الجمـــهوريـــة الجـــزائريـــة الديـمقراطيـــــــة الشـــعبيـــــة
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعـلـيـم الـعـالـــي والـبـحـث الـعـلـمي
MINISTRY OF HIGHER EDUCATION AND SCIENTAFIC RESEARCH
جـامـعـة عمّـــار ثلجيي بالأغـــواط
UNIVERSITY OF AMAR TELIDJI LAGHOUAT
كـلـيـــة الـعـلـــوم
FACULTY OF SCIENCES
DEPARTEMENT OF COMPUTER SCIENCES

MASTER THESIS

Domaine : Mathematics and Computer Science

Field : Computer Science

Option : Distributed Networks, Systems, and Applications

TOPIC

A Blockchain Based System for Patients' Digital Twin

Presented by: Maicha Nour El Houda and Benattia Zinab Bouchra

Defended Publicly in Front of the Jury Composed of:

Dr .T.Bendouma	**University of Laghouat**	**President**
Dr .Y.Guellouma	**University of Laghouat**	**Examiner**
Dr .M.A.Ameur	**University of Laghouat**	**Examiner**
Dr .C.A.Kerrache	**University of Laghouat**	**Advisor**

Academic Year 2022/2023

Dedication

I dedicate this thesis
To my father, who has been a constant source of support, encouragement, and inspiration.
To my mother, who has been my pillar of strength, supporting me throughout these years of study.
I would also like to dedicate this work to my beloved younger brother and my entire family.
Your unwavering love and guidance have shaped me into who I am today
and I am forever grateful.

Bouchra Zinab Benattia

Dedication

I dedicate this work
To the memory of my father
To my dear mother
To my brothers Bachir and Mohammed
To my dear cousin Imane
To my entire family for their support throughout my academic journey.

Nour El Houda Maicha

Acknowledgments

First and foremost, we express our gratitude to God for granting us the physical and intellectual strength to accomplish this endeavor. We extend our appreciation to all those who have directly or indirectly contributed to the outcome of this work, whether through their guidance, or encouragement.

We would like to offer a heartfelt tribute to our esteemed advisor, Mr. Kerrache Chaker Abdelaziz. It has been an honor to collaborate with him during our final projects. We are immensely grateful for his unwavering support, his profound understanding of pedagogical humanism, and his dedication to intellectual and moral rigor.

Lastly, we would like to extend our thanks to the members of the jury for their valuable time and effort in evaluating this work. Your expertise and insights have greatly contributed to its development and refinement.

ملخص

مع زيادة التركيز على الرعاية الصحية، وخاصة التحليلات في الوقت الفعلي والتشخيص الذاتي، زاد الاهتمام بالتقاط بيانات المريض في الوقت الفعلي بشكل كبير لكل من الأطباء والمرضى. ساهم تطوير الأجهزة الذكية التي يمكنها جمع البيانات مثل ضغط الدم ومعدل ضربات القلب ومستوى السكر في الدم وما إلى ذلك بشكل كبير في تحسين قدرات إدارة الصحة الفردية. ومع ذلك، تشكل هذه التطورات تحديات مثل المخاوف المتعلقة بالأمان والموثوقية ودقة التشخيص. وعادة ما تحدث مشكلات بشكل متكرر، خاصة عند تبادل المعلومات ونقل البيانات. للتغلب على هذه التحديات، يستخدم هذا المشروع تكنولوجيا البلوكشين لتحسين نقل وأمان البيانات. تستكشف الدراسة استخدام حلول البلوكشين في مجال الرعاية الصحية الذكية. بالإضافة إلى ذلك، يتم استخدام مفهوم التوأم الرقمي لتحسين التشخيص من خلال محاكاة تأثير الأدوية على كائنات افتراضية. استناداً إلى نتائج هذه المحاكاة، يمكن للأطباء اتخاذ قرارات مدروسة بشأن الأدوية المناسبة وتقييم حالة المريض بدقة. سيتم إنشاء نظام مراقبة للصحة باستخدام تقنية التوأم الرقمي والبلوكشين لتنظيم جمع معلومات المستخدمين بشكل آمن وتمكين تشخيص دقيق. يضمن هذا التكامل تخزيناً ونقلًا آمنين للبيانات، مما يؤدي إلى تحقيق نتائج صحية أفضل. في أطروحة الماجستير هذه، نقدم دراسة حول تكامل تقنية البلوكشين مع التوأم الرقمي لمراقبة صحة المريض. نقدم واجهة متصلة بقاعدة بيانات البلوكشين، مصممة خصي صًا للأطباء لمراجعة السجلات الصحية للمرضى من خلال عنوان محفظة المريض وتحديد الحالة الطبيعية لمعدل ضربات قلب المريض بناءً على بياناتهم الطبية. بالإضافة إلى ذلك، تسمح الواجهة للأطباء بالتنبؤ بتأثير الدواء على معدل ضربات قلب المريض وضغط الدم.

الكلمات المفتاحية: البلوكشين، التوأم الرقمي، مراقبة الصحة، الأدوية.

Abstract

With the increasing focus on healthcare, especially real-time analytics and self-diagnosis, the interest in capturing real-time patient data has increased significantly for both physicians and patients. The development of smart devices that can collect data such as blood pressure, heart rate, blood sugar level, etc., has greatly contributed to improving individual health management capabilities. However, these advances also, bring challenges such as concerns over safety, reliability, and accurate diagnosis. Problems often arise, especially when exchanging information and transmitting data. To overcome these challenges, this project uses blockchain technology to improve data transmission and security. This study explores the use of blockchain-based internet solutions by integrating blockchain into smart healthcare. Additionally, the digital twin concept is used to improve diagnosis by simulating the effects of drugs on virtual objects. Based on the results of these simulations, physicians can make informed decisions about appropriate medications and accurately assess a patient's condition. A health monitoring system using digital twin technology and blockchain can be implemented to securely organize the collection of user information and enable accurate diagnosis. This integration ensures secure storage and transmission of your data and improves your health outcomes. In this master's thesis, we present a study of integrating blockchain technology with Digital Twin for patient health monitoring. We showcase an interface connected to the blockchain database, specifically designed for doctors to review patient health records through patient wallet address and determine the normalcy of the patient's heart rate based on their medical data. Additionally, the interface allows doctors to predict the effect of medication on the patient's heart rate and blood pressure.

Key-words: Blockchain, Digital twin, Health monitoring, Medications.

Résumé

Avec l'attention croissante portée aux soins de santé, en particulier l'analyse en temps réel et l'autodiagnostic, la collecte de données en temps réel sur les patients pour les médecins et les patients est devenue essentielle. Les avancées technologiques telles que les appareils intelligents capables de collecter des données telles que la pression artérielle, la fréquence cardiaque et la glycémie ont considérablement amélioré la gestion de la santé personnelle. Cependant, ces avancées posent également des défis, notamment en termes de sécurité, de fiabilité et de précision du diagnostic. Des problèmes surviennent souvent, en particulier lors de l'échange d'informations et de la transmission de données. Pour surmonter ces défis, ce projet utilise la technologie blockchain pour améliorer la transmission et la sécurité des données. Cette étude explore l'utilisation de solutions basées sur la blockchain dans le domaine des soins de santé intelligents. De plus, le concept de jumeau numérique est utilisé pour améliorer le diagnostic en simulant les effets des médicaments sur des objets virtuels. Sur la base des résultats de ces simulations, les médecins peuvent prendre des décisions éclairées concernant les médicaments appropriés et évaluer avec précision l'état d'un patient. Nous allons construire un système de surveillance de la santé qui utilise la technologie des jumeaux numériques et la blockchain pour collecter en toute sécurité les informations des utilisateurs et permettre un diagnostic précis. Cette intégration garantit un stockage et une transmission sécurisés de vos données et améliore vos résultats de santé. Dans ce mémoire de master, nous présentons une étude sur l'intégration de la technologie blockchain avec les jumeaux numériques pour le suivi de la santé des patients. Nous proposons une interface connectée à une base de données blockchain, spécialement conçue pour que les médecins examinent les dossiers de santé des patients via l'adresse de portefeuille patient et déterminent la normalité de la fréquence cardiaque du patient en fonction de ses données médicales. De plus, l'interface permet aux médecins de prédire l'effet des médicaments sur la fréquence cardiaque et la tension artérielle du patient.

Mots-clés : Blockchain, Jumeaux numériques, Surveillance de la santé, Médicaments.

Table of content

1 General Introduction **1**

2 Internet of Thing based healthcare monitoring system **3**
2.1 Introduction . . . 3
2.2 Internet of Things . . . 3
2.2.1 Internet of Things Architecture . . . 4
2.2.2 Applications in Internet of Things . . . 5
2.2.3 Challenges of Internet of Things . . . 6
2.3 Internet of Things for healthcare . . . 8
2.3.1 Internet of Medical Things System Architecture . . . 8
2.3.2 Technologies Used for the Collection of Sensor-Based Medical Data . 9
2.3.3 Types of Internet of Medical Things devices . . . 11
2.3.4 Internet of Things Based Healthcare Systems and Their Applications 12
2.3.5 Internet of Things Applications in Health Monitoring . . . 12
2.3.6 The Significance of Internet of Thing Based Healthcare-Monitoring Systems . . . 13
2.3.7 Challenges and issues . . . 13
2.4 Cluster Computing . . . 14
2.5 Cloud Computing . . . 14
2.6 Fog Computing . . . 15
2.6.1 Fog Computing Service in the Healthcare Monitoring . . . 15
2.6.2 Features of Fog Computing . . . 16
2.7 Edge Computing . . . 17
2.7.1 Edge Computing Use Cases in Healthcare . . . 17
2.7.2 Features of Edge Computing . . . 18
2.8 Conclusion . . . 19

3 Blockchain and Digital Twin for healthcare monitoring **20**
3.1 Introduction . . . 20
3.2 Blockchain fundamentals . . . 20
3.2.1 Introduction of Blochchain . . . 20
3.2.2 Blockchain Components . . . 21
3.2.3 Block structure . . . 22
3.2.4 Consensus algorithms in Blockchain . . . 23

3.2.5 Performances of Consensus Algorithm . . . 27
3.2.6 Types of blockchain . . . 27
3.3 Healthcare Blockchain . . . 28
3.3.1 The use cases of Blockchain in healthcare . . . 28
3.3.2 Benefits of blockchain to healthcare applications . . . 30
3.4 Electronic Health Record . . . 30
3.5 Related work . . . 31
3.5.1 A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain 31
3.5.2 Discussion and critique . . . 31
3.6 Digital Twin fundamentals . . . 32
3.6.1 Introduction of Digital Twin . . . 32
3.6.2 A brief history of digital twin technology . . . 32
3.6.3 Digital Twin components . . . 32
3.6.4 Data life cycle management in Digital Twin Product Design . . . 33
3.6.5 Types of digital twins . . . 34
3.6.6 The characteristics of digital Twin . . . 34
3.7 Healthcare Digital Twin . . . 35
3.7.1 Current Research of Applications in Intelligent Medical Systems . . . 35
3.7.2 Concept of Digital Twin Healthcare . . . 36
3.8 Related Work . . . 37
3.8.1 Digital twins to personalize medicine . . . 37
3.8.2 Blockchain-Based Digital Twins Collaboration for Smart Pandemic Alerting: Decentralized COVID-19 Pandemic Alerting Use Case . . . 38
3.8.3 Design of Mobile Healthcare Monitoring System Using IoT Technology and Cloud Computing . . . 39
3.8.4 Discussion and critique . . . 39
3.9 Conclusion . . . 40

4 Implementing a Blockchain-based System for Patients' Digital Twin 41
4.1 Introduction . . . 41
4.2 Building a Blockchain-Based Digital Twin System for Patient Monitoring . . . 41
4.2.1 Set up Development Environment . . . 41
4.2.2 Dependencies . . . 42
4.3 Implementation . . . 43
4.3.1 Health care smart contract . . . 43
4.3.2 User management smart contract . . . 43
4.3.3 The deploy of smart contracts . . . 44
4.3.4 Test of contracts . . . 44
4.4 Diagrams and users interface . . . 45
4.4.1 Diagrams . . . 45
4.4.2 HealthLink interface . . . 47
4.5 Research challenges . . . 52
4.6 Advantages and disadvantages of the conceived system . . . 54

5 General Conclusion and Future Directions 55

List of Figures

2.1 Internet of Medical Things [18]. 8
2.2 System architecture of IoMT [19]. 8
2.3 RFID Scenario [26]. 9
2.4 A typical sensing node [26]. 10
2.5 Fog based architecture for healthcare systems [45]. 15

3.1 An example of blockchain which consists of a continuous sequence of blocks [64]. 21
3.2 Block Structure [64]. 22
3.3 Percentage distribution of the use cases of BC [78]. 29
3.4 Communication in Healthcare System to Cater Disaster Situations [93]. . . . 35
3.5 The digital twin concept for personalized medicine [97]. 38

4.1 Deployment in ganache. 44
4.2 Use Case Diagram. 45
4.3 Sequence diagram with the smart contract procedures. 46
4.4 Class Diagram. 46
4.5 Login page. 47
4.6 Registration page. 47
4.7 Home page. 48
4.8 Home page. 48
4.9 Patient Health Record Retrieval and Heart Rate Monitoring. 49
4.10 Patient health records. 49
4.11 Patient heart rate status. 49
4.12 Heart rate prediction. 50
4.13 List of medications. 51
4.14 Patient page. 51

List of Tables

2.1 Categories and examples of tools used in the IoMT framework. 11

3.1 Performance of PoW , PoS , DPoS and PBFT 27
3.2 Exploring Blockchain Classifications Based on Patient Data Transactions in Healthcare 28

List of Abbreviations

ABI Application Binary Interface

BSN Body Sensor Network

CC Cloud Computing

DIY Do It Yourself

DOS Denial of Service

DT Digital Twin

DTH Digital Twin Healthcare

DTPD Digital Twin Product Design

ECG electrocardiogram

EEG electroencephalogram

EHR Electronic Health Record

EMG Electromyography

EMR Electronic Medical Record

FC Fog Computing

HDA Health Data Analytics

HIPAA Health Insurance Portability and Accountability Act

IoMT Internet of Medical Things

IoT Internet of Things

IT Information Technology

MITM Man In The Middle

RFID Radio Frequency Identification

RPM Remote patient monitoring

SHS Smart Healthcare System

WSN wireless sensor network

Chapter 1

General Introduction

In today's world, numerous diseases pose a significant threat to individuals, particularly the elderly population. Conditions such as heart rate irregularities, high blood pressure, and diabetes, among others, are becoming increasingly prevalent due to the challenges of modern living. To safeguard themselves, people must actively monitor these vital signs on a daily basis. Therefore, our project aims to develop a blockchain and digital twin-based system for monitoring patients' heart rates using smart devices.

This system will continuously collect heart rate data from the smart devices and promptly analyze it to determine if the heart rate falls within the normal range. Real-time monitoring of this information will enable timely interventions, ensuring early detection of any abnormalities. Storing this data on a secure blockchain platform will prevent unauthorized access and malicious use.

In this project, our goal is to conduct virtual check-ups for patients to assess the effects of medications on their physical bodies. By doing so, we aim to make informed decisions regarding treatment options and improve the accuracy of diagnoses. This approach will ultimately lead to effective solutions for individuals, reducing the cost and time associated with traditional consultations.

Additionally, the system will facilitate doctors in accessing patients' diagnoses and health records stored on the blockchain. By utilizing this information, the system will provide doctors with insights regarding any increases or irregularities in heart rate. Furthermore, it will offer recommendations for suitable medication, enabling doctors to virtually test the efficacy and safety of medications before prescribing them to patients.

By combining the power of blockchain technology, digital twin concepts, and real-time monitoring, our system aims to enhance the healthcare industry's ability to prevent and manage heart-related issues effectively.

Our work is structured into five chapters:

- The first chapter presents a general introduction, providing a foundation for the subsequent content.
- The second chapter focuses on Internet of Things (IoT) based healthcare monitoring systems and their applications, technologies, and advancements.

- The third chapter delves into the utilization of Blockchain and Digital Twin technologies for healthcare monitoring.
- The fourth chapter outlines the steps involved in building our application, including the tools and technologies utilized.
- The final chapter analyzes the results obtained from our work and provides a comprehensive discussion of our findings, along with suggestions for future research and development.

