focused on how to achieve the brilliant and sane state of mobile phone innovation to create a breakthrough media framework. Kevin Ashton is one of the pioneers in discussing IoT. As reported by Atzori A.lera et al. Specifically, IoT is characterized by three of his standards in particular: I) web deployed (middleware), ii) deployed (sensors), iii) semantically deployed (knowledge). Neil Gershenfeld of the Massachusetts Institute of Technology's MIT Media Lab says something similar in his 1999 book When Things Start to Think. In 1999, the Auto-ID Lab and MIT created the Electronic Product Code EPC, an attempt to use RFID to recognize things on the system. From 2003 to 2004, companies such as Cool Town, Internet, and Disappearing Computer activities began to develop, and IoT suddenly appeared in the title of a book. RFID is being widely deployed by the US Department of Defence. In 2005, IoT entered another level when the first report was released from the International Telecommunication Union ITU.

In 2008, various people from organizations such as Cisco, Intel, SAP, and more than 50 people came together to form the IPSO Alliance to promote the use of Internet Conventions (IP) and implement IoT ideas. In 2008-2009, IoT was "designed" by the Cisco Internet Business Solutions Group (IBSG). From an earlier perspective, IoT can be seen as an arrangement of great things/questions. Household appliances, mobile phones, personal computers, etc., were all connected via their connection to the Internet and were fed by the extraordinary planning that made them connected. [17]. There has been an enormous exertion as of late to adapt to security issues in the IoT worldview. Some of these approaches target security issues at a particular layer, though, different methodologies go for giving end-to-end security to IoT. An ongoing overview by Alaba arranges security issues as far as application, engineering, correspondence, and information. This proposed taxonomy for IoT security is not quite the same as the traditional layered architecture. The dangers of IoT are then examined for equipment, system, and application segments. Thus, another study by Granjal et al. talks about and examines security issues for the conventions characterized by IoT. The security examinations introduced to talk about and look at changed key administration frameworks and cryptographic calculations, also the creators in focus on a near

assessment of intrusion discovery frameworks. An investigation of security issues for mist processing is displayed. A survey by Sicari et al talks about commitments giving confidentiality, security; get to control, and protection for IoT alongside the security for middleware. The creators talk about trust administration, verification, protection issues, information security, organizational security, and interruption discovery frameworks. For edge registering based ideal models including versatile distributed computing, portable edge processing, and mist figuring, the personality and validation, get-to-control frameworks, organize security, trust administration, adaptation to non-critical failure, and usage of legal sciences are overviewed in [13]. The connections enable things to trade and process metadata, determine significant insight, and respond self-ruling to their condition. In any case, the heterogeneity of things, their abilities, upheld activities, properties, diverse correspondence advancements, and conventions add to the intricacy of viable acknowledgment of the stages [19].

Proposed Process Model

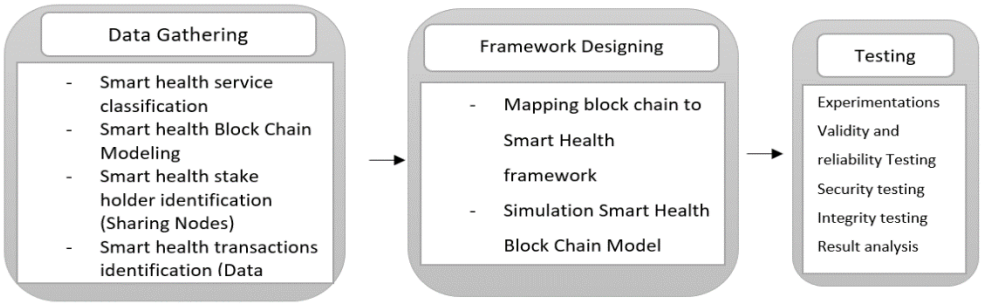

Fig. 4: Proposed Process Model for integrating Smart Health with Blockchain

Methodology

The hottest topic in the application domain in the era of the Internet of Things is intelligent health services, a set of technologies and facilities deployed in this intelligent environment. But there are still flaws that need to be fixed and controlled. IoT emphasizes people's comfort and luxurious life. As long as this era's development goes on, keep going. This research journey will remove all the barriers that are the main reason for the unreliability of smart health environments. This is one of the most important factors when using smart health services, as it allows smart health users to trust the privacy and integrity of their health data when using blockchain. The main purpose of choosing this topic as a research topic is that it helps patients communicate with their doctors without leaving their homes and enables doctors to see multiple patients at the same time, so smart health is very important in this era. is important to If this problem is solved, the smart health trend will rise and the hurdles between users will be removed. The Internet of Things is the most used technology today, especially in the medical field. So, we can say that we are introducing a new framework that solves some security problems, but there are still some problems that need more attention and time to solve [14]. Due to the many benefits of remote well-being monitoring, many scientists see IoT as a potential healthcare solution. Some research has created his IoT social security framework for specific gifts, such as recovery, diabetes management, and assisted living for the elderly (AAL) for older adults, but this is just the tip of the iceberg. It's not too much. These frameworks are intended for broad purposes but are linked through the use of equally empowering advances. Recovery from physical damage is a topic of particular interest to some scholars.

Competency Questions

A framework was created to create a personalized recovery plan according to symptoms. Patient conditions are compared and a database of past side effects, illnesses, and medications is created to accomplish this. The framework requires an expert to physically enter indications and review recommended treatments. In 87.9% of cases, the experts fully agreed with the framework and made no changes to the proposed treatment plan. On the other hand, a numerical model is proposed to measure the joint point of the physical hydrotherapy framework, allowing improvements in joint development that can be tracked through treatment. His IoT advances in the existing evaluate its usefulness in a framework for reviewing patients with Parkinson's disease.

- *CQ1:* How we can make the sharing of data in smart health services more secure and reliable?
- *CQ2:* How we can make sure the element of integrity in the transmission of data of health services?
- *CQ3:* How we can prevent confidential data from unauthorized access?
- *CQ4:* How patient's guardian keeps a check on his/her health conditions?