Chapter 2

Internet of Thing based healthcare monitoring system

2.1 Introduction

Health monitoring is the act of assessing one's physical, functional, and cognitive status in order to spot changes that could be signs of a health issue and to enable the right kind of intervention. Health monitoring is crucial when it comes to prevention, especially if early disease identification could save suffering and medical costs. The early detection and treatment of many diseases can significantly enhance the patient's options for medical care. The use of sensors can detect people at risk by monitoring and transmitting vital signs to medical professionals, who may then decide what needs to be done to safeguard the patient's health. This is particularly true in the case of cardiovascular illnesses and diabetes. On the other hand, health monitoring involves keeping track of any aspect of a structure's health using consistently measured data, analytical simulations, and heuristic experience in order to describe the present and expected performance of the composite part in advance for at least the most serious limit events. The minimum standards needed for analytical modeling for trustworthy computer simulations, as well as how measurements, loads, and tests are planned and carried out in conjunction with the analytical simulations, are the most significant differences between health monitoring and a typical in-depth composite part evaluation and testing practice.

2.2 Internet of Things

The term Internet of Things (IoT) was coined by Kevin Ashton in 1999 and refers to the data on the internet that are connected to an evolving global service architecture [1]. IoT is the result of advanced research on information and communications technology. It stands for an interconnected network of devices and objects that can collect and exchange data through the internet. These devices can include anything from smartphones, sensors, and smart appliances to vehicles and industrial machinery. The idea behind IoT is to make our world more efficient and productive by allowing devices to communicate and work together seamlessly, often without human intervention. IoT has the potential to revolutionize industries such as healthcare, transportation, manufacturing, and agriculture by providing real-time data that can improve processes and inform decision-making. However, the proliferation of IoT devices also raises concerns around data security, privacy, and the ethical implications of collecting and using personal data [2, 3].

2.2.1 Internet of Things Architecture

The current Internet relies on the TCP/IP protocol stack for communication between network hosts, which was proposed a long time ago. However, with the advent of the IoT and the connection of billions of objects, there is a need for a more robust architecture due to the increased traffic and data storage requirements. Privacy and security concerns also pose significant challenges for IoT.

To address these issues, the proposed architecture for IoT must consider factors such as scalability, interoperability, reliability, and quality of service (QoS). As IoT connects various devices and enables information exchange, network traffic and storage needs will exponentially increase. Therefore, the development of IoT relies on advancements in technology and the design of new applications and business models.Generally, IoT security architecture is divided into six layers. These layered architectures aim to enhance the security of IoT systems by providing multiple levels of protection against cyber threats, unauthorized access, and data breaches.

1. **Coding Layer:** The coding layer serves as the fundamental component of the IoT, providing identification for the objects involved. Within this layer, each object is assigned a unique ID, enabling easy differentiation between objects [4].

2. **Perception Layer:** The device layer in the IoT provides physical attributes to each object. It incorporates various types of data sensors such as RFID tags. This layer collects valuable information from sensor devices associated with the objects and transforms it into digital signals. These signals are then transmitted to the Network Layer for further processing and action[5].

3. **Network Layer:** The Communication Layer plays a vital role in the IoT architecture by receiving digital signals from the Perception Layer and transmitting them to the processing systems in the Middleware Layer. It utilizes various transmission mediums such as WiFi, Bluetooth, 3G, etc. Its primary purpose is to facilitate the seamless exchange of information between different layers of the IoT ecosystem[6].

4. **Middlware Layer:** The Middleware Layer is responsible for processing the information obtained from the sensor devices. It incorporates technologies such as cloud computing and ubiquitous computing to enable direct access to the database for storing the necessary information. By employing intelligent processing equipment, the received information is analyzed and automated actions are performed based on the processed results. This layer plays a crucial role in executing intelligent and automated operations within the IoT ecosystem [7].

5. **Application Layer:** The Application Layer is where the potential of IoT is realized across various industries by leveraging the processed data. This layer plays a vital role in driving the development of IoT networks on a large scale. By utilizing the capabilities of IoT, this layer facilitates the integration of intelligent solutions into different domains[8].

6. **Business Layer:** The Management and Research Layer is responsible for overseeing and managing the applications and services of IoT. It plays a crucial role in conducting research and development activities related to IoT. This layer focuses on generating innovative business models and formulating effective strategies to ensure the successful implementation of IoT solutions [9].

2.2.2 Applications in Internet of Things

The majority of the everyday apps we often encounter are already intelligent, but they are unable to connect and share essential information, which will result in the creation of a broad variety of creative applications [10]. These newly developed apps with some autonomy would undoubtedly enhance the standard of our lives. There are now a handful of these apps on the market, and more might be developed in the future which would be very beneficial. We briefly discuss a couple of these uses in this part. To summarize, the following applications are found to be of the most interest[11]:

- **Smart Wearable**: Are wearable devices, low energy consumption, equipped with sensors and networked to collect data on users to monitor daily physical activity (to keep track of progress) or other information useful for health to identify possible problems on time and do prevention.
- **Smart Environment**: Innovative IoT technologies will enable the prediction of natural disasters like floods, fires, earthquakes, and more. These advancements will also facilitate effective monitoring of air pollution in the environment.
- **Smart Home**: IoT will offer DIY solutions for home automation, providing the capability to remotely control household appliances according to individual preferences. This technology will enable effective monitoring of utility meters, energy consumption, and water supply, leading to resource conservation and the early detection of anomalies such as overloading and water leaks. Furthermore, IoT will facilitate the implementation of reliable encroachment detection systems, enhancing home security and preventing burglaries. Additionally, gardening sensors will play a significant role by measuring essential factors like light, humidity, and temperature, while also automating plant watering based on their specific requirements.
- **Smart City**: A network of sensors can be used to efficiently manage water resources, transport, energy, waste collection, etc., which would reduce pollution and waste and increase the comfort of citizens.
- **Smart Hospitals**: Hospitals will integrate smart and adaptable wearables embedded with RFID tags, which will be provided to patients upon their arrival. These wearables will enable not only doctors but also nurses to monitor patients' vital signs such as heart rate, blood pressure, temperature, and other relevant conditions. This monitoring capability will extend beyond the confines of the hospital premises, allowing healthcare professionals to track patients' health status both inside and outside the hospital environment [12].
- **Smart Agriculture (Precision agriculture)**: Through the utilization of a network comprising sensors and actuators, it becomes possible to effectively monitor the health status and specific requirements of crops. This enables the optimization and precise allocation of resources such as water, fertilizers, and other necessary inputs, resulting in a more efficient and targeted approach to agriculture [13].

2.2.3 Challenges of Internet of Things

The implementation of IoT in various industries, including healthcare, has the potential to revolutionize the way we live and work. However, there are several challenges that need to be addressed to ensure that the technology is used effectively and safely. In this part, we will discuss the challenges of implementing IoT.

1. **Data security and privacy concerns**

   The IoT enables the localization and accessibility of everything and everyone, leading to a notable enhancement in our quality of life. However, the widespread adoption of IoT is hindered by concerns regarding the security and privacy of user data. Without a sufficient level of confidence in these areas, many individuals may be reluctant to embrace IoT technologies. Therefore, it is crucial for IoT to establish a robust security infrastructure in order to gain broad acceptance. Here are some potential challenges associated with IoT:

   (a) **Unauthorized Access to RFID:** A significant concern in the realm of IoT is the unauthorized access to tags that store identification data, which poses a serious threat to the confidentiality of user information. This issue requires immediate attention and mitigation measures. It is not only possible for malicious individuals to read the information stored in the tags but they can also manipulate or potentially even damage the tags [14].

   (b) **Sensor-Nodes Security Breach:** WSNs are vulnerable to various types of attacks due to the sensor nodes being involved in part of a bi-directional sensor network, which means other than the transmission of data, acquisition of data is also possible[15]. Outlined some of the expected attacks, which include jamming, tampering, Sybil, flooding, and a few more, which are summarized below:

      - Jamming disrupts the entire network by interfering with sensor node frequencies.
      - Tampering is a type of attack in which the attacker extracts or modifies node data in order to create a controlled node.
      - The Sybil attack claims several pseudonymous identities for a node, giving it significant power.
      - Flooding is a kind of DOS attack triggered by a high volume of traffic, resulting in memory exhaustion.

   (c) **Cloud Computing Abuse:** Cloud computing is a large network of convergent computers that share resources. These shared resources are vulnerable to a variety of security concerns, including MITM attacks, phishing, and so on. Steps must be made to assure the clouding platform's total security. Cloud Security Alliance highlighted various potential concerns, including malicious insiders, data loss, account hijacking, and egregious usage of shared computers, which are outlined below[16]:

      - The Malicious Insider danger implies that someone from the inside with access to the user's data may be involved in data modification.
      - Data Loss is a danger in which any unauthorized user with unauthorized network access can change or remove existing data.
      - MITM is a type of Account Hijacking attack in which the attacker can alter or intercept communications between two parties.

- Cloud computing has the potential to be exploited in monstrous ways because if an attacker can upload malicious software to the server, for example, via a zombie army (botnet), the attacker might gain control of many additional associated devices.

2. **Interoperability issues**

   Interoperability is a significant barrier to IoT applications in a variety of industries, including healthcare, it is typical for these devices to employ several communication protocols. This can make it difficult for various devices to communicate with one another and properly share data. A hospital, for example, may have IoT devices from many vendors that interact using different protocols. This can make data sharing across devices challenging, resulting in incomplete or erroneous information. As a result, patient care and decision-making may suffer. This might make it difficult for the devices to communicate data, resulting incomplete or incorrect information. Standardization of communication protocols is critical for addressing interoperability difficulties. Standardization guarantees that devices from many manufacturers may interact with one another using the same language. This promotes data exchange and improves the overall efficacy of IoT devices [11].

3. **Need for reliable connectivity**

   In addition to these challenges, the need for reliable connectivity is crucial for IoT systems to function correctly. Poor connectivity can cause delays or loss of data, leading to inaccurate or incomplete information. This can have significant consequences, particularly in healthcare, where timely and accurate data can be critical in making informed decisions.

2.3 Internet of Things for healthcare

The internet of medical things (IoMT) refers to a group of devices that are linked to the internet and are used to offer health-related services [17]. Essentially, IoMT is a connected framework of medical equipment, software programs, and services, as illustrated in Figure 2.1. Specifically, connecting devices and sensors allows healthcare organizations to improve the efficiency of their clinical operations and workflow management, as well as monitor patient health even from remote locations. By integrating the digital and physical worlds, IoMT speeds up the diagnosis and treatment process with greater accuracy, leading to better patient health outcomes and real-time modification of patient behavior and health status [18]. The connection of medical devices will have a significant impact on patients and clinicians.

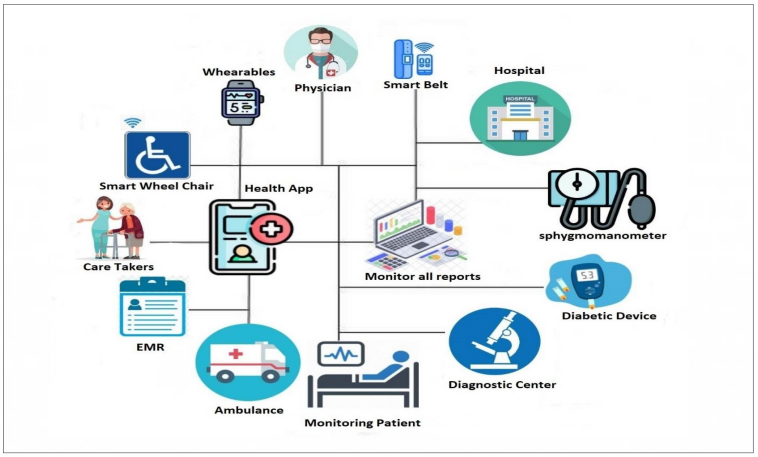

Figure 2.1: Internet of Medical Things [18].

2.3.1 Internet of Medical Things System Architecture

The majority of modern IoMT systems include four layers, as indicated in Figure 1.2. These layers span the entire data life cycle, from biometric data collection to storage and visualization for medical analysis. The patient can also view their current state of health generally thanks to the cloud.

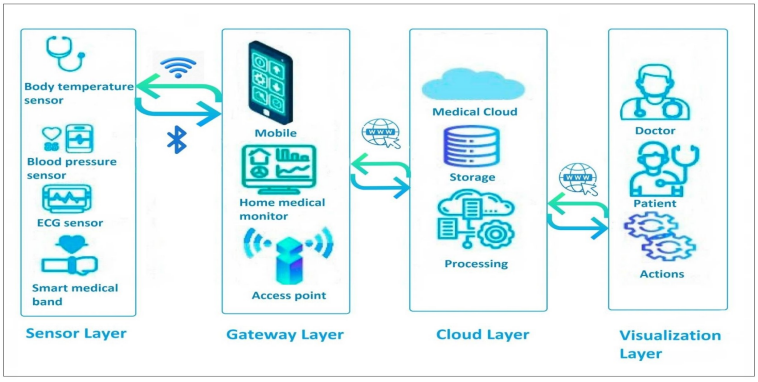

Figure 2.2: System architecture of IoMT [19].

- **Sensor/Perception layer**: All devices connected to the IoMT network to serve medical purposes belong in the monitoring and handling group. Any medical information obtained from any medical sensor node is intended to pass through the IoMT network and reach a physical person [19].
- **Gateway layer**: Is a group of nodes that have the computing power to operate a convoluted routing protocol and serve as the state administrators for lower SNs[20]. These are capable of carrying out the most simple AI-based inquiries as well as basic pre-processing duties including data validation and short-term data storage. Additionally, these middle ware units utilize the internet to send the sensor data they have acquired to the cloud layer.
- **Cloud layer**: This is in charge of handling the data received from the gateway's storage, analysis, and provision of secure access. Data processing may be used to identify any changes in the patient's health, which will then be provided to medical specialists for further consideration[20].
- **Application layer**: This displays the data to physicians and patients for monitoring. It also includes advice from the doctor based on the patient's medical condition[21]. Examples of action include suggesting or altering a wide range of medications.

2.3.2 Technologies Used for the Collection of Sensor-Based Medical Data

IoMT-based SHS use a variety of methods, including BSN, WSN, and RFID , to gather and transmit sensor data to servers [22].

- **BSN**: Is an Internet of Things (IoT)-based medical technology that uses a variety of wireless sensor nodes with low weight and power consumption to monitor the health of patients [23].
- **Radio Frequency Identification (RFID):** Is a contactless method for automatically identifying targets with radio frequency and two-way data transfer in several zones designated by their distinctive designations [24]. The RFID consists of 3 parts, namely, the reader, database management system, and radio frequency electronic tag [25]. The RFID tag's performance in terms of resonant frequency, gain and reading range [26].

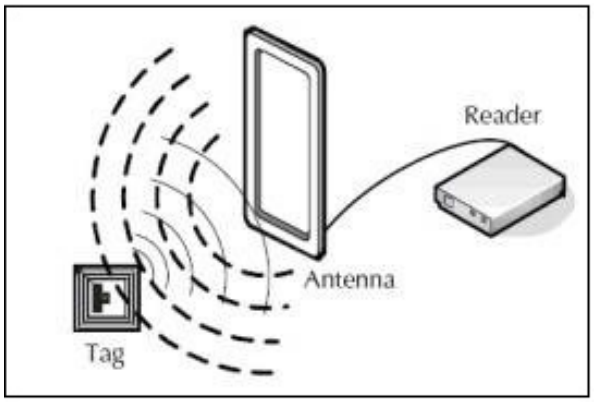

Figure 2.3: RFID Scenario [26].

- **WSN**: Is a collection of various monitoring sensors dispersed throughout a homogeneous or heterogeneous environment. is a sensor network that is connected wirelessly with the help of different communication protocols. This review compares the brief overview of different deep learning algorithms and the WSN used to analyze and strengthen IoT in healthcare [27]. WSN can be utilized in IoMT to track the physiological state of the subject of the observation in real-time [28].

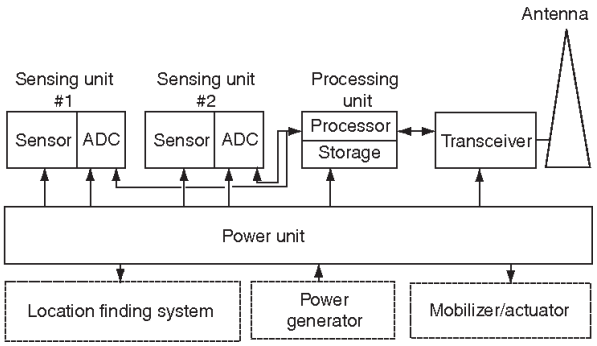

Figure 2.4: A typical sensing node [26].

2.3.3 Types of Internet of Medical Things devices

A variety of sensors and devices attached to the IoMT infrastructure are used inside the human body, outside the human body, or in the environment.