Their study hypothesizes that wearable sensors that monitor gait patterns, tremors, and general activity levels, combined with vision technology (such as cameras), could be used around the home to monitor the progression of Parkinson's disease. The developers also suggest that machine learning could later lead to improved treatment design. A practical framework for checking blood glucose levels in diabetic patients has been proposed. In this framework, patients are required to physically measure their blood glucose levels at set intervals. From this point on, he thinks of his two types of dysglycemia [49-50]. The first is abnormal blood sugar levels and the second is forgetting to test your blood sugar. The framework at this point will investigate the severity of the fraud and choose who to notify. Patients themselves, parents, relatives, or emergency service providers. B. Specialist. This framework has proven to be realistic and workable but could be further enhanced with automated glucose estimation. The heart attack detection system uses instant segments and a custom wireless cable. was created by an electrocardiogram sensor used to quantify heart movements produced by a microcontroller. This data is sent via her Bluetooth to the customer's mobile phone, where her ECG information is further processed and displayed in a client application.

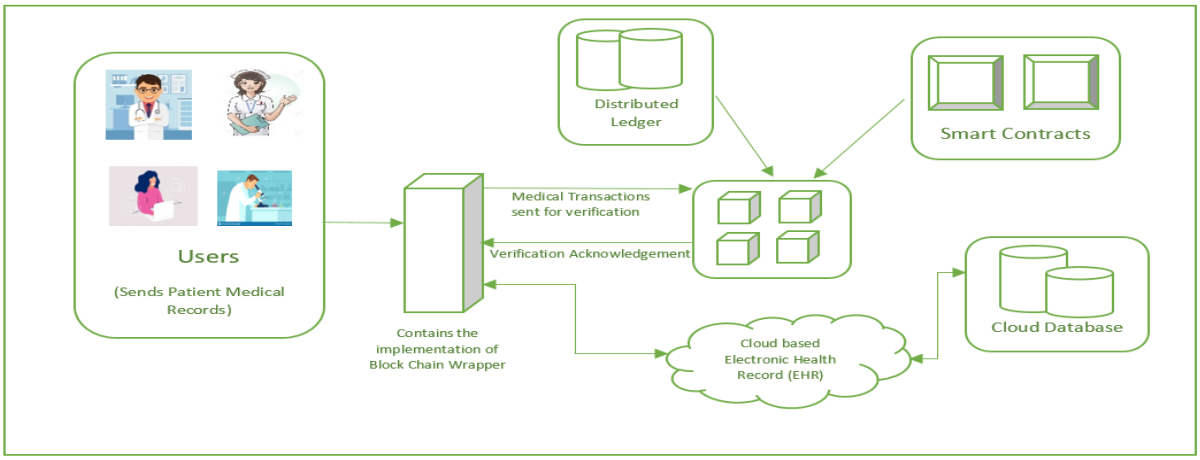

Fig. 5: Architecture of IoT in smart health adapted by [43]

Developers recognize that the framework will be improved by creating a heart attack prediction program. It facilitates improvement by estimating respiratory rate, which is known to help predict heart attacks [8]. Over the past decade, vast urban areas around the world have begun to incorporate innovation into their day-to-day management. These gorgeous urban areas take advantage of cutting-edge advancements in innovation. The United States is a major architect and the healthcare services industry is at the forefront of leveraging these improvements. His use of Electronic Health Records (EHRs) can be traced back to the 1960s. Unfortunately, as technology has advanced, so have how advanced protection and security are compromised [48]. The health services industry in particular is under the spotlight for data theft, as medical records often contain personal information such as patient names, state disability numbers, and addresses. The Health Information Innovations for Economic and Clinical Health (HITECH) Act sought to remedy the inadequate information security of human services, a feature of the American Recovery and Reinvestment Act of 2009 but was not adequate to the problem. could not cope with. In 2015, 78.8 million patients, nearly a quarter of the US population, had their data stolen after the protection company Song of Devotion was hacked. As of June 2017, nearly 2.6 million people had been attacked, according to the U.S. Department of Health and Human Services. 20 Weak security frameworks and regulatory requirements have made EHR theft proliferate. EHRs are typically monitored by private providers. This means that all personal records are stored in a database maintained by the provider responsible for producing the reports. This demonstrates the security, protection, and control issues that smart urban community development needs to address. 25 First, medical practices are known to improperly secure confidential information [24].

Security as Issues

For two a long time, Independent Study Evaporators directed research on the vulnerabilities of healing center security. The gathering could effectively get to and modify the databases of numerous social insurance offices over the United States. Second, because suppliers are exclusively in charge of keeping up the records, information honesty 30 can be hard to affirm if a malevolent element modifies the single duplicate of the record [44].

Blockchain Technology

Blockchain is the technology that was first introduced into Bitcoin and the technology that underpins it. It uses different kinds of technologies such as consensus mechanisms, digital signatures, and even hash chains. Store data and records in Bitcoin and centrally build a decentralized shared database. Today, it is one of the most widely adopted technologies because it is considered a consensus in untrusted networks. Transferring value in a robust and decentralized manner is the most difficult feature of blockchain. Therefore, in the future, we can predict that blockchain will update the current information internet into a valuable internet and rapidly change our society and the way we live. [14] The Internet of Things was introduced as a set of technologies, from wireless sensor networks to radio frequency identification (RFID), that provide the ability to sense, activate, and communicate over the Internet. According to various researchers, there will be 20-50 billion connected devices by 2020. This is mainly due to his IoT placement on a large number of devices.

Today, many smart gadgets and items work with sensors to detect continuous data from our planet. Nevertheless, this worldview suggests that all important things - sensors, PCs, brilliant cars, smart appliances, mechanical and useful modules - are connected through a system of systems and

equipped with information. That changed with the advent of IoT. Analytical capacity in this sense has changed the way we play, live, and work [25].