Category of devices	Location	Examples
Wearables Devices	Refers to a device worn by a person that can monitor multiple biometric, such as heart rate, step count ,sleep habits ,and other related information.	Include smartwatches, fitness trackers, and other health monitoring devices.
Remote patient monitoring (RPM) devices	These devices allow healthcare providers to remotely monitor patient health and vital signs in real-time, often enabling early detection of health problems.	Include blood glucose monitors, blood pressure monitors, and other medical monitoring devices.
Implantable devices	These are medical devices that are implanted in the body to monitor and/or treat health conditions.	Include pacemakers, implantable cardioverter defibrillators, and neurostimulators.
Smart inhalers	These devices can track the patient inhaler use and provide healthcare providers with feedback on medication compliance and efficacy.	Cohero Health,Propeller Health,NuvoAir,Hailie...
Telehealth devices	These are devices used to facilitate virtual visits and consultations with healthcare providers.	Remote monitoring devices,Telemedicine carts,Mobile health apps...
Smart pills	These are ingestible sensors that can monitor medication adherence and track health data from within the body.	SmartCapsule,PillCam..
Medical robots	These are devices used in healthcare to assist with tasks such as surgery, medication dispensing, and patient monitoring.	Da Vinci Surgical System,InTouch Health RP-VITA,Xenex Germ-Zapping Robots...

Table 2.1: Categories and examples of tools used in the IoMT framework.

2.3.4 Internet of Things Based Healthcare Systems and Their Applications

IoT-based healthcare systems facilitate people's lives in a variety of ways, such as:

1. **Remote healthcare**: Wireless IoT-driven solutions bring healthcare to patients rather than the patient to healthcare. IoT-based sensors are used to gather data, which is then securely processed before being shared with medical specialists so they can make the best suggestions [29].

2. **Real-time monitoring**: IoT-driven non-invasive-monitoring sensors collect comprehensive psychological information [29]. Gateways and cloud-based analysis manage the storage of data.

3. **Preventive care**: IoT healthcare systems use sensor data, which helps with the early detection of emergencies and alerts family members. Machine learning for health-trend tracking and early anomaly detection is achieved through the IoT approach [29].

2.3.5 Internet of Things Applications in Health Monitoring

IoT could have various applications in the medical industry to enhance life quality, save lives, and lower treatment costs. Utilizing IoT-based technology, the medical sector may enhance the healthcare system's capacity to reduce human error while also streamlining the treatment process and patient and caregiver quality of life. Doctors can benefit from therapies and symptom prediction using IoT-based monitoring systems before beginning a diagnosis. A monitoring system can also sound an alert in cases of a medical emergency, such as an elderly patient tripping and patients acting strangely in an intensive care unit (ICU). The following are a few examples of IoT-based healthcare use cases or application areas.

1. **Health Monitoring:** Medical sensors and wearable devices can capture vital health signs for health monitoring and personal fitness program. sensors can capture blood pressure, blood glucose, ECG, heart rate and body temperature, etc to monitor pediatric and aged persons [30].

2. **Personal Fitness Monitoring:** This class of sensor application is for those who want to stay fit and healthy. Sensors used here are weight measuring sensors, activity monitors sensors like walking time counter, step counter, speed counter, calorie counter, and heart rate and blood pressure measuring sensors [30].

3. **Chronic Disease Monitoring:** Millions of people are suffering from Chronic diseases like cancer, diabetes, asthma, heart diseases, sleep disorders, and arthritis. special care is needed for such kind of disease. It required disease-specific diet and treatment plans. By using physiological sensors like ECG , EMG and EEG with activity monitor sensors like step counter, speed counter, calorie counter, etc can be used for early detection of symptoms and adverse changes in a patient's health condition that will cause early and timely medical treatments [31].

4. **Safety Monitoring:** There are many sensors and wearable devices available to improve the healthcare system for the aged and pediatric population. sensor for fall detection, epileptic seizure detection, and heart attacks symptom detection can be used for the safety monitoring of the patient. These sensors have a push button that sends alarm signals to caregivers or family members [31].

5. **Medication Management:** It is the general human tendency of noncompliance with medication prescribed by physicians. this may cause a threat to patient health as well as financial loss. IoT-based intelligent packaging method for medicine boxes can be used for medication management. This packaging method has controlled sealing which is based on delaminating materials and that is controlled by wireless communications [31].

6. **Real Time Location Tracking:** Through IoT Patient and equipment used for treatments tracking is possible. By using RFID tags health care providers can track real-time location, assigned physicians and progress of treatment, etc. Medical equipment and devices like defibrillators, ECG machines, spirometry, nebulizers, etc can be tagged with sensors and tracked easily with IoT [32].

2.3.6 The Significance of Internet of Thing Based Healthcare-Monitoring Systems

The development of monitoring systems for healthcare is attracting a lot of interest from researchers and industry experts in the medical field. Several successful research projects have been conducted in this area, and many more are currently in progress [33]. The rising number of elderly people and patients with chronic illnesses is directly contributing to a considerable rise in the number of care gaps being offered by healthcare providers. The primary drawback is that healthcare is only offered in hospitals, making it unsuitable for the elderly and those with disabilities and frequently unable to fulfill their needs [34]. The IoT, with the help of sensor values and telecommunications, provides an effective and practical solution to the issue of real-time monitoring of the health status of the elderly.

It has been shown that the IoT, in conjunction with smart technologies, can provide various improved and enhanced services. Using sensors, researchers have developed various emergency systems using technologies that enable intelligent and remote wireless communication. These technologies have been used for various medical purposes, particularly in monitoring the health of the elderly. This way, data can be collected on general health and dangerous situations by capturing important vital signs [35].

2.3.7 Challenges and issues

Every emerging technology has some challenges. IoT-based Healthcare Monitoring has some bottlenecks and challenges too. Some of them are as follows:

- **Security and Privacy:** Healthcare devices and applications collect personal health information, and these devices are connected to the Internet and can be accessed anytime, anywhere. So it may trick hackers into stealing your personal information. Personal health information must be used after patient approval [36]. Data security in healthcare should address the following challenges [37]:
  - Physical security of health devices.
  - Providing secure routing for data communication.
  - Providing data transparency in the cloud computing environment.
  - Maximum security with minimum resource consumption.

In IoT-based healthcare, patient health information is collected by various medical sensors and wearable devices [37]. Medical devices need to connect to other devices and multiple users to collect data. Thousands of vendors manufacture devices without following standard rules and regulations regarding compatible interfaces and protocols for communication between devices, data collected by these devices is therefore not visible to other devices.

- **Device Designing issue:** IoT devices used in healthcare are small sensors with processors with low processing power, small storage capacity, and limited battery power. Also, IoT devices are inherently mobile and connected to the Internet. Wearable devices need to connect to various networks to provide medical information to caregivers [38]. The development of IoT devices with higher computing power, more storage capacity, higher battery performance, and security in case of mobility complaints remains a research challenge.

- **Scalability:** IoT devices used in healthcare are small sensors with processors with low computational power, small storage capacity, and limited battery power. Also, IoT devices are inherently mobile and connected to the Internet. Wearable devices need to connect to various networks to provide medical information to caregivers [38]. Developing IoT devices with higher computing power, greater storage capacity, higher battery performance, and security in the face of mobility obstacles remains a research challenge.

- **Trust:** Information generated and delivered by medical devices is vulnerable to security attacks, although the information looks correct, it can be infected with malware or corrupted during data transfer [39]. Hackers can use this information to harm individuals as caregivers make decisions and develop treatment plans based on the information generated by these sensors [40]. This falsified information can lead to life-or-death decisions. So how can we trust treatments based on medical sensor data, this is a major challenge in IoT-based health monitoring.

2.4 Cluster Computing

Cluster computing is a type of computing that connects multiple computers (nodes) to form a single high-performance computing system. The nodes in a cluster are typically connected by a high-speed network and work together to perform complex computing tasks that are difficult or impossible for a single computer to complete in a reasonable time frame. In a cluster computing system, the workload is distributed among the nodes [41]. With the increasing popularity of virtualization technology and software as a service (SaaS) and other cloud-based services, cluster computing began to evolve into what it is today, which has become known as cloud computing.

2.5 Cloud Computing

Cloud computing can play a key role in containing healthcare integration costs, optimizing resources, and ushering in a new era of innovation. The current trend is aimed at accessing information anytime, anywhere[42]. This can be achieved when health information is moved to the cloud. This new delivery model can make healthcare more efficient and effective and reduce the cost of technology budgets. In addition, the protection of sensitive patient information and the importance of Network and Communication Technologies Vol. There are also certain obstacles due to concerns related to regulatory compliance, HIPAA , etc...

Despite these security and privacy risks, healthcare organizations can certainly leverage cloud computing solutions to deliver significant benefits, including Improving the quality of service to patients, reducing overall healthcare costs, and exchanging data between different systems. This capability is much needed in healthcare [43]. For example, cloud computing can help a healthcare provider shares information such as his EHR , medical certificates, prescriptions, insurance information, and test results stored in various information systems.

2.6 Fog Computing

Central control and data storage seem to be required in large-scale IoT networks to ensure efficient and successful IoT infrastructures. To do this, IoT networks may benefit from major resources like computing power and storage provided by cloud computing. However, there are certain disadvantages to cloud computing [44]. The communication delay that occurs when an IoT device and the cloud are in communication is one of the main downsides of cloud computing. One of the most popular solutions is to create a new layer, called fog computing, which acts as a link between cloud computing and edge computing.

2.6.1 Fog Computing Service in the Healthcare Monitoring

Healthcare systems are facing major hurdles due to rising patient numbers and chronic diseases. Most hospitals manually measure the values of biometric parameters and then enter the data into the system. Based on the patient's medical information, the medical team will take additional steps. In hospitals, manual methods waste a lot of time. For hospitals, automating processes saves unnecessary money and time. Healthcare systems need to save costs while providing quality care to patients [45].

Fog computing can be used in medical systems to simplify patient data management and analysis of information generated by networks of sensors. Integrating fog computing into healthcare systems can remotely monitor patients, improve efficiency and quality, and reduce healthcare costs [44, 46]. The FC framework is distributed throughout the network and uses many different devices. These units are widely connected at the network edge and provide flexible communication, storage, collaboration variables, and computational capabilities. FC offers many advantages in various areas such as real-time, low latency, and high response time, especially in healthcare applications.

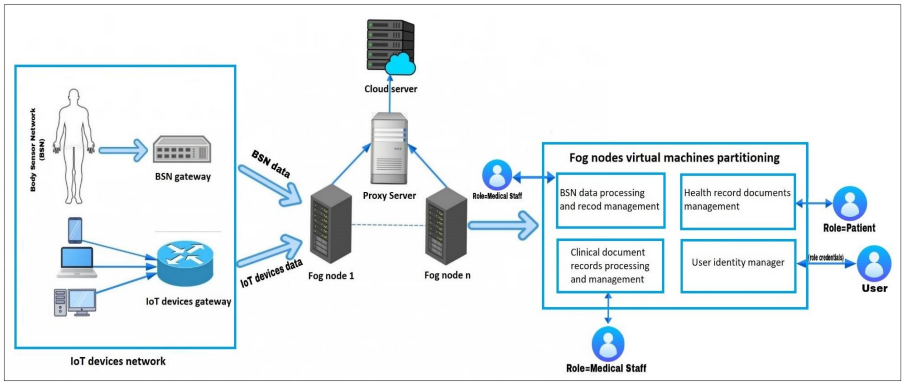

Figure 2.5: Fog based architecture for healthcare systems [45].

2.6.2 Features of Fog Computing

Current Integrated CC Frameworks Face Others IoT application topic. For example, Time-sensitive demands such as augmented reality and audiovisual Streaming are not supported. Fog solves these problems [47]. FC can enhance healthcare monitoring by providing real-time data processing and analysis at the edge of the network. Some of the main features of fog computing in healthcare monitoring include:

- **Real-time monitoring:** Fog computing enables healthcare providers to monitor patients in real time by processing data locally at the edge of the network. This can improve the accuracy and timeliness of diagnoses, leading to better patient outcomes.
- **Data security:** Fog computing provides additional layers of security by encrypting data and processing it locally. This can help protect sensitive patient information and reduce the risk of data breaches.
- **Reduced network latency:** By processing data locally, fog computing can reduce network latency and improve the responsiveness of healthcare monitoring systems.
- **Bandwidth efficiency:** Fog computing reduces the amount of data that needs to be transmitted to the cloud, improving network bandwidth utilization and reducing network congestion.
- **Scalability:** Fog computing enables computing resources to be added or removed dynamically, making it easy to scale healthcare monitoring systems based on changing demands.

2.7 Edge Computing

Edge computing is a connectivity paradigm that focuses on placing processing as near as feasible to the source of data to decrease latency and network use. Edge computing, in simple words, implies executing fewer activities on the cloud and relocating them to designated locations, such as a user's PC, an IoT device, or an interface server. Edge computing broadly is all computing outside the cloud happening at the edge of the network, and more specifically in applications where real-time processing of data is required [48]. CC operates on big data while edge computing operates on "instant data" which is real-time data generated by sensors or users.

2.7.1 Edge Computing Use Cases in Healthcare

Edge computing has the potential to transform the healthcare industry by enabling real-time data processing, improving patient outcomes, and reducing costs. Here are some potential use cases of edge computing in healthcare:

1. **IoT Devices:** IoT devices generate vast amounts of data that need to be processed in real-time, making edge computing an ideal solution for more effective user experiences, intelligent technologies that access the internet can benefit from executing coding on the machine itself instead of on the server [48].

2. **Medical Monitoring Tools:** Medical monitoring equipment must answer in real-time without having to wait for a response from a cloud platform.

3. **Remote Patient Monitoring:** Edge computing can be used for remote patient monitoring, allowing patients to be monitored in real-time and providing alerts to healthcare providers when necessary. For example, wearable devices can collect vital signs data such as heart rate, blood pressure, and oxygen levels, and send it to edge nodes for processing. Edge nodes can analyze the data in real-time, alerting healthcare providers if there are any abnormalities or changes in the patient's condition [48, 49].

4. **Telemedicine:** Edge computing can enable telemedicine by providing real-time video and audio communication between patients and healthcare providers. By processing the data locally, edge computing can reduce latency and improve the quality of the video and audio feeds. This can be particularly important for remote areas where access to healthcare is limited [50, 51].

5. **Predictive Analytics:** Edge computing can be used for predictive analytics, enabling healthcare providers to detect and prevent illnesses before they occur. For example, edge nodes can process data from electronic health records, wearable devices, and other sources to identify patterns and trends in patient health. This can help healthcare providers to detect and treat illnesses earlier, reducing costs and improving patient outcomes [52, 53].

6. **Medical Imaging:** Edge computing can improve the speed and accuracy of medical imaging by processing data locally. For example, edge nodes can be used to process images from MRI machines, enabling healthcare providers to quickly and accurately diagnose conditions such as tumors, aneurysms, and other abnormalities [54, 55].

2.7.2 Features of Edge Computing

Edge computing has some characteristics similar to cloud computing. However, the differentiators that make edge computing unique are:

- **Dense Geographical Distribution:** Edge computing brings cloud services closer to users by deploying many computing platforms in edge networks [56]. The dense geographical distribution of the infrastructure assists in the following ways:
  - The network administrators can facilitate location-based mobility services without traversing the entire WAN [56].
  - Big data analytics can be performed rapidly with better accuracy [57].
  - The Edge systems enable real-time analytics at scale [58].
- **Mobility Support:** With the increasing number of mobile devices, Edge computing is also catering to mobility requirements. In edge computing, mobility denotes the capability of edge devices to relocate from one place to another without losing their connectivity to the network, thereby, ensuring interrupted computing services[59]. Mobility is a crucial attribute of edge computing as it enables edge devices to be utilized in different environments and contexts like smart homes, factories, and transportation systems.
- **Location Awareness:** The location-aware attribute of edge computing allows mobile users to access services from edge servers closest to their physical location [60]. Users can locate electronic devices using a variety of technologies such as cellular infrastructure, GPS, and wireless access points.
- **Proximity:** Edge computing brings computing resources and services closer to users, improving their experience. The availability of computing resources and services in an on-premises environment enables users to leverage network contextual information to make offloading decisions and service usage decisions.
- **Heterogeneity:** Heterogeneity in EC refers to the existence of different platforms, architectures, infrastructure, computing, and communication technologies used by EC elements (end device, edge server, and network) [61]. End-device heterogeneity makes software, hardware, and technology variations the main drivers of heterogeneity. Edge server-side heterogeneity is primarily due to APIs, custom policies, and platforms. These existing differences create interoperability issues and pose a significant challenge to successful EC deployments. Network heterogeneity refers to the different communication technologies that affect the network Providing edge services.
- **Low Latency:** Edge computing enables the processing of data in near real-time, reducing the time it takes to receive results and make decisions. This is particularly useful in applications that require quick response times, such as autonomous vehicles and industrial automation systems.

2.8 Conclusion

The Internet of Things (IoT) has emerged as a transformative technology that offers new opportunities to improve patient outcomes, reduce healthcare costs, and enhance the overall quality of care. In this chapter, we first present a comprehensive overview of IoT, including IoT technologies and architecture, and we discuss IoT's challenges. We then explore the potential of the IoT in healthcare and provide a brief overview of cluster computing and the Cloud-Edge-Fog (CEF) paradigm in healthcare.

Overall, the combination of IoT and CEF holds significant promise for improving healthcare delivery, enhancing patient outcomes, and lowering healthcare expenditures. However, some challenges need to be addressed, such as privacy and security concerns, interoperability, and the need for new skills and expertise. In the next chapter, we will provide a brief background on BlockChain and Digital Twin technologies, specifically Healthcare Digital Twin. We will also critically review some relevant research studies.

Chapter 3

Blockchain and Digital Twin for healthcare monitoring

3.1 Introduction

In this chapter, we will delve into the potential of blockchain technology in securing data. We will begin by introducing the fundamentals of blockchain, including its structure and consensus algorithms, understanding these fundamental aspects will provide a solid foundation for exploring the applications of blockchain technology in data security.

Furthermore, we will explore the concept of digital twins, with a specific focus on healthcare monitoring. We will provide an overview of digital twins, highlighting their capabilities and benefits in improving healthcare services.

Additionally, we will review previous works and research that have focused on healthcare solutions leveraging the combination of blockchain and digital twin technologies. Examining these existing studies will provide valuable insights into the practical implementation and effectiveness of blockchain and digital twins in healthcare

3.2 Blockchain fundamentals

3.2.1 Introduction of Blochchain

BC is a decentralized node network that stores data. It is a great technology for protecting confidential data within the system. This technology facilitates secure data sharing while maintaining its confidentiality. It is the ideal tool for securely storing all relevant documents in one location in a safe manner, moreover, the BC is a decentralized peer-to-peer (P2P) network of personal computers called nodes, that maintains, stores, and records transaction or historical data [62, 63, 64]. BC is a sequence of blocks, which contain a list of transaction records. Figure 3.1 illustrates an example of a BC. Each block is composed of a header and body, where a block header contains the hash of the preceding block, which is referred to as the parent block, each block has only one parent, except the first block has no parent block it's called a genesis block, while the body block contains a list of transactions.

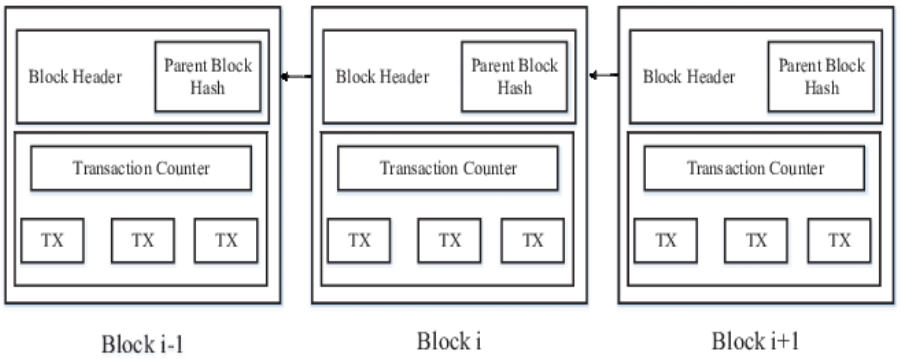

Figure 3.1: An example of blockchain which consists of a continuous sequence of blocks [64].

3.2.2 Blockchain Components

BC is a decentralized, distributed digital ledger that records transactions on a network of computers, it's called a "chain" because each block of data is linked to the previous one, creating a chain of blocks, the structure of a BC consists of three main components: blocks, transactions, and nodes.

- **Blocks:** A block is a package of data that contains information about transactions, such as the sender, recipient, and amount transferred. Each block is verified and added to the BC by network participants known as miners. Each block also contains a unique cryptographic hash that links it to the previous block in the chain, ensuring that no previous transaction can be altered without invalidating subsequent blocks.
- **Transactions:** A transaction is an exchange of value between two parties. In a BC, transactions are recorded in blocks and are publicly visible on the network. Each transaction is verified by nodes on the network and must meet certain criteria before it can be added to the BC.
- **Nodes:** Nodes are computers or devices that participate in the blockchain network. Each node maintains a copy of the blockchain and verifies transactions before adding them to the network. Nodes communicate with each other to ensure that each copy of the blockchain is up-to-date and accurate.

The structure of a blockchain is designed to be transparent, secure, and decentralized. By distributing the ledger across a network of nodes, no single entity has control over the entire BC, and it's extremely difficult to tamper with or corrupt the data in the BC.

3.2.3 Block structure

As previously stated, a block consists of the block header and the block body as shown in Figure3.2.

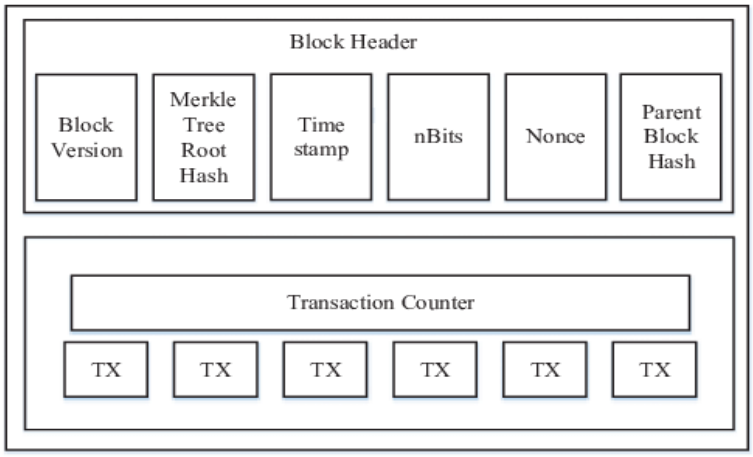

Figure 3.2: Block Structure [64].

In particular, the block header includes:

1. **Block version:** Indicates which set of block validation rules to follow.
2. **Merkle tree root hash:** The hash value of all the transactions in the block.
3. **Timestamps:** Current time as secondes in the universal time since January 1, 1970.
4. **Nbits:** Target threshold of a valid block hash.
5. **Nonce:** A 4-byte field, which usually starts with 0 and increases for every hash calculation.
6. **Parent block hash:** A 256-bit hash value that points to the previous block.

3.2.4 Consensus algorithms in Blockchain

Consensus is a key feature of BC technology that enables a decentralized network of computers to agree on the state of a distributed ledger without relying on a central authority or intermediary[65], in a BC network, the consensus is reached through a set of rules and protocols that ensure that all participants agree on the current state of the ledger, the most mechanisms that help us to implement this solution are:

1. **Proof of Work** (PoW): In a PoW consensus mechanism, participants in the network compete to solve complex mathematical problems to validate new transactions and add them to the BC, this requires significant computing power and energy consumption, making it an expensive and slow process [65, 66]. The basic idea behind PoW is to add a new block to the blockchain, a miner must first solve a difficult mathematical puzzle. This puzzle requires the miner to find a nonce (a random number) that, when combined with the block data and hashed, produces a hash value that meets certain criteria, such as being below a certain target value. The target value is adjusted based on the network's hash rate to maintain a consistent block production rate [66].

Algorithm 1: Proof-of-work algorithm

Input: a block of data D, a target value T
Output: a nonce N such that $H(D||N) < T$

```
// initialize the nonce to zero
N ← 0
// compute the hash of the data and nonce
H ← hash(D||N)
// iterate over nonces until the hash meets the target
while H > T do
    N ← N + 1 // increment the nonce
    H ← hash(D||N) // compute the new hash
end
return N
```

2. **Proof of Stake** (PoS): Is an alternative consensus algorithm used in some blockchain networks instead of Proof of Work (PoW). In PoS, validators, also called nodes or stakers, are chosen to create new blocks on the BC based on their ownership or share in the network [67]. Here is a simple explanation of how PoS works:

   (a) The network selects a validator to create the next block based on their stake in the network. The more stake a validator has, the more likely they are to be chosen.

   (b) The validator creates the block and includes a transaction fee for their work.

   (c) Other validators on the network verify the block and check that the transaction fee is reasonable.

   (d) If the block is valid, it is added to the BC, and the validator who created it receives the transaction fee as a reward.

   (e) Validators are incentivized to act honestly and not try to create invalid blocks or attack the network because their stake in the network is at risk of being lost.

Algorithm 2: Proof of Stake algorithm

Input: a block of data D, a list of validators V, their respective stakes S, a target value T
Output: a validator v who is chosen to create the next block

```
// calculate total stake
```
$totalStake \leftarrow \sum_{i=1}^{|V|} S_i$
```
// initialize the validator list
```
$validValidators \leftarrow$ empty list
```
// iterate over the validators
```
for $i \leftarrow 1$ **to** $|V|$ **do**
```
// calculate the probability of being selected
```
$p \leftarrow S_i / totalStake$
```
// add the validator to the list with probability p
```
for $j \leftarrow 1$ **to** $\lfloor p \rfloor$ **do**
add V_i to $validValidators$
end
```
// add the validator with the remaining probability
```
if $rand() < (p - \lfloor p \rfloor)$ **then**
add V_i to $validValidators$
end
end
```
// choose a validator from the list with a random selection
```
$v \leftarrow$ randomly select a validator from $validValidators$
return v

3. **Delegated Proof of Stake** (DPoS): Similar to PoS, but instead of every validator participating in the consensus process, token holders vote for a small number of delegates who are responsible for validating transactions and creating new blocks. This can lead to faster consensus and more efficient use of resources, but it can also lead to centralization [68]. In DPoS, stakeholders can vote for a set of validators, also known as delegates, who are responsible for validating transactions and creating new blocks. The number of delegates can vary from network to network, but it is typically around 20. The delegates are elected based on the number of votes they receive from stakeholders. The more votes a delegate receives, the more likely they are to be elected.

Algorithm 3: Delegated Proof of Stake algorithm

Input: a block of data D, a list of delegates D, their respective stakes S, a target value T
Output: the next block in the blockchain

```
// calculate total stake
```
$totalStake \leftarrow \sum_{i=1}^{|D|} S_i$
```
// initialize the delegate list
```
$validDelegates \leftarrow$ empty list
```
// iterate over the delegates
```
for $i \leftarrow 1$ **to** $|D|$ **do**
```
    // calculate the probability of being selected
```
    $p \leftarrow S_i / totalStake$
```
    // add the delegate to the list with probability p
```
    for $j \leftarrow 1$ **to** $\lfloor p \rfloor$ **do**
        add D_i to $validDelegates$
    end
```
    // add the delegate with the remaining probability
```
    if $rand() < (p - \lfloor p \rfloor)$ **then**
        add D_i to $validDelegates$
    end
end
```
// choose a delegate from the list based on a deterministic
   algorithm
```
$d \leftarrow$ choose a delegate from $validDelegates$ based on the algorithm
```
// validate transactions and create a new block
```
$block \leftarrow$ validate transactions and create a new block with delegate d
return $block$

4. **Proof of Authority** (PoA): In this algorithm, validators are known and trusted entities who are responsible for validating transactions and creating new blocks[69]. It is faster and more energy-efficient than PoW and PoS, but it can be more centralized. In PoA, the validators are known as authorities and are typically selected by the network organizers or the community. The selection is based on factors such as reputation, expertise, and trustworthiness. Once selected, the authorities are responsible for validating transactions and creating new blocks.

Algorithm 4: Proof of Authority algorithm

Input: a block of data D, a list of authorities A
Output: the next block in the blockchain

```
// select a random authority from the list
```
$a \leftarrow$ select a random authority from A
```
// validate transactions and create a new block
```
$block \leftarrow$ validate transactions and create a new block with authority a
return $block$

5. **Practical Byzantine fault Tolerance** (PBFT): Practical Byzantine Fault Tolerance is a consensus algorithm used in distributed systems to ensure that a network of nodes can reach an agreement on a particular state of the system, even in the presence of faulty nodes [70]. A client sends a signed request to the primary node of PBFT and should hear back directly from at least F+1 backups where F is the number of faulty nodes. If the client does not hear back soon enough, then the client broadcasts directly to backups and keeps sending its request until the request is replicated. The primary should set an order for every request made by the client, the protocol assumes valid signatures on all replicas and has some bounds on response times to ensure liveness is still possible in the case that responses are delayed arbitrarily.

Algorithm 5: Practical Byzantine Fault Tolerance algorithm

Input: a request r from a client
Output: the response to the client
`// send the request to all nodes`
broadcast r to all nodes;
`// pre-prepare phase`
for *node* i *in the network* **do**
  $<$ PRE-PREPARE, view, seq, digest(r) $>_i \leftarrow$ prepare message;
  send $<$ PRE-PREPARE, view, seq, digest(r) $>_i$ to all nodes;
end
`// prepare phase`
for *node* i *in the network* **do**
  wait for $2f$ PRE-PREPARE messages from different nodes for the same (view, seq) pair;
  $<$ PREPARE, view, seq, digest(r) $>_i \leftarrow$ prepare message;
  send $<$ PREPARE, view, seq, digest(r) $>_i$ to all nodes;
end
`// commit phase`
for *node* i *in the network* **do**
  wait for $2f + 1$ PREPARE messages from different nodes for the same (view, seq) pair;
  $<$ COMMIT, view, seq, digest(r) $>_i \leftarrow$ commit message;
  send $<$ COMMIT, view, seq, digest(r) $>_i$ to all nodes;
end
`// response phase`
if *node* i *received* $2f + 1$ *COMMIT messages for the same* (*view*, *seq*) *pair* **then**
  execute the request r and send the response to the client;
end

Each consensus algorithm has its own strengths and weaknesses, and the choice of algorithm depends on the specific use case and the trade-offs that are deemed most important.

3.2.5 Performances of Consensus Algorithm

The performance of a consensus algorithm can be measured by several metrics such as scalability, throughput, latency, fault tolerance, and energy efficiency. Here's a brief overview of each of these metrics:

Consensus algorithm	PoW	PoS	DPoS	PBFT
Basis for assigning accounting rights	Computing power	Stake	Stake Votes	Digital signatures and authentication
Threat to security	Concentration of power	Lack of active nodes	Destruction of the witnsses	Network partition attacks
Ressource consumption	The highest	Lower than PoW, higher than DPoS	The lowest	Hight
Average time generate blocks	10 min	64s	3s	Around 2-3 s
Typical application	Bitcoin,Ethereum	Peercoin	Bitshare	Hyperledger Fabric blockchain platform
fairness	Relativity fair	Relativity unfair	Relativity unfair	Relativity fair
Scaliblity	Good	Good	Good	Good

Table 3.1: Performance of PoW , PoS , DPoS and PBFT

3.2.6 Types of blockchain

The Blockchain can be categorized as follows [71]:

- **Public Blockchains** : Does not have any restrictions on the reading of the blocks and on submitting of the transactions for inclusion into the BC. This type is open to the public and anyone can participate as a node in the consensus process.

- **Private Blockchains**: Has limited to a predefined list of users with direct access to the blocks and submitting transactions.

- **Regulate Blockchains**: Is a type of BC technology that is subject to regulatory oversight and compliance requirements. In a regulated BC, the network and its participants are required to adhere to specific regulations and standards to ensure that the technology is being used securely and lawfully.

Another way of categorizing is by how the transactions are processed and how data is accessed, as shown in the following table.

	The processing of the transactions	
Access to the data	Permissioned	Permissionless
Public	Patients and healthcare providers can view patient data on the blockchain, but only authorized users with the appropriate permissions can add or modify data [72].	The decentralized nature of a public permissionless blockchain can make it difficult to ensure data accuracy and consistency [72].
Regulated	Patients and regulators have limited access to directly read and create transactions [72].	However, there is the risk of not having full control over who can access the network and view patient data [72].
Private	Network access is restricted to authorized participants such as healthcare providers and regulators who must meet specific compliance and regulatory requirements [73].	Anyone can join the network and participate in transactions, but access to sensitive patient data is restricted to authorized participants [73].