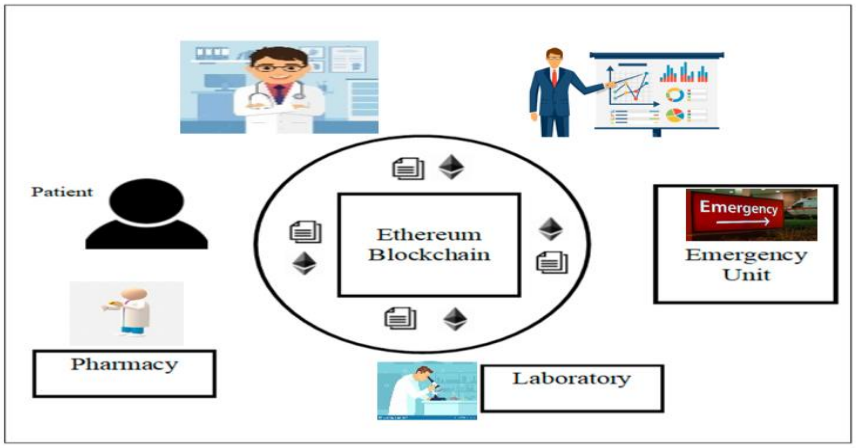

Fig. 6: Smart health data processing using blockchain adapted by [48]

Working of Blockchain

A blockchain can be described as a decentralized record design used to hold a growing list of required exchanges grouped into squares and stored multiple times for data persistence. especially. At a time, at the blockchain, only one square can be included and verified (using cryptography) scientifically improved the situation of each square to ensure that it continues to cluster previous squares, keeping the agreement intact across the entire decentralized system. The verification process known as Proof of Work (POW) or "mining", is the process of gaining achievements between system centers (also known as "miners") to get the first square in the box next square in the blockchain by solving a computational problem. Expensive puzzle. The arrangement is then communicated to the entire system by the winner, allowing them to raise some of the crypto-mining prizes [45]. This system coordinates cryptography, hijacking hypothesis, and pulse generation to allow the system to come to an agreement regarding each square of the blockchain and ensure that there is no modification of the transaction history. The blockchain stores all transaction records, which are transmitted to all the centers in the system. It helps in finding honesty, straightforwardness, and strength (when it comes to deception, there is no single point). Comparatively, the blockchain layout is operated from isolated obstacles in the form of linked start times along the current or communicated position in place of the starting point. The squares are passed into the system after receiving data from the subtle elements. The squares are then fixed by framing a sequence and can never be refreshed, upgraded, or expelled. It also enables successful crime scene investigations and improves the traceability of information in potentially hazardous situations in the context, or when customers mismanage information when it comes to methods. collection method. A square is processed from an individual event where an event can be described as the date and age when the request was made until the square is broadcast in the blockchain. For example, when an accredited body needs to review framework inconsistencies, a request is submitted and the agency must then authorize an investigation of the irregularities. For such anomalies, agreement centers in the results. This is not particularly troublesome since it is possible to connect the squares to the immutable nature of the blockchain [21].

A blockchain consists of an ever-changing set of records called a square. Each square is about an exchange arrangement and is cryptographically connected to its previous square, thus forming a chain. A blockchain is overseen by a distributed central system that approves new squares using agreement computation. Calculating the chord ensures that the next square in the blockchain is the most realistic shape ever, thus effectively preventing incredible enemies from splitting the chain in half [26]. In such a case, Medical Researchers can approach a conveyed 'pool of information' of therapeutic medications and social insurance results are given qualities put away using e-Health and m Heath in web/cloud clinical Stages. In addition, by empowering therapeutic analysts to sift through particular highlights of the information they are searching for, one could accomplish assistance in the arrangement of statistic companions, and upgrade the accuracy of prescription [46].

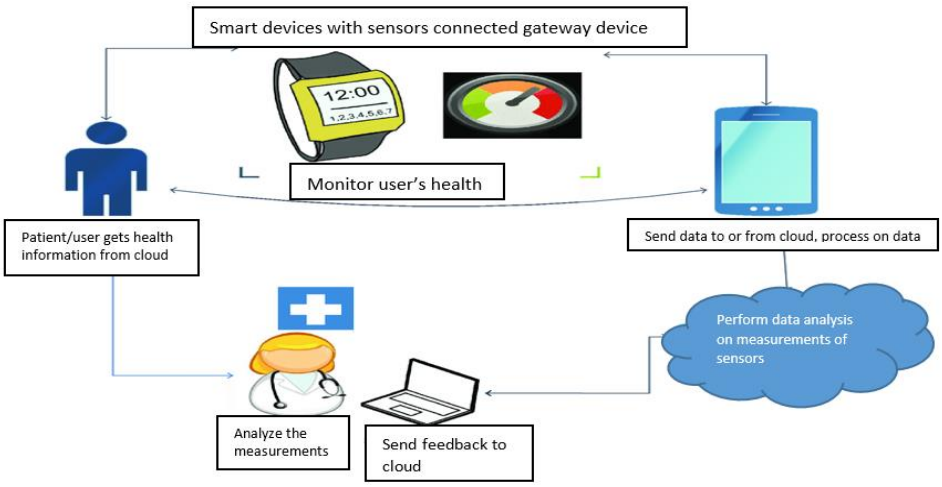

Fig. 7: Adapted from [27] Smart Healthcare Infrastructures

Before we depict our engineering configuration, give us a chance to audit some specialized highlights concerning blockchain e-Health well-being streams.

- E-health blockchain
- Distributed database
- Peer-to-peer transmission
- Transparency and auto-tracking
- Irreversibility of records
- Computational logic

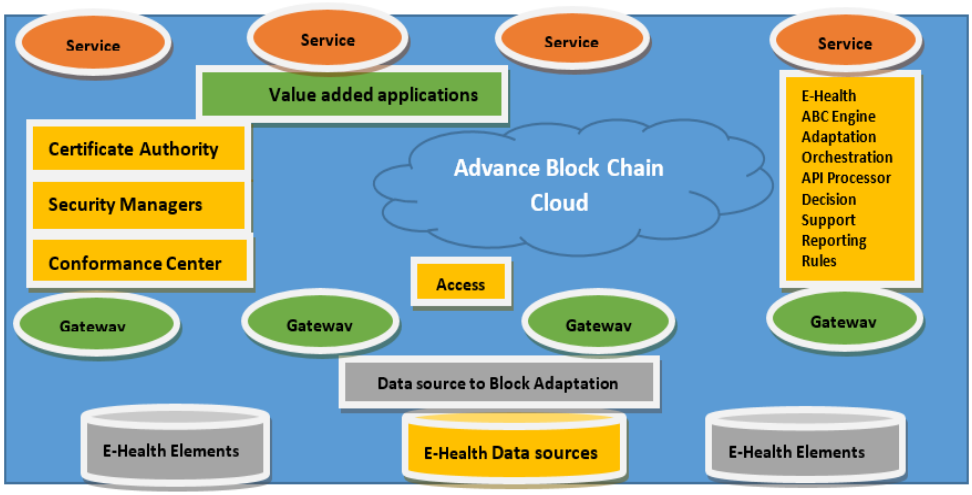

Fig. 8: Advance Blockchain Cloud Architecture adapted by [16]

Use Cases

There are 5 use cases developed for 5 various cohesive systems (using analysis of 26 systems) for ontologies engineering with usages of blockchain services. These use cases establish the numerous service area of different systems composed to achieve one goal. These services are coined together to make an integrated IoT healthcare system.