Table 3.2: Exploring Blockchain Classifications Based on Patient Data Transactions in Healthcare

3.3 Healthcare Blockchain

The healthcare industry faces a significant challenge in managing and safely retrieving the massive amount of personal health data generated through normal business operations and service provision, as well as from monitoring technologies like wearables. This data is typically inaccessible, non-standardized across systems, and difficult to understand, use, and share due to being pulled from various sources and stored in centralized IT systems. As a result, requesting, sending, receiving, and compiling patient data is a time-consuming and resource-intensive task. Proper management and safe retrieval of health data can help healthcare systems create comprehensive patient views, improve care quality and treatments, enhance communication, and ultimately improve health outcomes. The rise of BC technology has presented numerous new opportunities for healthcare applications.

3.3.1 The use cases of Blockchain in healthcare

Although there are many potential use cases for BC technology in healthcare, some of the most important ones include the following:

- **Electronic Medical Record**: One of the most common use cases for BC in healthcare is managing electronic medical records. EMRs stored in BC can provide a secure and transparent platform for managing and sharing patient health information. BC technology empowers patients to own and control their medical data, which they can access and share with their healthcare providers when they need it [74]. By storing EMRs on the BC, healthcare organizations can improve data security and prevent data breaches and unauthorized access.

- **Remot patient monitoring**: Telemonitoring of patients involves the collection of biomedical data via body area sensors and mobile devices to remotely monitor patients outside of the traditional healthcare setting. BC technology has been proposed as a means of storing, sharing, and retrieving remotely collected biomedical data. Research shows that BC platforms can support real-time patient monitoring applications and provide automated interventions in a secure environment [75].

- **Health insurance claims**: The healthcare industry can benefit from using blockchain technology to process insurance claims due to its transparency, decentralization, and immutability features [76]. Insurance claims processing is a critical aspect of healthcare, which involves the verification and payment of medical claims for healthcare services. The traditional method of processing and verifying health insurance claims can be slow, costly, and prone to errors. BC technology can enhance the efficiency, security, and transparency of health insurance claims to process.

- **Health data analytics**: BC technology, combined with new technologies such as deep learning and transfer learning techniques, enables predictive analytics of health data and offers unique opportunities to advance precision medicine research [76]. Health data analytics (HDA) is the process of collecting, processing, and analyzing large amounts of health data from various sources to generate insights into patient health, health trends, and health outcomes. HDA uses data analysis techniques such as statistical analysis, data mining, and machine learning to identify patterns and trends in healthcare data [77]. HDA's goals are to improve patient outcomes, reduce healthcare costs, and inform clinical decision-making.

The upcoming image illustrates the proportion of BC utilization across various healthcare categories.

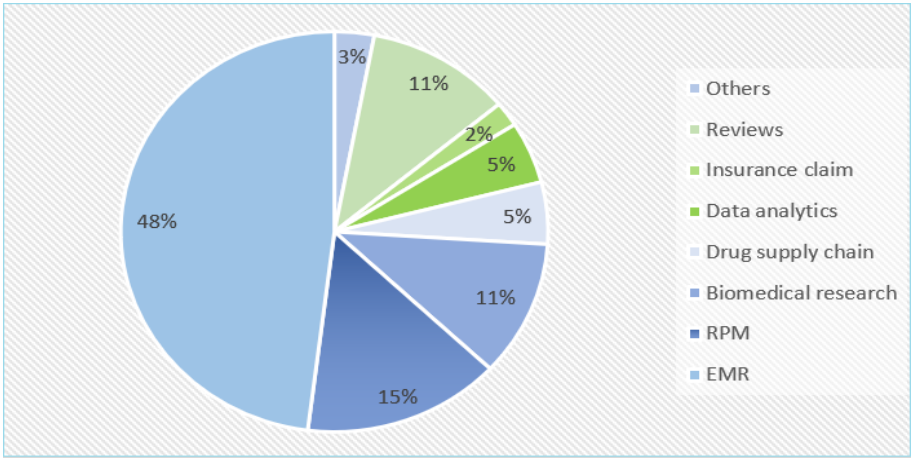

Figure 3.3: Percentage distribution of the use cases of BC [78].

3.3.2 Benefits of blockchain to healthcare applications

BC technology offers several benefits to healthcare applications, including:

- **Decentralization**: The healthcare industry involves various stakeholders and requires a decentralized management system. BC technology can serve as the backbone for managing health data in a decentralized manner, allowing all stakeholders to have controlled access to the same health records without any central authority controlling the global health data [78].
- **Improved data security and privacy**: The security of health data stored on a BC is greatly enhanced by its immutability feature. Once stored, the data cannot be manipulated, changed, or retrieved. Health data is encrypted, time-stamped, and chronologically ordered on the BC [78]. Additionally, the patient's identity and privacy are protected by the cryptographic keys used to store data on the BC.
- **Health data ownership**: To ensure patients have ownership and control over their health data and prevent misuse by other parties, it is important to use strong cryptographic protocols and clear smart contracts [78]. BC technology can address these concerns by providing patients with the necessary assurances and tools.
- **Availability/robustness**: Records on the BC are replicated across multiple nodes, so the system is robust and resistant to data loss, data corruption, and some data availability security attacks, ensuring the health of the BC stored [79].
- **Transparency and trust**: By providing an open and transparent system, BC establishes trust in distributed healthcare applications, thereby increasing acceptance of these applications among healthcare stakeholders [78, 79].
- **Data verifiability**: The integrity and validity of plain text records stored on the BC can be verified without access to those records. This feature is very useful in medical fields where verification of records is required [79].

3.4 Electronic Health Record

An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users. While an EHR does contain the medical and treatment histories of patients, an EHR system is built to go beyond standard clinical data collected in a provider's office and can be inclusive of a broader view of a patient's care. EHRs are a vital part of health IT and can[80]:

- Contain a patient's medical history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results.
- Allow access to evidence-based tools that providers can use to make decisions about a patient's care.
- Automate and streamline provider workflow.

One of the fundamental characteristics of an EHR is the ability of authorized clinicians to produce and manage health information in a digital format that can be shared with other providers across multiple healthcare organizations. EHRs incorporate data from all doctors engaged in a patient's care since they aim to share information with other healthcare providers and organizations, such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics.

3.5 Related work

3.5.1 A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain

The purpose of the work

This work addresses the potential of combining BC and IoT in healthcare monitoring, leveraging the security and transparency features of BC technology [81]. The proposed work utilized the BC-based IoT where the system detects abnormal movements such as falls with sensor values received from acceleration sensors and analyzes basic biosignals of an individual's blood pressure, heart rate, and body temperature after detecting abnormal movements. This work is a mobile app, implemented using a JAVA-based Android service environment, so that users, guardians, and experts can check the user's measured biometric information anytime and anywhere using a smartphone.

Methodology

In this study, they utilized four biometric signals for about 20,000 systolic blood pressure, diastolic blood pressure, heart rate, and body temperature datasets of each of the 50 individuals when an abnormal movement from the sensor unit was detected. In addition, each data was classified into four conditions good, abnormal, severe, and emergency, according to an expert's diagnosis. Since the biosignal data used in the experiment used irregular data, the error rate had to be measured. In this experiment, the error rate according to the size change of the sliding window was measured.

Implementation and the obtained results

The smart healthcare monitoring system has been implemented which consists of a sensor unit that can sense the user's condition, a control unit that can control it, and a monitoring system that can be checked on smartphones, Also they used an algorithm that detects abnormal movements such as falls with the sensor values received from the acceleration sensor and analyzes the biosignals after abnormal movements are detected to determine the user's current state according to the user's biological condition. The performance evaluation was assessed using biological signals, including 500 datasets of systolic blood pressure, diastolic blood pressure, heart rate, and body temperature from 50 individuals. The experiment results showed that the algorithm, utilized for analyzing these biosignals, exhibited an average error rate of 2 percent.

3.5.2 Discussion and critique

The previous study presents an innovative application of BC and IoT in healthcare monitoring. By leveraging blockchain's immutability and IoT's data collection capabilities, the proposed system offers potential benefits in enhancing data security and enabling personalized diagnosis. The integration of

multiple biosignals contributes to a comprehensive understanding of an individual's health status. However, several limitations should be addressed to strengthen the study. Expanding the scope of abnormal movement detection to include a broader range of health events or conditions would enhance the system's utility and relevance. Additionally, increasing the sample size to include a more diverse population would provide a more robust evaluation of the system's performance. Lastly, conducting a comparative analysis against existing healthcare monitoring approaches or technologies would help establish the unique advantages and effectiveness of the proposed BC-based solution.

3.6 Digital Twin fundamentals

3.6.1 Introduction of Digital Twin

Digital Twin stands for the representation of the anatomy of a digital asset in a digital space which is the depiction of physical phenomena from a physical space. It is a complex system that keeps the consistency between digital and physical space and can develop cognitive knowledge about the physical environment [82]. The most significant task of DT is the interaction between the physical and digital scenarios [83]. With the rapid growth of a new generation of information technologies like RFID and Internet of Things, data collection from each aspect of a physical phenomenon can be modulated conveniently.

3.6.2 A brief history of digital twin technology

The concept of digital twin originated in the early 2000s, when Dr. Michael Grieves, a researcher at the University of Michigan, introduced the idea of using a virtual representation of a physical product to optimize its design and performance in a 2003 presentation [84]. One of the early examples of digital twin application was NASA's Digital Twin program, which was launched in 2010 to create virtual models of spacecraft components and simulate their behavior in space [85].

3.6.3 Digital Twin components

The basic model of a digital twin for a product comprises three key elements: the physical entities present in the physical environment, the virtual models that represent these entities in the virtual environment, and the connected data that establish the link between the physical and virtual worlds.

- **The physical model:** It is made from materials and parts through processes such as machining and assembly. Entities have different characteristics, behaviors, and performances during manufacturing, use, maintenance, repair, overhaul, disposal, etc., and generate a lot of data.
- **The virtual model:** A virtual model is a mirror image and representation of a physical product in a virtual space. You can simulate, monitor, diagnose, predict, and control the state and behavior of the corresponding physical entities, reflecting the entire lifecycle process. The virtual model contains not only the geometry model but also all rules and behaviors such as material properties, mechanical analysis, health monitoring, etc.
- **The connected data:** Related Data includes subsets of physical and virtual data, and some "new data" collected after the integration, fusion, and analysis of physical and virtual data. During the design and production process, the virtual model parameters are passed to the production line to

process the virtual model into a real physical product. Digital recognition or measurement feeds product attributes, operating conditions, and other data back into the virtual model, enabling a two-way data transmission process.

3.6.4 Data life cycle management in Digital Twin Product Design

From a data science perspective, a digital twin can be viewed as a system that filters and integrates information. On the one hand, it filters large amounts of data to obtain relevant information that can be used for design operations. Meanwhile, it integrates different types of data to uncover hidden patterns and validate analytical results. The data life cycle includes multiple phases such as data ingestion, transmission, storage, integration, processing, cleansing, analysis, and mining. This life cycle transforms raw data into valuable information that designers can easily access for decision-making. The following steps relate to are illustrated as follow:

- **Data collection:** Data collection is the first step in the whole process. DTPD has physical product data Collected from both consumer and product sensors or extracted from online sources through interviews and downloads or reading the documentation [86].

- **Data integration:** This is a key step in the digital twin process as it enables the combination of data from various sources and formats, providing a unified view of the system being modeled. Digital twins require data integration to create a complete and accurate representation of physical systems within virtual environments [87]. The process of data integration involves identifying relevant data sources and formats, transforming the data into a consistent format, and combining it into a single unified view. This integrated view can be used for analysis, modeling, and simulation in the digital twin environment.

- **Data cleaning:** Data cleansing refers to the process of identifying, eliminating, and correcting various types of errors Included in the DTPD data set. Common data cleansing tasks include record matching, identifying inaccurate data, assessing overall quality, duplication, and column segmentation [88].

- **Data mining:** The goal of the data mining process in DTPD is to extract information from a data set and transform it into a visualization structure for further use [89]. Apart from raw analysis Step one covers database and data management aspects, data preprocessing, model and inference considerations, interesting metrics, complexity considerations, post-processing of discovered structures, visualization, and online updates.

3.6.5 Types of digital twins

Digital Twin can be divided into two types depending on for which purpose it will be used [90]:

1. **Digital Twin for Developing a Product:** This type represents a physical product that has not been developed yet, moreover, its representative DT already has all the information necessary to develop the physical product. In this respect, by using previous knowledge, the current state of the development, work distribution, product description, etc, DT can predict the workflow and the behavior of the product. For example, a DT can be implemented while in the manufacturing phase of a hospital [90].

2. **Digital Twin for an Individual Instance:** This type of DT has the awareness of a physical product or a non-spatial phenomenon and can constantly update the virtual state with the real-time data from the physical space through IoT devices [91].

3.6.6 The characteristics of digital Twin

Digital Twin is a contemporary era that has received a reputation in current years because of its capacity to bridge the bodily and digital worlds. It has been confirmed to be a powerful device for product design, manufacturing, and maintenance, presenting several blessings to industries that include aerospace, automotive, and healthcare. To apprehend its significance, it's miles essential to look at the following traits that make Digital Twin precise and valuable [92]:

- **Real-time reflection**: Different kinds of physical object data need to be integrated and continuously mapped to real-world objects in real time.

- **Interaction and convergence**: Are important aspects of DT technology. Interaction refers to the ability of the DT to communicate with the physical system and receive data in real time. This allows for the DT to update and adjust its virtual representation of the physical system based on new information.

- **Evolution and iteration**: Are key aspects of DT technology. As the physical system being modeled changes, the DT must also evolve to maintain an accurate representation of the system, this requires a continuous feedback loop between the physical system and the DT to collect and analyze data to update models and improve accuracy.

3.7 Healthcare Digital Twin

The demand for convenient and accurate medical services is growing rapidly. This will drive the development of medical technology toward connectivity, digitization, and intelligence, as shown in Figure 3.4. Advances in cloud computing, the Internet of Things (IoT), big data, and the mobile internet are shifting the healthcare model from current evidence-based medicine to precision medicine, which emphasizes personalized and targeted medicine [93]. The goal of precision medicine is to actively fight disease using technologies such as genetics, genomics, and intelligent health monitoring systems. Treat unavoidable illnesses with individualized methods rather than with a one-size-fits-all approach. Moreover, precision medicine based on data-driven intelligent health services requires different types of data, including patient data, medical data, service data, and fusion data.

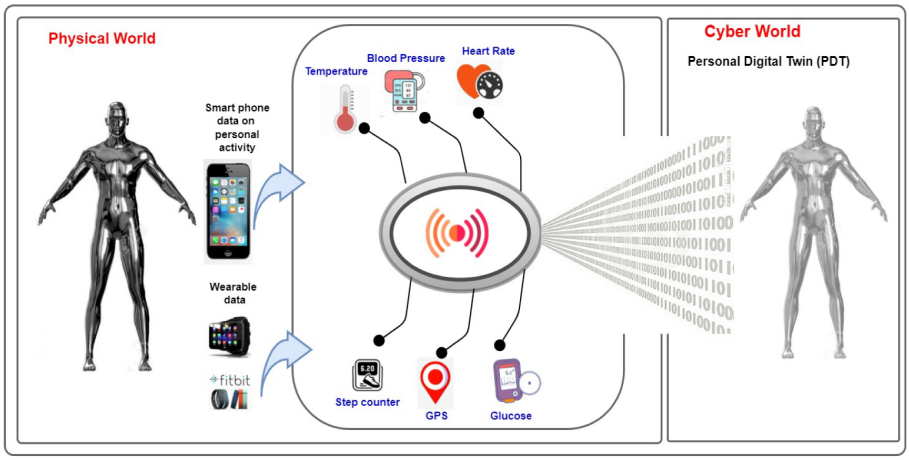

Figure 3.4: Communication in Healthcare System to Cater Disaster Situations [93].

As a result of these changes, the healthcare industry is moving towards a continuous and personalized service model, with an emphasis on intelligent systems and platforms that can provide data-driven smart healthcare.

3.7.1 Current Research of Applications in Intelligent Medical Systems

Currently, most researches and commercial applications mainly focus on the following aspects of intelligent medical systems:

- **Platforms**: Employs a tiered distributed architecture to simplify information sharing and management It will be available through a centralized platform and implements fast and flexible delivery through a decentralized platform [94].
- **Business model**: Changes in the medical business Model brought about by cloud computing such as Cloud Medical reduction service and cloud health image service Improved total construction costs and utilization means [94].
- **Standards**: To achieve this, we use a combination of international, national, and region-specific specifications for personalized innovation [94].

- **Interoperability in Health IoT**: To improve the interoperability of medical devices and enhance monitoring and alerting capabilities, IoT and mobile internet technologies are being utilized in the health IoT domain. However, despite significant advancements in intelligent medical services, there are still some persisting problems that need to be addressed. These include the following problems [95]:
  - The lack of real-time interactions between medical institutions and patients.
  - The absence of continuous personal health management services throughout the entire life cycle of the elderly.
  - Low accuracy of crisis warning services for elderly patients.
  - Incomplete fusion of medical physical systems with information systems.

3.7.2 Concept of Digital Twin Healthcare

The advancement of IoT and CPS technologies has facilitated the process of conducting precise simulations using multi-science and multi-physics models. By integrating physical models, sensor data, and historical information, it becomes feasible to achieve accurate simulations. In the healthcare domain, for example, real-time parameter data obtained from healthcare devices can be fed back into digital models through sensors. This enables quick verification of simulations and allows for prompt dynamic corrections. DTH is a revolutionary medical simulation approach that uses DT technology along with multi-science, multi-physics, and multi-scale models to deliver fast, accurate, and efficient medical services. DTH mainly consists of three parts [96]:

- The physical object may be a medical device or a wearable device for the patient, an external factors such as social behavior, weather influencing their health, or it is a system consisting of several or all of these unit objects.
- The virtual object could be the medical device model, wearable device model, digital patient model, external factor model, and digital system model.
- The healthcare data encompasses a wide range of information, including detection data derived from external systems or medical devices, real-time monitoring data obtained from wearable devices, simulation data generated from digital models, historical data and patient records sourced from medical institutions, as well as service data originating from platforms or systems that bridge the gap between the physical and virtual realms.

There are four primary stages in the DTH operation mechanism.

- First, accurate DT models should be established corresponding to the physical entity objects using advanced modeling techniques .
- Second, data connection, ensure real-time interaction between physical and virtual objects, it is essential to establish data connectivity using health IoT and mobile internet technologies. This enables seamless communication and synchronization between the physical environment and the virtual world.
- Third, The accuracy of the simulation is verified through rapid execution and calibration processes to ensure the correctness of the model.

- Fourth, Based on the requirements and current circumstances, continuous model evolution should be undertaken to optimize and iterate the DT models. Subsequently, data from the DT models are utilized to enhance the performance of physical objects and service systems, thereby offering improved healthcare solutions.

The application of DTH in the healthcare industry can be categorized into two main areas: hospital management and design, and patient healthcare. By utilizing DTH approach, a range of potential solutions can be evaluated within virtual environments prior to the execution of real-world interventions. This includes conducting simulations of surgical procedures and virtual drug experiments. For example, a DT of a human body can allow doctors to discover ailments before they are apparent, experiment with treatments and prepare better for surgeries. In the absence of DTH, hospital staff can only rely on their domain knowledge and basic analysis to plan new facilities and new treatments, and wait to see their effects. With a DTH, problems can be predicted before they occur in patients to reduce risks and save costs [96].

3.8 Related Work

3.8.1 Digital twins to personalize medicine

The purpose of the work

The purpose of this work is to integrate digital twin technology as a solution to address the problem of patients who do not respond to drug treatment. This issue leads to patient suffering and increased healthcare costs. The researchers propose a study that involves creating multiple digital replicas or twins of the patient, each based on computational network models incorporating thousands of disease-relevant variables. These digital twins are then subjected to computational treatment using various drugs, aiming to find the most suitable medication [97].

Methodology

This study follows a specific methodology to explore the concept of digital twins in healthcare. Figure 3.5 illustrates the methodology employed. An individual patient is denoted as a in the figure, has a local sign of disease (red). Where b is a digital twin of this patient constructed in unlimited copies, based on computational network models of thousands of disease-relevant variables. Each twin is computationally treated with one or more of the thousands of drugs . Based on the results of the computational treatment, we identify the drug that exhibits the most favorable effect on the digital twin. This drug, indicated in the figure as d, is then selected for the actual treatment of the patient.

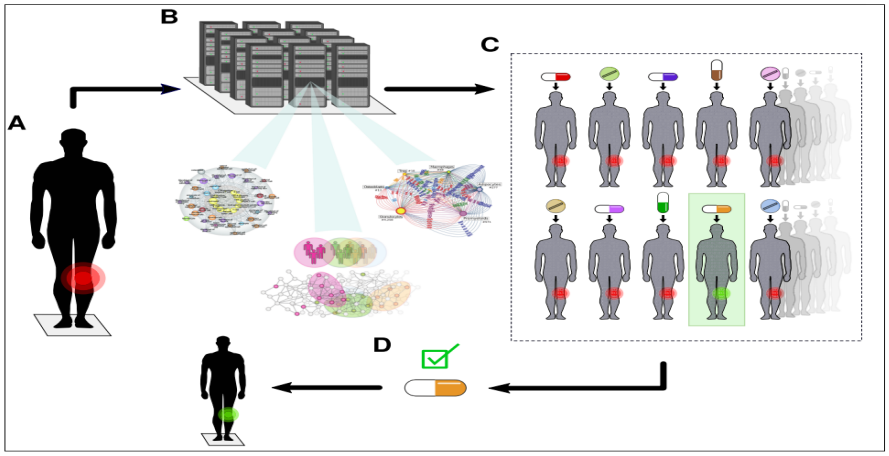

Figure 3.5: The digital twin concept for personalized medicine [97].

Implementation and Results

The implementation of digital twins in clinical settings poses various challenges that need to be addressed. These challenges encompass technical, medical, ethical and theoretical aspects.

However, the successful integration of digital twins has the potential to greatly enhance healthcare and deepen understanding of disease mechanisms. Additionally, it may open up new avenues for research. The development and implementation of digital twins could also inspire advancements in technology, potentially reducing costs and difficulties.

3.8.2 Blockchain-Based Digital Twins Collaboration for Smart Pandemic Alerting: Decentralized COVID-19 Pandemic Alerting Use Case

The purpose of the work

The purpose of the study is to explore the potential of using BC-based DT in collaboration with smart pandemic alerting systems. The passage discusses the significance of Healthcare 4.0 in revolutionizing healthcare through a data-driven learning healthcare system. It emphasizes the role of technologies like IMoT, digital twins and big data in this transformation. The integration of digital twins with BC technology is proposed as a viable approach to establishing secure and interconnected MCPS [98].

Implementation and Results

The main goal of this research is to create a framework for setting up decentralized COVID-19 pandemic alerts using collaborative digital twins based on BC technology. This framework aims to develop intelligent distributed systems that use the shared data intelligence of digital twins to predict potential risks.The physical world represents people involved in the healthcare system, such as patients, doctors, and nurses. In the cyber world, advanced technologies such as BC, digital twins, AI, big data, edge computing, and cloud computing work together to provide valuable information to decision-makers. MCPS decision-makers include hospitals, healthcare organizations and governments.

3.8.3 Design of Mobile Healthcare Monitoring System Using IoT Technology and Cloud Computing

The purpose of the work

The purpose of this work is to explore the potential of Internet of Things (IoT) technology in enabling remote control and monitoring of physical events through the connection of distant objects. IoT facilitates seamless communication between humans, smart devices, and interconnected devices without the need for direct human interaction. IoT applications extend to smart wearables, smart cities, home automation, healthcare systems, and more. In healthcare, IoT has revolutionized traditional patient monitoring by enabling remote verification of health parameters [99].

Implementation and Results

Four people were tested in this project. The first is a young healthy man, the second is a young woman, the third is an older man, and the fourth is an older woman. The heart rate of each of these people. In this project, we compare her three other methods to compare the accuracy of the heart rate sensor:

- The first method is to put the index and middle finger on the underside of the opposite wrist under the base of the thumb and check the beats for example in 15 seconds and multiply the beats by 4 so the heart BPM can be calculated. This method is manual measurement.
- The second method is to use a pulse oximeter fingertip device and record the shown heart rate.
- The third one is to use a digital blood pressure device with heart rate measurement.

This article presents an experimental model of a remote biosignal monitoring system based on IoT technology. The system is portable, and has low power consumption. The biosignals obtained from this system have been validated and compared to measurements from medical devices used by doctors and healthcare providers to ensure their accuracy. The system successfully uploads biosignals to a mobile application, enabling medical professionals to monitor and diagnose multiple health parameters simultaneously. The mobile application also allows you to manage multiple cases simultaneously. Moreover, this project is cheap and easy to buy.

3.8.4 Discussion and critique

1. The first proposed work should provide a detailed explanation of the security measures implemented to protect the digital twins and the sensitive patient data involved. As the digital twins are representations of real patients, it is essential to ensure the confidentiality, integrity of the data throughout the process. Safe guarding patient privacy and complying with relevant data protection regulations should be a priority. Additionally, the work should address the potential vulnerabilities and risks associated with the computational network models and the digital twin system itself. Any weaknesses or vulnerabilities in the models or the system could be exploited by malicious actors, leading to unauthorized access to patient data. Integrating BC technology into the proposed work for personalized medication can enhance security and data integrity factors .

2. In the second project, they established a framework that uses BC technology to create a digital twin for healthcare system. The framework emphasizes the importance of secure data exchange and real-time updates. Moreover, this work introduces valuable concepts and highlights the potential benefits of BC, the framework's security and real-time capabilities require further investigation and clarification as:

    - By outlining measures to address potential vulnerabilities and protect sensitive health data, the project will gain credibility.
    - The undertaking states that the database within side the ledger will allow real-time updates among virtual twins. It is crucial to make clear how those updates are accomplished and if any delays or synchronization problems might affect real-time functionality. Providing facts approximately the underlying infrastructure or protocols used to assist real-time updates will help assess the feasibility and performance of the proposed system.
    - Given the sensitivity of medical data, protecting privacy is paramount.
    - In practice, it is important to ensure that the system can handle increased workloads and maintain real-time capabilities as the network grows.

3. The third project aims to design a mobile health monitoring system that utilizes IoT technology and cloud computing. However, there are several obstacles that need to be addressed in order to successfully implement the system. These challenges include:

    - This work doesn't include fog computing to improve real-time monitoring and immediate information acquisition for therapeutic purposes.
    - BC technology is not used to ensure data security and protect against malicious use.
    - This project overlooks the use of digital twins to predict disease and identify problems in virtual environments.

3.9 Conclusion

Blockchain has demonstrated its potential to transform traditional industries with its key characteristics, including decentralization, persistence, and anonymity. In this chapter, we aim to provide a comprehensive overview of blockchain technology. We start by introducing the fundamentals of blockchain, including its structure and consensus mechanisms. We then delve into the concept of digital twins, an emerging advanced technology that is making significant strides in various fields. We explore the role of digital twins and their applications in healthcare monitoring. Additionally, we have reviewed previous works that have focused on healthcare solutions leveraging BC and DT technologies. This review has provided valuable insights that will guide our implementation in the upcoming chapter, allowing us to improve upon existing approaches and contribute to the field of healthcare monitoring.

Chapter 4

Implementing a Blockchain-based System for Patients' Digital Twin

4.1 Introduction

In this chapter, we embark on a journey to revolutionize the healthcare industry by harnessing the power of BC technology and DT patient simulation. Our primary objective is to develop a cutting-edge healthcare system that can accurately predict heart rate, and identify critical patient conditions. By integrating various scenarios and input parameters, our solution aims to provide doctors with invaluable insights for timely interventions and improved patient care. First, we will explore the process of building a web interface using BC and DT technologies for healthcare applications. Therefore, we need to create a Healthcare contract and deploy it on the blockchain network. Throughout this chapter, we will dive into the tools and technologies that we will be using to accomplish this task and we will also reflect on the challenges encountered during the development process.

4.2 Building a Blockchain-Based Digital Twin System for Patient Monitoring

Our main focus will be on creating a healthcare contract and deploying it onto the BC network. This contract will serve as the foundation for securely storing patient medical records on the simulator of BC. Furthermore, we will develop a dedicated web interface HealthLink tailored specifically for doctors. This interface will enable doctors to seamlessly interact with the BC and leverage the digital twin patient simulation feature. By utilizing the digital twin simulation, doctors will be able to predict the heart rate and blood pressure of patients based on various scenarios and input parameters.

4.2.1 Set up Development Environment

Set up the appropriate development environment for blockchain development, which includes installing the essential software, frameworks, and tools such as Truffle, Ganache, and Web3.js, that provide the necessary tools to start developing blockchain applications. Truffle provides a project structure and development workflow and it is used to compile and deploy the smart contracts, Ganache offers a local blockchain environment for testing, and Web3.js enables interaction with the Ethereum network.

4.2.2 Dependencies

In order to build our BC based system for patient body digital twins, we need a few dependencies to come along, the list below shows some of the essential dependencies required for building the project.

Node Package Manager(npm)

The first dependency we need to use is Node Package Manager, or npm, which is a package manager for JavaScript and is commonly used for managing dependencies in Node.js projects.

Solidity Compiler

We need the Solidity compiler to compile our smart contracts written in the Solidity programming language. The most common Solidity compiler is the Solidity Compiler (solc).

Ethereum Development Kit (Truffle)

Truffle is a development framework that provides a suite of tools for building, testing, and deploying smart contracts. It simplifies the development process by providing utilities for contract compilation, migration, testing, and network management.

Ganache

Ganache is a personal blockchain for Ethereum development. It allows us to create a local development blockchain network, which is useful for testing and simulating interactions with smart contracts. Ganache provides a set of accounts with pre-funded Ether for testing purposes.

Metamask

Metamask is a browser extension that acts as a digital wallet and allows users to interact with Ethereum-based applications. It provides a secure way to manage accounts and sign transactions. Metamask will be used by doctors to connect their wallets and interact with the blockchain-based healthcare system.

Web3

Web3 is a JavaScript library that allows interaction with Ethereum and smart contracts. It provides a set of APIs to connect to an Ethereum node, send transactions, and interact with smart contracts.

React

React is a JavaScript library for building user interfaces. We will be using React to develop the web interface for doctors to interact with the healthcare system.

Remix Ethereum

Is a powerful web-based integrated development environment (IDE) specifically designed for Ethereum smart contract development. we have used it to get the ABI of our smart contract.

4.3 Implementation

4.3.1 Health care smart contract

The goal of our project is to enable doctors to monitor the heart rate of each patient and determine if it is normal or not. Additionally, we aim to predict the effect of medication on the patient's heart rate to help ensure their well-being. To achieve this, we have developed a smart contract named "HealthCare.sol". The Health Care smart contract is specifically designed to execute predefined functions and operate within the constraints of the BC platform. The following functions have been implemented:

- **AddPatient**: This function allows for the addition of a new patient to the system.
- **CreateHealthRecord**: With this function, a new health record can be created for a specific patient.
- **GetPatientHealth Records**: This function enables the retrieval of a patient's health records.
- **GetHeartRate and UpdateHeart Rate**: The function enables the retrieval of a patient's heart rate, while the update Heart Rate function is responsible for altering the heart rate of a patient.
- **isHeartRateNormal**: Function is designed to inform the doctor whether a patient's heart rate is within the normal range or not.

By implementing these functions in the Health Care smart contract, we can establish a direct and secure connection between patients and their doctors without the need for intermediaries. This ensures efficient and reliable healthcare monitoring while maintaining patient confidentiality and trust in the process.

4.3.2 User management smart contract

In our project, access to patient information such as diagnosis, heart rate, medication, etc., is limited to authorized doctors. To achieve this, we have developed a smart contract named "UserManagement.sol" that allows doctors to securely access patient data using their email and password credentials. By implementing a private permissioned system, we ensure enhanced security and privacy measures for the data involved. Here's an explanation of the functions in the contract:

- **isValidLogin**: This function takes an email address and password as parameters and checks if the provided credentials match the stored user credentials. Compares a stored hash of a user's email and password with the provided values and returns a Boolean value indicating the validity of the login.
- **registerUserThis**: Feature allows users to register by entering a username, email address, and password. Set the provided user details to the user's mapping of the user's address and emit a registration event with the user's address.
- **login**: This function is called when a user wants to log in. It sets the loggedIn status of the user's address to true and emits a Login event with the user's address.
- **logout**: This function is called when a user wants to log out. It sets the loggedIn status of the user's address to false and emits a Logout event with the user's address.

- **isUserLoggedIn**: This function takes a user's address as input and returns a boolean indicating if the user is currently logged in.