Use Case 1: Arrhythmia Detection

- ECG Filtering
- Heart Beat Segmentation
- Feature Extraction
  - Discrete Wavelet Transform (DWT)
- Classification
  - Support Vector Machine (SVM)

Use Case 2: Heart Disease Monitoring

- Sensing heart rate
- Blood pressure checking
- Data Transmission
  - Data storage on the cloud

Use Case 3: Heart Rate Monitoring

- Heart Rate Sensing
- Monitoring Heart Rate using HEART (wearable device)
- Supervised Learning using AI
  - K-Nearest Neighbor (KNN) algorithm for supervised learning
- Transmitting data to Cloud

Use Case 4: Cardiac Auscultation Monitoring

- Heart Sound Sensing
- Analyzing Heart Sound
  - Signal Pre Processing
  - Feature Extraction

    - Data Clustering
- Transmission to Android App

Use Case 5: Chronic Metabolic Disorders

- Attaining Patients Vital Parameters
- Disease Manager
    - Defining Post-Processing Rules
- Bi-direction Communication (between Doctor and Patient and between different experts)
- Medical Diagnosis

Roles Identification

After developing several systems, we can define different roles (stakeholders) and their rights accordingly.

Table I: Stakeholders along with their rights

Stakeholders	Rights
Doctor	The doctor can prescribe the medicine to the patient.
Patient	A patient can provide his information to the doctor regarding his disease
Nurse	A nurse can only follow the instructions of the doctor
Lab Assistant	Lab assistants can perform operations of the testing patient and deliver the reports to the doctor
Pathologist	The person who does blood, and other types of chemical tests
Diabetic Core Team	A diabetic team can measure the sugar level of a patient and can prescribe medicine accordingly
Medical Expert	A medical expert can provide medicine to a patient as per the prescription
Care Giver	Caregivers can follow the instructions of the doctor and take care of the timings of medicine of patient
Guardian	Guardian can look after his patient and can give medicine to his patient on time.
Wristband	The wristband can detect the pulse rate of patient
Ambulance	The ambulance can take the patient to the hospital for an immediate checkup
Radiologist	persons who do x-rays, ultrasounds
Thyroid Cancer Expert	Thyroid cancer experts can prescribe patients medicines according to their disease
Hospital Admin	Hospital admin can just check on the doctor and other staff that whether they are doing take care of the patient or not.
Cancer Specialist Doctor	A cancer Specialist doctor can diagnose the type of cancer a patient is suffering from.
Android app	Android app can connect the patient to the concerned doctor

Smart Watch	The smartwatch can detect the time and can record other measurements of the human body
Wearable Device	A wearable device can detect the blood pressure or temperature of the patient

In the above table, we have defined several stakeholders having individual importance and certain tasks to perform. Each stakeholder has a certain place in a smart health environment that would make the whole hierarchy.

Roles Taxonomy

There are numerous roles in a smart health system that plays a vital role in the processing of maintaining data record and accessing that data from time to time according to the requirement.