4.3.3 The deploy of smart contracts

To test and connect Ganache with smart contracts, we need to deploy the contracts. To do this, we create two files: "migration.js" for the contracts . When we run the command "truffle migrate", both contracts will be deployed in Ganache. Result of Truffle Migrate Command in Ganache illustrated in the following image:

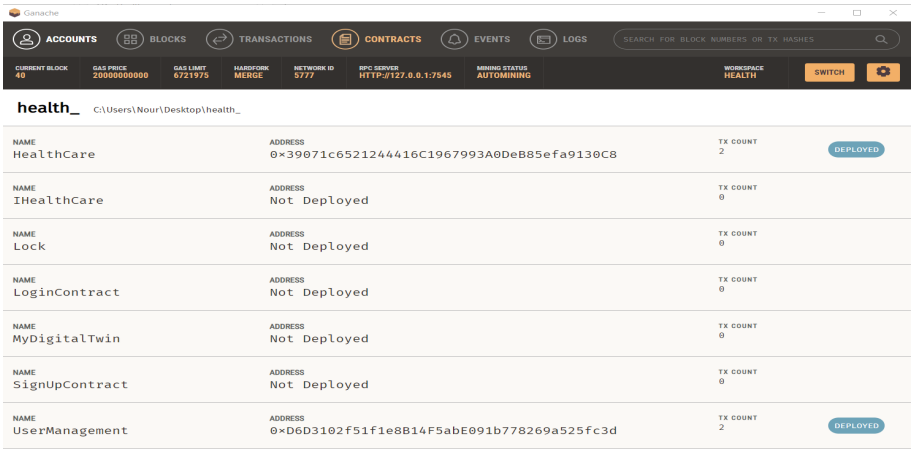

Figure 4.1: Deployment in ganache.

4.3.4 Test of contracts

To validate the behavior and intended functionality of a smart contract, we have developed a JavaScript file. Its purpose is to ensure that the contract operates as intended and to verify its expected behavior. This file contains a comprehensive set of test cases that encompass various scenarios and functionalities of the smart contract. These tests are performed using a testing framework, such as Truffle's built-in testing framework. To obtain the test results, we execute the following commands:

- Run the command "truffle console –network development" to access the Truffle console, which connects us to the development network for testing purposes.
- Within the Truffle console, execute the command "truffle test" This command initiates the execution of the tests defined in the JavaScript file and provides us with the test results.

4.4 Diagrams and users interface

4.4.1 Diagrams

To illustrate the functionalities of our proposed system we show in the section the main three UML diagrams namely Use Case, Sequence, and Class diagrams.

Use Case Diagram

The Use Case Diagram presents the different use cases or functionalities provided by the website. It highlights the actors and their interactions with the system, including actions such as authentication, accessing patient health records, monitoring heart rate, and checking medication effect on heart rate.

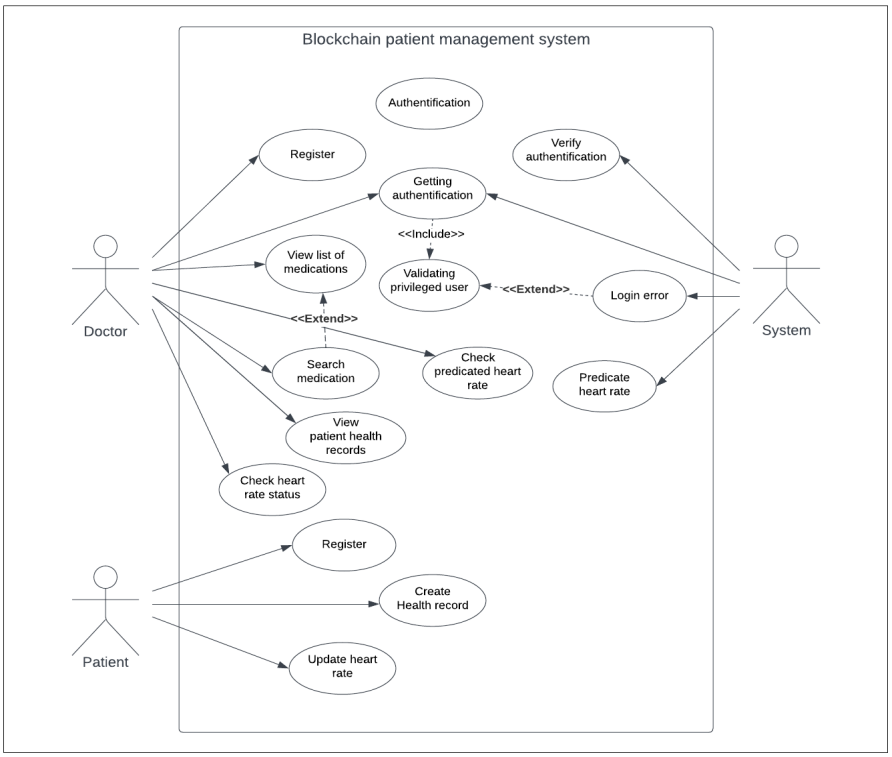

Figure 4.2: Use Case Diagram.

Sequence Diagram

The Sequence Diagram illustrates the interactions between the doctor and the system for specific use cases. It showcases the flow of messages and actions, highlighting how the doctor's requests and inputs are processed by the system to retrieve patient information.

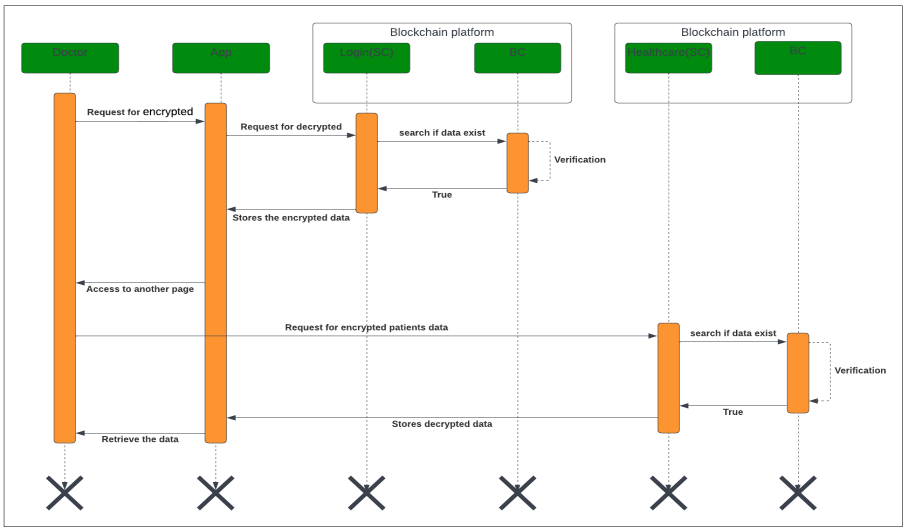

Figure 4.3: Sequence diagram with the smart contract procedures.

Class Diagram

The Class Diagram illustrates the various classes and their relationships within the system. It showcases the entities involved, such as Doctor, Patient, Authentication, HealthRecord. The relationships between these classes depict how data flows and interactions occur within the system.

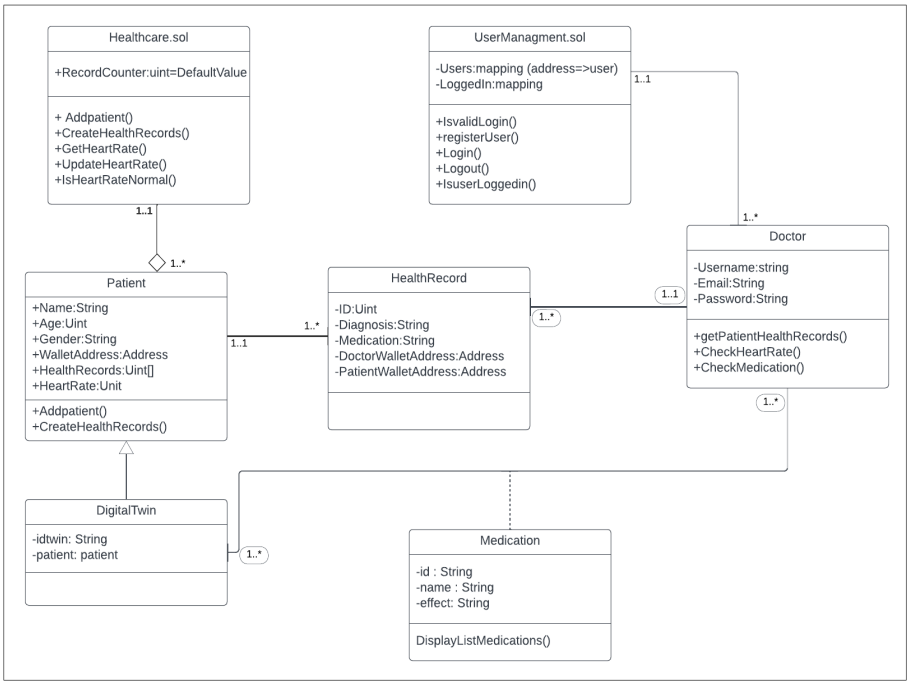

Figure 4.4: Class Diagram.

4.4.2 HealthLink interface

Our web-based interface, called HealthLink, serves as the main platform for doctors to access and interact with the system's features and functionalities. It provides a secure interface for efficient healthcare management. The interface includes the following key components:

- **Authentication Page:** Upon accessing the web interface, doctors are required to authenticate themselves by entering their credentials (email and password) Figure 4.5 shows that. Additionally, doctors need to connect to their account in the MetaMask wallet to establish a secure connection between the website and the Ganache platform. If doctors don't have an account, they can register by creating a new MetaMask account and providing the required credentials Figure 4.6. This ensures secure access to patient data and system functionalities.

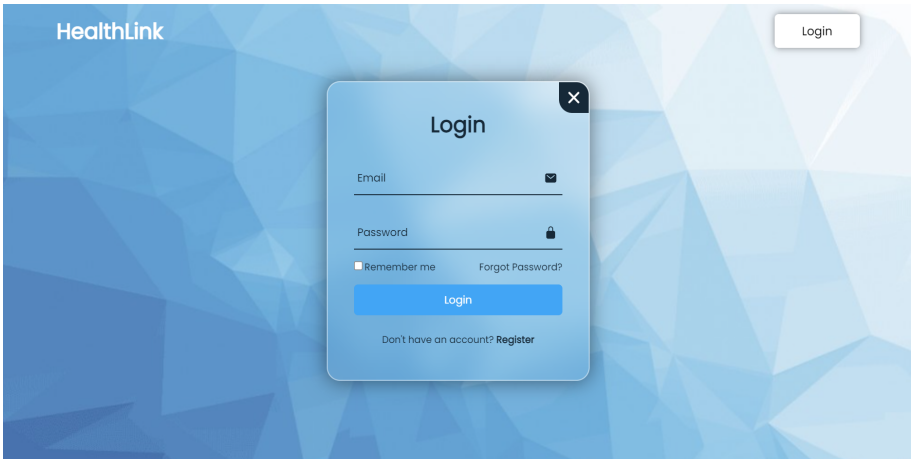

Figure 4.5: Login page.

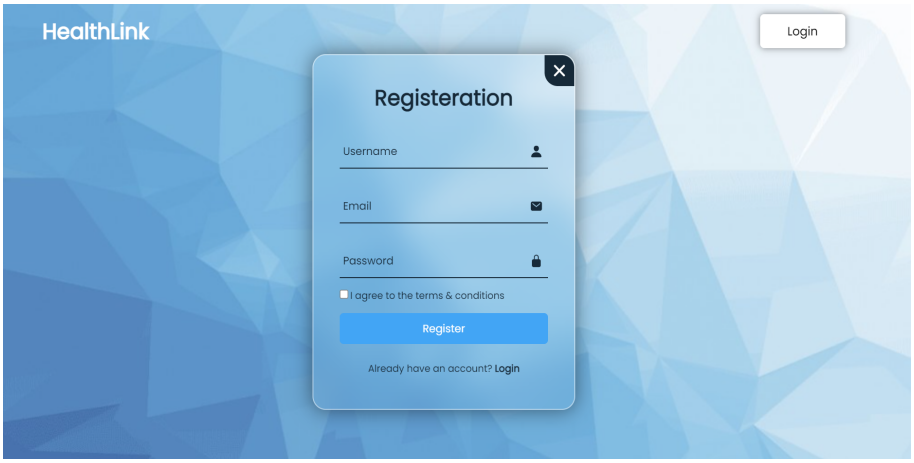

Figure 4.6: Registration page.

- **Home Page:** The home page serves as the primary landing page for doctors when they access and authenticate to the HealthLink website. It presents an intuitive and visually appealing interface that allows doctors to navigate through the system's functionalities.

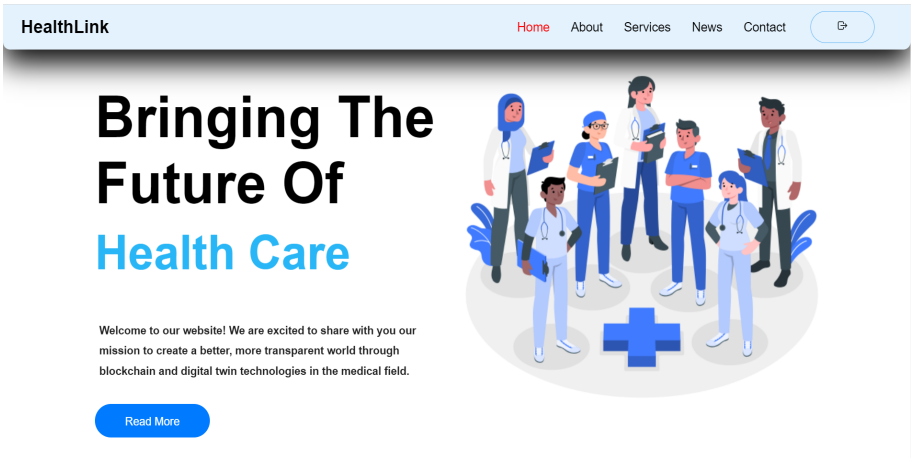

Figure 4.7: Home page.

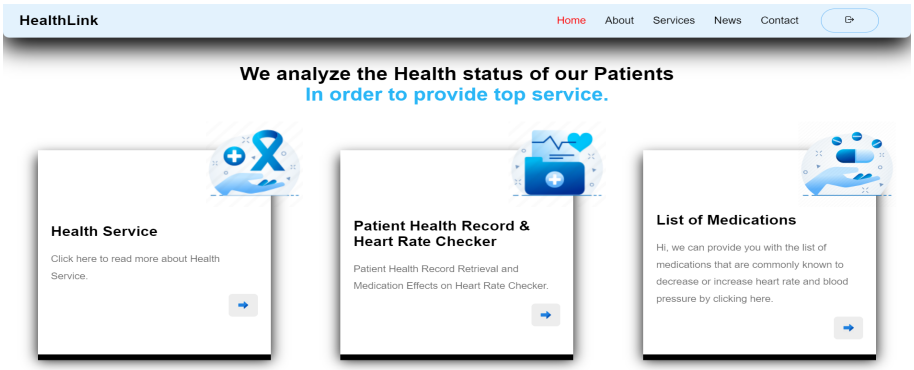

Figure 4.8: Home page.

- **Patient Health Record and medication checker:** On this page, we combined the fundamental services of our website, and it appears as follows:
  - **Patient Health Record:** Once authenticated, doctors can search and access the health records of patients by entering the patient's wallet address after importing the address from blockchain. The system grants the doctor permission to view the patient's medical data that are stored in the BC.
  - **Check Heart Rate:** The website allows doctors to monitor the real-time heart rate of patients. By entering the patient's wallet address and initiating the heart rate monitoring feature, doctors can view the patient's current heart rate status and assess whether it falls within the normal range or not. The figures below show that.

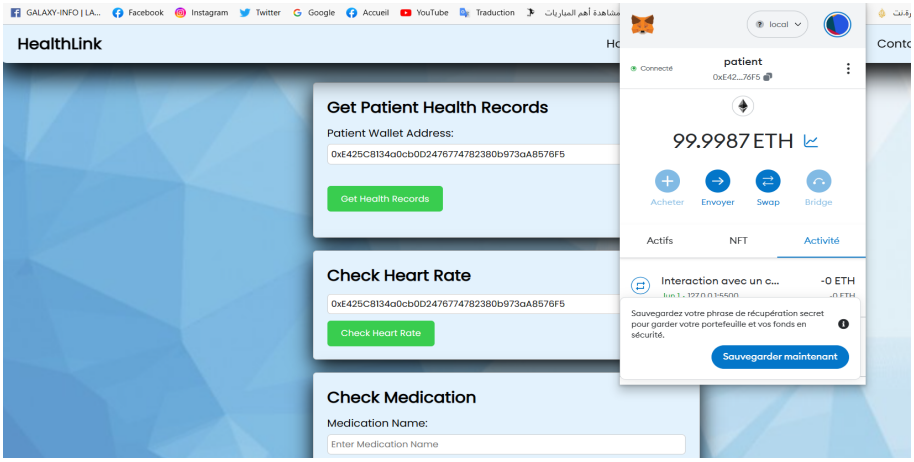

Figure 4.9: Patient Health Record Retrieval and Heart Rate Monitoring.