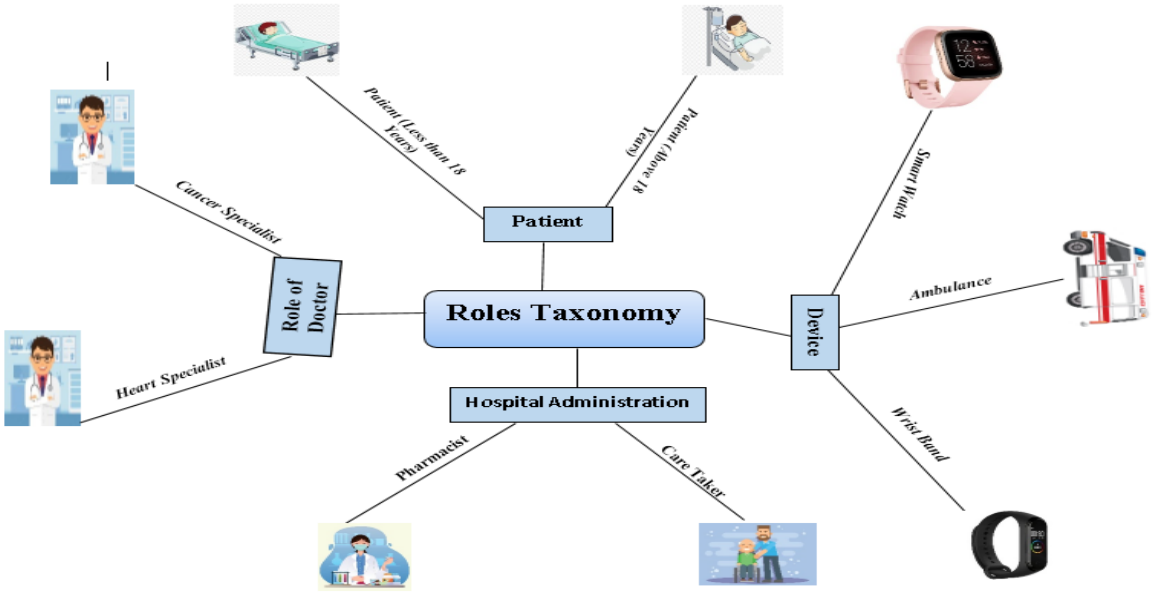

Fig. 9: Roles Taxonomy

Roles Specific Task

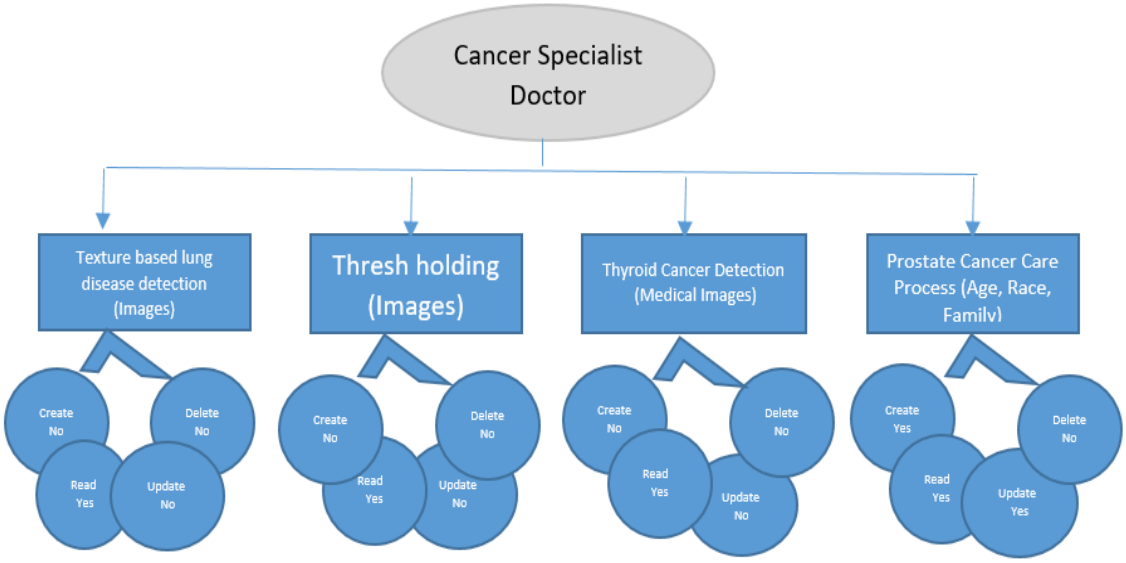

Fig. 10: Data Access Control to Cancer Specialist Doctor

In figure 10 we can see that a cancer Specialist Doctor Can perform the following tasks as mentioned above he can detect lung cancer disease, can perform the process of thresh holding similarly he can detect thyroid cancer and prostate cancer care process as well. But on the other side when the data is generated in that particular process cancer specialist doctors can only read the data in texture-based lung disease detection but cannot create, update or delete it. The same permissions have been granted in the case of threshing holding and thyroid Cancer Detection. But Prostate Cancer Care Process allows cancer specialist doctors to create updates and read but they cannot delete any data.

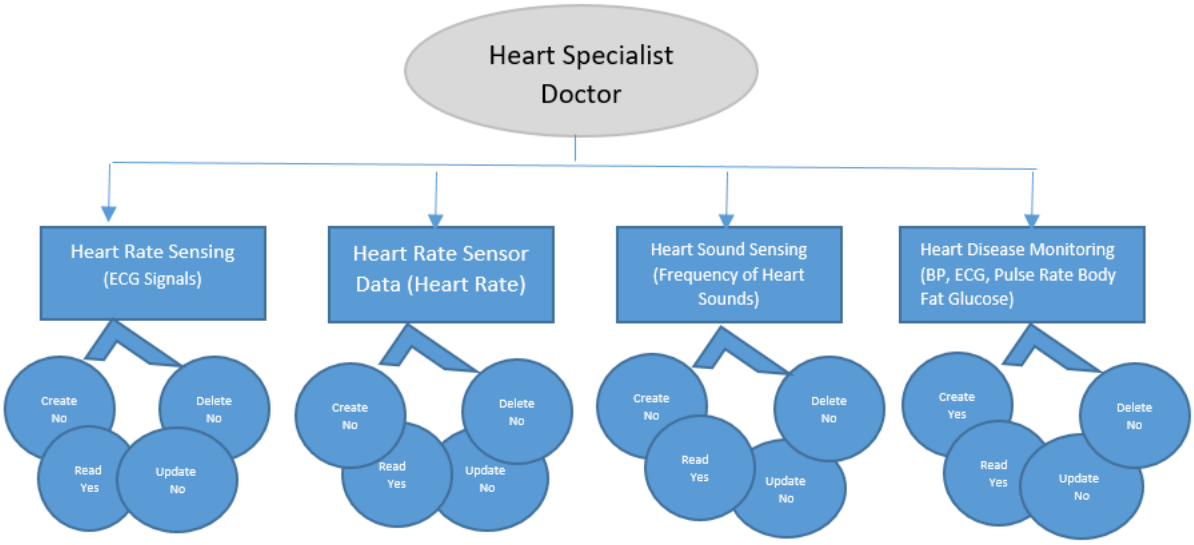

Fig. 11: Data Access Control to Heart Specialist Doctor

In Fig. 11 it is visible that a heart specialist doctor can perform these numbers of tasks like he can do sensing the heart rate of his patient, similarly, he read the heart rate sensor data, can observe

the heart sound sensing, as well as heart disease monitoring. A heart Specialist doctor can read all data mentioned but cannot create, update or delete any of it.

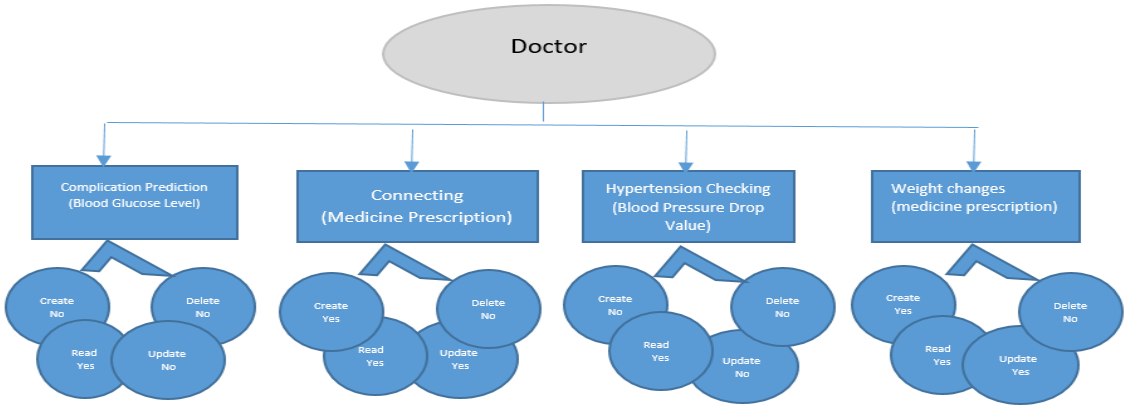

Fig. 12: Data Access Control to Doctor

Previously we have studied cancer and heart specialist doctors now we can see in Fig. 12 that doctors can diagnose the patient, predict the complication, and check hypertension, similarly, they can create, read and update medicine prescriptions in case of connecting or weight changes but cannot delete them. Whereas in case of complication process or hypertension checking doctor can only read but cannot perform other operations.

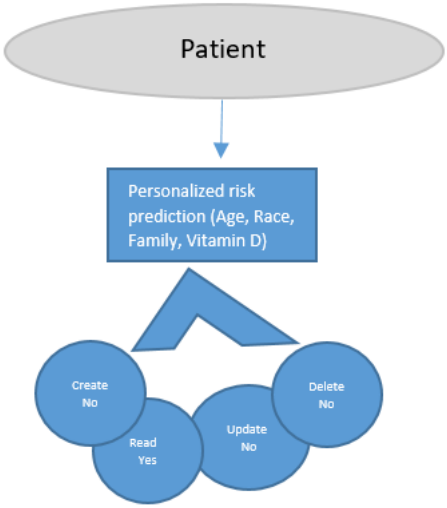

Fig. 13: Data Access Control to Patient

In Fig. 13 we can see that patient can only predict risk by sensing his health condition and after sensing he can just ask the doctor to diagnose the disease and suggest medicine accordingly. If we talk about data access controls patients cannot create, update or delete but can read data only.

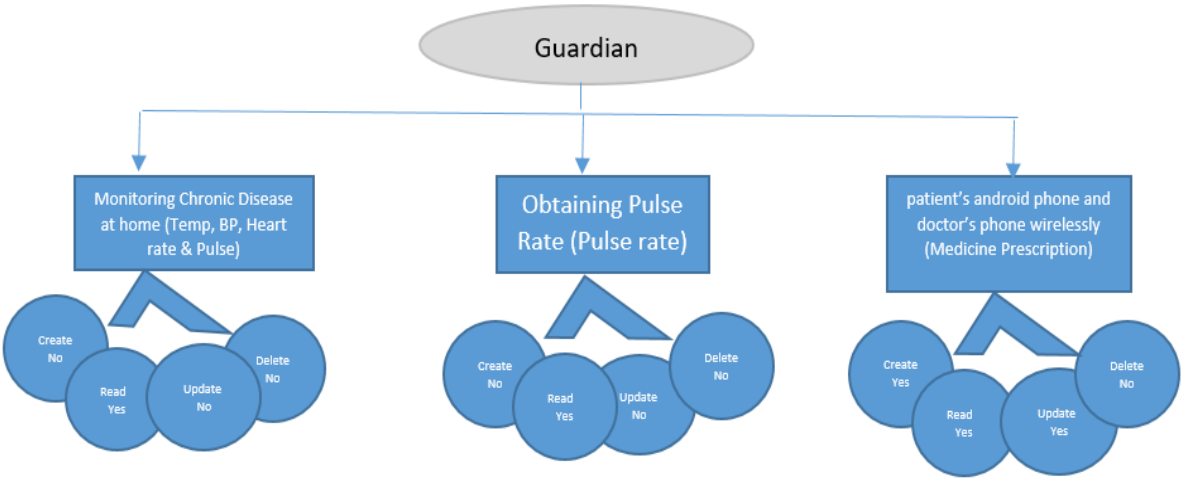

Fig. 14: Data Access Control to Guardian

In Fig. 14 we can see the role of the guardian as he can monitor the chronic disease of the patient at home as well as he can obtain the pulse rate and also can connect the patient and doctor on wireless devices using a smart health environment. But here if we talk about access control guardian cannot create, update or delete the data but can read only.

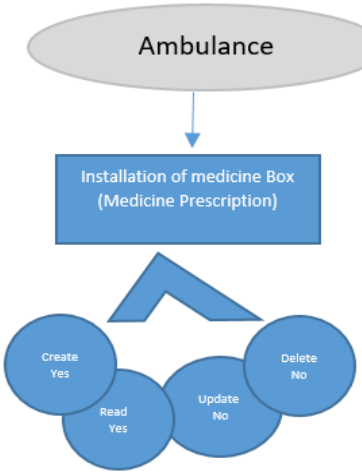

Fig. 15: Data Access Control to Ambulance

In Fig. 15 we can see that the ambulance can perform tasks including installing of medicine box and providing the medicine to the patient at an appropriate time. Here the Data access rights are just to the extent of creation and reading, but no updating and deletion are allowed.

Results and Discussions

Hyper ledgers (CTO: Blockchain Model)

Assets

In a blockchain, these assets are saved in form of code so that when we will require them, we can just easily find them. We will define some asset types along with their codes to give a brief vision of how the system will run background commands.

asset blood glucose identified by bloodGlocouseID {
- o String bloodGlocouseId
- o integer value
- o String date
- o String time
- --> patient owner

}

Blood Glucose is a type of data we collect or measure in the smart health environment. The patient blood glucose level helps the doctor to determine his health condition and to suggest medicine accordingly.

asset blood pressure identified by blood pressure {
- o String blood pressured
- o integer Sis
- o integer dis
- o String date
- o String time
- --> patient owner

}

Blood pressure helps determine patients' health condition and to suggest hi medicine accordingly.

asset patient identified by patientID {
- o String patientId
- o String name
- o String firstName
- o String lastName
- o integer age
- o integer gender
- o String race
- o String country
- --> patient owner

}

The patient is an actor and stakeholder in a smart health environment but besides this knowing, some personal information helps the doctor to suggest him appropriate medicine.

asset temperature identified by TempID {
  o String TempID
  o String Date
  o String Time
  o Integer value
  --> patient owner
}

Temperature is another medical term that can cause fever if it goes to a high level. A doctor should know about the patient's temperature.

asset Heartrate identified by HeartrateID {
  o String heartrateID
  o String Date
  o String Time
  o Integer value
  --> patient owner
}

Herat rate of the patient is an important aspect in the medical field as if it gets disturbed a death can occur. It is calculated in integer values.

Transactions

In a blockchain, these transactions are saved in form of code so that when we will require them,s we can just easily find them. We will define some transaction types along with their codes to give a brief vision of how the system will run background commands.

transaction ReadingHeartRate {
  --> HeartRate asset
  o String newValue
  o String date
  o String time
}

In this transaction, the data type of heart rate generates and helps the doctor and other medical staff to diagnose the disease.

transaction ReadingPulseRate {
  --> PulseRate asset
  o String newValue
  o String date

  o String time
}

In this transaction, the pulse rate will be measured by some instrument and the doctor will keep it in the record for future correspondence

transaction ReadingBodytemperature {
  --> Bodytemperatureasset
  o String newValue
  o String date
  o String time
}

In this transaction, body temperature will be measured by a doctor or caretaker to identify the health condition of the patient.

transaction ReadingBloodglucoselevel {
  --> Bloodglucoselevelasset
  o String newValue
  o String date
  o String time
}

Blood glucose level is the type of transaction where a patient blood glucose level is measured to identify the health condition of the patient.

transaction ReadingRespiratoryrate {
  --> Respiratoryrateasset
  o String newValue
  o String date
  o String time
}

Respiratory rate reading is the transaction that took place by a doctor or other medical staff to keep an eye on patients' health conditions.

Participants
In the blockchain, these participants are saved in form of code so that when we will require them,s we can just easily find them. We will define some participants' types along with their codes to give a brief vision of how the system will run background commands.

Participant Lab assistant identified by LabassistantID {

  o String **LabassistantID**
  o String Date
  o String Time
}

Lab assistants perform all the tasks co-related to the lab. All types of tests and other experiments were done by him.

Participant patient identified by patientID {
  o String **patientID**
  o String Date
  o String Time
}

The Patient himself is a participant as he is the main actor on which the whole working performed. Measuring his body's health conditions to curing his disease.

Participant Doctor identified by DoctorID {
  o String **DoctorID**
  o String Date
  o String Time
}

In the blockchain, these participants are saved in form of code so that when we will require them on time for any transaction we can just easily find them.

Participant Nurse identified by NurseID {
  o String **NurseID**
  o String Date
  o String Time
}
Here Nurse is a kind of caretaker who looks after the patient’s health.

Conclusion & Future Work

Here, we can conclude that from this research we can solve security and privacy issues in the smart healthcare environment. Likewise, we can observe and control the permission to access data by setting certain rules. Throughout this research, we have observed that blockchain systems can make smart healthcare environments safer and more applicable. We have studied in many different systems how smart health works. Several participants are performing various transactions and with their help we get the work done. In addition, by using blockchain technology, we can protect confidential data and prevent unauthorized access, granting access to private patient data only to authorized individuals and we can store data in block form through which we can easily access data in difficult times. We can improve our data rules and access control lists to be more secure

and safe. In addition, we may implement other strategies to improve physician and patient response rates and performances to complete transactions safely and fast.

Author's Contribution: Z.I., Conceived the idea; Z.I., Designed the simulated work, and M.I.T., did the acquisition of data; R.A.K, executed simulated work, data analysis or analysis and interpretation of data and wrote the basic draft; K.S., Did the language and grammatical edits or Critical revision.

Funding: The publication of this article was funded by no one.

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

Acknowledgment: The authors would like to thank Daniyal Ahmad for his assistance with the collection of data.

References:

[1] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," J. Comput. Commun., vol. 03, no. Published Online May 2015 in SciRes, pp. 1–10, 2015.
[2] M. I. Tariq et al., "Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks," Sensors, vol. 20, no. 5, p. 1310, 2020.
[3] A. M. Rahmani et al., "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," Futur. Gener. Comput. Syst., vol. 78, pp. 641–658, 2018.
[4] S. López-Torres et al., "IoT monitoring of water consumption for irrigation systems using SEMMA methodology," presented at the International conference on intelligent human computer interaction, 2020, pp. 222–234.
[5] D. Ding, R. A. Cooper, P. F. Pasquina, and L. Fici-Pasquina, "Sensor technology for smart homes," Maturitas, vol. 69, no. 2, pp. 131–136, Jun. 2011.
[6] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," IEEE Access, vol. 5, no. c, pp. 26521–26544, 2017.
[7] M. Bhatia and S. K. Sood, "A comprehensive health assessment framework to facilitate IoT-assisted smart workouts: A predictive healthcare perspective," Comput. Ind., vol. 92–93, pp. 50–66, 2017.
[8] L. Y. Mano et al., "Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition," Comput. Commun., vol. 89–90, pp. 178–190, 2016.
[9] S. Sicari, A. Rizzardi, L. A. Grieco, G. Piro, and A. Coen-Porisini, "A policy enforcement framework for Internet of Things applications in the smart health," Smart Heal., vol. 3–4, no. May, pp. 39–74, 2017.
[10] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," Futur. Gener. Comput. Syst., vol. 86, pp. 1437–1455, 2018.
[11] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.
[12] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," CAAI Trans. Intell. Technol., vol. 3, no. 2, pp. 114–118, 2018.
[13] A. M. Saghiri, M. Vahdati, K. Gholizadeh, M. R. Meybodi, M. Dehghan, and H. Rashidi, "A Framework for Cognitive Internet of Things based on Blockchain," 4th Int. Conf. Web Res., pp. 138–143, 2018.

[14] W. Liu and U. Krieger, “Advanced Block-Chain Architecture for e-Health Systems,” no. Etpha, pp. 37–42, 2017.
[15] Z. H. Ali, H. A. Ali, and M. M. Badawy, “Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions,” no. October 2015.
[16] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, “Service composition approaches in IoT: A systematic review,” J. Netw. Comput. Appl., vol. 120, pp. 61–77, 2018.
[17] A. Bröring, S. Antipolis, C. Bonnet, and S. Antipolis, “Session V : DISCOVERY & CONFIGURATION A Categorization of Discovery Technologies for the Internet of Things,” pp. 131–139, 2016.
[18] L. Zhang, H. Tong, H. O. Demirel, V. G. Duffy, Y. Yih, and B. Bidassie, “A Practical Model of Value Co-creation in Healthcare Service,” Procedia Manuf., vol. 3, pp. 200–207, 2015.
[19] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. S. Tavares, and V. H. C. de Albuquerque, “A medical records managing and securing blockchain-based system supported by a Genetic Algorithm and Discrete Wavelet Transform,” Cogn. Syst. Res., vol. 52, pp. 1–11, 2018.
[20] A. Onasanya and M. Elshakankiri, “IoT Implementation for Cancer Care and Business Analytics / Cloud Services in Healthcare Systems,” pp. 205–206, 2017.
[21] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, Blockchain Technology Use Cases in Healthcare, 1st ed. Elsevier Inc., 2018.
[22] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” Sustain. Cities Soc., vol. 39, pp. 283–297, 2018.
[23] P. K. Sharma, M. Y. Chen, and J. H. Park, “A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT,” IEEE Access, vol. 6, no. c, pp. 115–124, 2018.
[24] A. Theodouli, S. AraklIoTis, K. Moschou, K. Votis, and D. Tzovaras, “On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing,” Proc. - 17th IEEE Int. Conf. Trust. Security. Privacy. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018, pp. 1374–1379, 2018.
[25] M. Kalmeshwar and A. P. D. N. P. K S, “Internet Of Things: Architecture, Issues, and Applications,” Int. J. Eng. Res. Appl., vol. 07, no. 06, pp. 85–88, 2017.
[26] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” J. Am. Med. Informatics Assoc., vol. 24, no. 6, pp. 1211–1220, 2017.
[27] C. Li, X. Hu, and L. Zhang, “The IoT-based heart disease monitoring system for pervasive healthcare service,” Procedia Comput. Sci., vol. 112, pp. 2328–2334, 2017.
[28] B. Martínez-Pérez, I. de la Torre-Díez, and M. López-Coronado, “Privacy and Security in Mobile Health Apps: A Review and Recommendations,” J. Med. Syst., vol. 39, no. 1, 2015.
[29] K. Khujamatov, K Ahmad, E. Reypnazarov, D. Khasanov, “Markov Chain Based Modeling Bandwith States of the Wireless Sensor Networks of Monitoring System,” International Journal of Advanced ScienceScience and Technology, vol. 29, No.4, 2020, pp. 4889–4903.
[30] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.
[31] N. Panwar, S. Sharma, and A. K. Singh, “A survey on 5G : The next generation of mobile communication,” Physical Communication, vol. 18, pp. 64–84, 2016
[32] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, “Security for 5G and beyond,” IEEE Communications Surveys & Tutorials, 2019
[33] K. Christidis and M. DevetsikIoTis, “Blockchains and smart contracts for the internet of things,” Ieee Access, vol. 4, pp. 2292–2303, 2016.

[34] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–564.
[35] C. Thuemmler, C. Rolffs, A. Bollmann, G. Hindricks, and W. Buchanan, “Requirements for 5G based telemetric cardiac monitoring,” in 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2018, pp. 1–4.
[36] 5G and blockchain: The building blocks of the shared economy. [Online]. Available: https://www.ericsson.com/en/blog/2019/ 10/5G blockchain-shared-economy.
[37] M. Chaudhry, “Joint Ieee spectrum and comsoc talk, test and measurement virtualization and blockchain: Enablers for 5G networks,” Nov 13, 2018.
[38] H. L. Cech, M. Großmann, and U. R. Krieger, “A fog computing architecture to share sensor data utilizing blockchain functionality,” in 2019 IEEE International Conference on Fog Computing (ICFC), 2019, pp. 31–40
[39] Saba T, Haseeb K, Ahmed I, Rehman A (2020) Secure and energy-efficient framework using Internet of Medical Things for e- healthcare. J Infect Public Health 13(10):1567–1575
[40] Li J, Cai J, Khan F, Rehman AU, Balasubramaniam V, Sun J, Venu P (2020) A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System. IEEE Access 8:135479–13549013549
[41] Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., & Yi, X. (2019, July). A novel architecture for tamper-proof electronic health record management system using blockchain wrapper. In Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure (pp. 97-105).
[42] A. D. Acharya and S. N. Patil, "IoT-based Health Care Monitoring Kit," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 363-368, DOI: 10.1109/ICCMC48092.2020.ICCMC-00068.
[43] Tariq, N., Qamar, A., Asim, M., & Khan, F. A. (2020). Blockchain and smart healthcare security: a survey. Procedia Computer Science, 175, 615-620.
[44] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.
[45] Taralunga DD, Florea BC. A Blockchain-Enabled Framework for eHealth Systems. Sensors. 2021; 21(8):2828. https://doi.org/10.3390/s21082828
[46] Khatoon A. A Blockchain-Based Smart Contract System for Healthcare Management. Electronics. 2020; 9(1):94. https://doi.org/10.3390/electronics9010094
[47] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7), 1-7.
[48] H. Batool, M. I. Tariq, S. Shoukat, and U. A. Zafar, “An Audit: IoT-Based Smart Cities,” in Advances in Smart Vehicular Technology, Transportation, Communication and Applications, Springer, 2021, pp. 171–182.
[49] M. I. Tariq, S. Tayyaba, M. W. Ashraf, and V. E. Balas, “Deep learning techniques for optimizing medical big data,” in Deep Learning Techniques for Biomedical and Health Informatics, Elsevier, 2020, pp. 187–211.
[50] M. I. Tariq, S. Tayyaba, M. U. Hashmi, M. W. Ashraf, and N. A. Mian, “Agent Based Information Security Threat Management Framework for Hybrid Cloud Computing,” IJCSNS, vol. 17, no. 12, p. 57, 2017.