The following figure displays the result obtained by clicking the ”Get Health Record” button. The system executes the function getPatientHealthRecords() to retrieve the stored patient health record from the Ganache network. Each patient may have one or multiple health records associated with the treatments they have received.

Figure 4.10: Patient health records.

The figure 4.11 illustrates the result obtained by clicking the ”Check Heart Rate” button. Based on the stored or captured patient’s heart rate data, the system will indicate whether the heart rate is within the normal range or not.

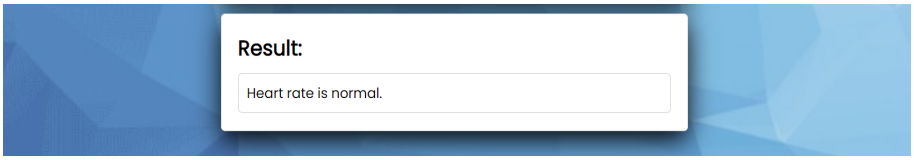

Figure 4.11: Patient heart rate status.

– **Check medication:** Another key functionality of the HealthLink website is the ability for doctors to enter the medication name and receive predictions of the patient's heart rate response. This feature provides valuable insights into how the medication may affect the patient's heart rate.

When doctors enter the medication name into the system, advanced algorithms and the captured patient data are utilized to analyze the potential impact of the medication on the patient's heart rate. The system takes into account factors such as the patient's current heart rate, and known effects of the medication on heart rate. In our case, we do not have a physical implementation of a sensor for monitoring heart rate. Instead, we will manually enter the heart rate data, which we believe has already been captured and stored in the system.

Once the manual entry is completed, the system will utilize the entered heart rate information for further analysis or display. The web interface generates predictions based on these inputs, allowing doctors to assess whether the medication is likely to cause an increase or decrease in the patient's heart rate. If the predicted heart rate is outside the normal range, the system will display an alert, notifying the doctor of potential concerns or adverse effects. This functionality provides doctors with valuable information when considering medication options for their patients. By leveraging advanced algorithms and patient data, the system empowers doctors to test medication on patient Digital Twin and make informed decisions and ensures patient safety by proactively identifying potential heart rate-related risks associated with specific medications.

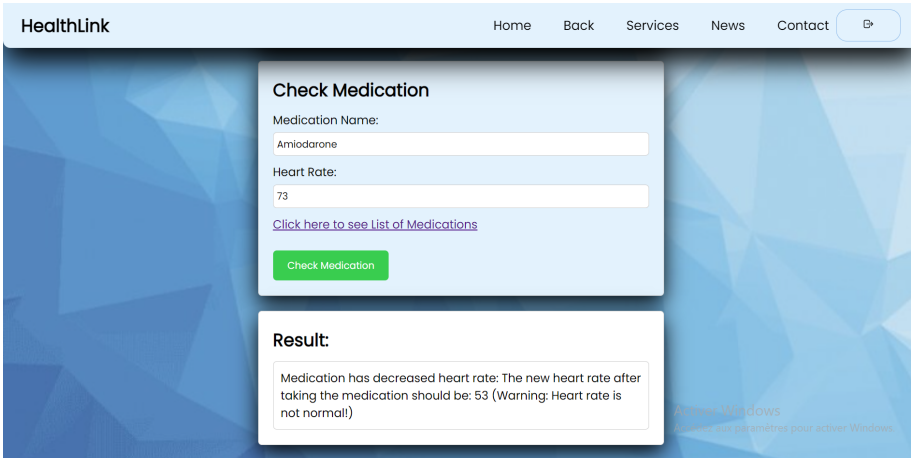

Figure 4.12: Heart rate prediction.

The figure above illustrates the result obtained after entering a medication. The system will display information about the medication, including whether it decreases or increases heart rate, and the effect of the drug on heart rate value. The system will update the heart rate accordingly. If there are any potentially dangerous cases, it will show up a warning message. These functionalities are implemented using algorithms we integrated into the system.

We have added another page that displays a medication list, helping doctors in selecting the appropriate drugs based on the patient's diagnosis. This feature assists doctors in prescribing the right medication for the specific medical condition.

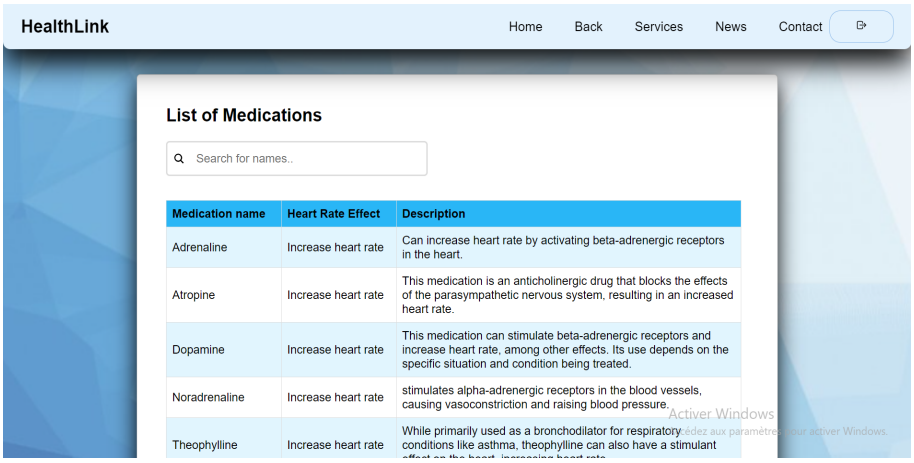

Figure 4.13: List of medications.

The lack of physical implementation such as sensors for capturing and collecting patient medical data and securely storing them in the BC simulator, we have developed a dedicated web page that allows adding patient data and creating health records. Additionally, we have included an updated data feature to accommodate real-time monitoring by the sensors, which continuously capture the patient's heart rate and automatically update it based on changes in the patient's medical or physical status.

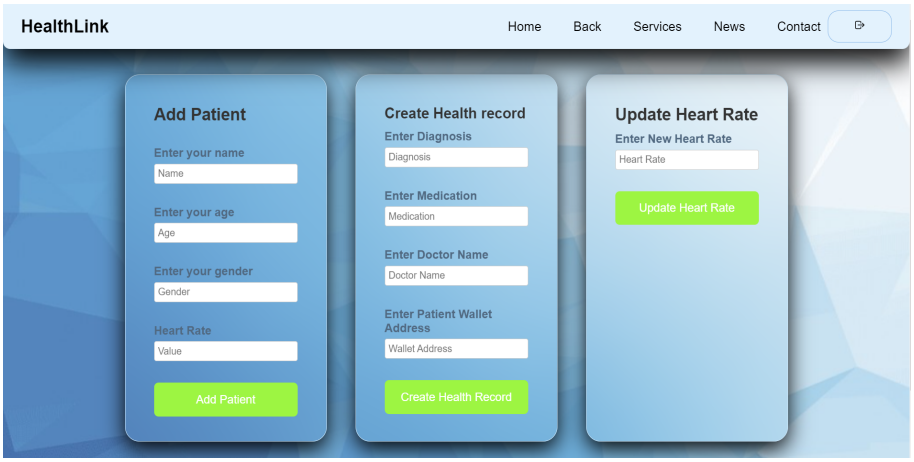

Figure 4.14: Patient page.

4.5 Research challenges

- **lack of resources:** We encountered a difficulty in our project while establishing a connection between our application and the smart contract, and also in finding the right resources for assistance and guidance. It can be difficult to locate comprehensive and up-to-date documentation that specifically addresses app-to-smart-contract integration.

  Moreover, understanding the intricacies of interacting with smart contracts requires a certain level of knowledge and expertise in BC development. Students like us may struggle to find an expert with the necessary skills to help us navigate the process.

- **Absence of a physical implementation:** One of the significant challenges we faced is the absence of a physical implementation for capturing patient heart rate. The unavailability of a dedicated sensor or device to directly measure heart rate poses a limitation in obtaining real-time and accurate heart rate data. This absence hinders the ability to monitor and track changes in heart rate, which are crucial for assessing patient health and identifying potential abnormalities.

- **Integration and Connectivity Issue**: We encountered a challenge in establishing a connection between our web interface and a Metamask account. Metamask serves as a digital wallet and a bridge between web applications and the Ethereum BC. One of the main issues we faced was ensuring communication and synchronization between the web interface and the Metamask account. This involved handling authentication, securely transmitting data between the interface and the account, and managing user permissions and access. Additionally, we had to address compatibility issues and ensure that the web interface functions smoothly across different browsers and versions of Metamask. Overcoming this challenge required thorough testing, troubleshooting.

- **troubleshooting:** The challenge of troubleshooting involves identifying and resolving issues within a system or application. It requires systematic investigation, analysis of symptoms. Troubleshooting can be complex, especially in intricate systems, and limited information or time constraints can further complicate the process.

- **Scalability**: The biggest challenge in healthcare is the lack of scalability associated with storing health monitoring data on the BC. In health monitoring, the continuous monitoring of vital signs such as heart rate generates large amounts of dynamic data that must be stored and registered on the BC. Storing all this data on the BC can quickly become resource intensive and costly, as the size of the BC grows, so do the storage and bandwidth requirements of each node in the network, which can lead to scalability issues.

- **The duration required to include a transaction in a block**: Including a transaction in a block can be time-consuming as it requires choosing the right consensus algorithm and performing the calculations necessary to validate the transaction. Well-known consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) require large amounts of computing resources and active stakeholder participation. The process may take longer if the number of participants increases.

- **Connect to ethereum**: Establishing a stable and reliable connection to the Ethereum network can be a hurdle. Since the network is decentralized, it relies on a network of nodes spread all

over the world. Problems such as network congestion, latency, or unreliable internet connection can affect your connection to the Ethereum network.

- **Node Synchronization**: When connecting to Ethereum, all BC history must be downloaded and verified to synchronize with the BC network. This process, called node synchronization, can be time-consuming and resource intensive, especially for new nodes or slow network connections.
- **Gas Fees**: Ethereum uses a gas mechanism where users pay for computing resources and storage space on the network. Gas prices fluctuate according to network demand and can be prohibitively expensive, especially during peak times. This can affect the usability and accessibility of Ethereum in certain use cases. When using smart contracts, gas fees are often required to perform operations on the BC. High gas prices can limit the ease and affordability of interacting with smart contracts, especially for applications with frequent or complex interactions.
- **Development and Integration Complexity**: Building and integrating applications on the Ethereum network can be complex and requires knowledge of the Ethereum smart contract programming language (Solidity) and related tools.
- **Complexity of Smart Contract Development**: Developing smart contracts requires expertise in a BC programming language like Solidity for Ethereum. To develop smart contracts, it is important to understand the intricacies of each BC platform, manage state transitions, and implement secure coding techniques. The complexity of smart contract development can be daunting.
- **Limited Programmability**: Smart contracts have limited programming capabilities compared to traditional software applications. They are designed to perform predefined functions and operate within the constraints of the BC platform. This limited programmability can make it difficult to implement complex business logic or modify smart contracts after deployment.
- **Security Vulnerabilities**: Smart contracts are immutable once deployed on a BC. This means that bugs and vulnerabilities in your code cannot be easily fixed. This poses a significant security risk, as mistakes in smart contracts can have irreversible economic or operational consequences. Ensuring the security and auditing of smart contracts is essential, but it can be a complex task.
- **Limited tools**: As students, we faced a challenge when it came to accessing a digital environment, specifically Azure Microsoft. Although Azure offers a comprehensive suite of services for building, deploying, and managing applications and services, it primarily operates on a paid model. This posed a limitation for us. While Azure provides a robust infrastructure and platform with various benefits for creating digital twins.
- **Integration Complexity**: Integrating a smart contract into a React application involves interacting with the BC network, deploying the contract, and calling contract methods. This process can be complicated and may require the use of additional libraries such as web3.js and ethers.js to interact with the BC through React application.
- **Test**: To ensure the correctness and reliability of smart contracts, it is important to create comprehensive tests for smart contracts. Testing React components that interact with smart contracts adds further complexity as it involves mimicking or simulating a BC environment and handling asynchronous operations in test cases.

4.6 Advantages and disadvantages of the conceived system

Advantages:

- New Implementation in the Field: Implementing a new technology or approach in a medical field brings innovation and the potential for improved new experiences.
- No Installation Required: The advantage of not requiring any installation is that it eliminates the need for users to go through complex installation processes.
- Use of Modern Web Development Tools: Leveraging modern web development tools offer several advantages.
- Easy Deployment and Upgrades: Implementing a web-based solution allows for easier deployment and upgrades compared to traditional software.

Limitations:

- Limited Network Scope: A blockchain simulation network is isolated to a local machine or network environment This limits the ability to perform transactions on a public blockchain network.
- Lack of Real-world Conditions.
- Security Risks: There are some required security measures. For example, ensuring that only authorized individuals have access to the network, securing private keys, and implementing appropriate security practices to protect against potential vulnerabilities.

Chapter 5

General Conclusion and Future Directions

In this thesis, we have presented a comprehensive study on Internet of Thing-based healthcare monitoring systems. We begin by providing a brief survey on the Internet of Things technology, then We delve into the IoT for healthcare by presenting the essential dots for exploring the potential of IoT in the medical industry. Furthermore, we discussed the significance of cluster computing and the Cloud-Edge-Fog (CEF) paradigm in revolutionizing healthcare services. Besides, we investigate the fundamental aspects of Blockchain and digital twin technologies and highlight their main features. By integrating BC and DT, we propose a new approach to mitigate system inefficiencies and advance the medical field. This integration allows secure and transparent data sharing, improved patient monitoring, and real-time alerts. The combination of these two technologies has the potential to revolutionize healthcare by enabling more personalized and proactive care.

The study we made focused on a Blockchain-Based System for patient Digital Twin. Our primary objective revolved around creating a healthcare contract and deploying it onto the BC network. This contract serves as the foundation for securely storing patient medical records on the BC simulator. To facilitate seamless interaction with the BC, we developed a dedicated web interface called HealthLink, tailored specifically for doctors. By validating transactions with a certain fee (gas), doctors can connect to the BC through the HealthLink website.

In addition, we integrated predictive algorithms into our system, which greatly assisted us in our endeavors. Through the HealthLink interface, doctors can effortlessly engage with the BC and harness the DT patient simulation feature. This functionality enables doctors to test the effects of medications on patient DT. Leveraging the DT simulation, doctors can predict patient heart rate and blood pressure based on various scenarios and input parameters. our work in developing this project has been a little difficult due to the utilization of new technologies and tools, but we continue until we reached a significant part of our project. In the future, our plan is to enhance the accessibility, exchange, and development of the system for commercial purposes. To achieve this, we aim to establish an official website that will serve as a platform utilizing an external blockchain network. This work will help doctors to have the ability to prescribe the most suitable medication for patients based on their health records, ensuring accurate and personalized treatment. Furthermore, the platform will have the potential to incorporate the prediction of various other diagnoses, such as diabetes and hypertension,

and more. By offering a comprehensive range of functionalities, the system aims to serve as an all-in-one solution. This integrated approach will assist doctors in their decision-making processes and provide valuable support to patients. Additionally, we plan to integrate a patient interface that allows individuals to test their medication at home without the need for frequent visits to the doctor. This home-based testing capability will enhance the convenience and encourage active patient participation in managing their healthcare.

Finally, a Blockchain-Based System for patient Digital Twin has been invented to secure patient medical data, Perhaps in the future, all medical transactions will be based on decentralized systems, because it is strong with a high level of trust. Additionally, the system may incorporate physical implementations such as the use of body sensors for capturing patient heart rate. By incorporating such technologies, the data collection process becomes more reliable and trustworthy, further enhancing the overall system functionality.

References

[1] R Alekya, Neelima Devi Boddeti, K Salomi Monica, R Prabha, and V Venkatesh. Iot based smart healthcare monitoring systems: A literature review. *Eur. J. Mol. Clin. Med*, 7:2020, 2021.

[2] IBM. What is the internet of things (iot)? https://www.ibm.com/topics/internet-of-things, Accessed: 2023.

[3] Cisco. Internet of things (iot). https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html, Accessed: 2023.

[4] Xu Cheng, Minghui Zhang, and Fuquan Sun. Architecture of internet of things and its key technology integration based-on rfid. In *Fifth International Symposium on Computational Intelligence and Design*, pages 294–297. IEEE, 2012.

[5] Debasis Bandyopadhyay and Jaydip Sen. Internet of things-applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69, 2011.

[6] Ying Zhang. Technology framework of the internet of things and its application. In *Electrical and Control Engineering (ICECE)*, pages 4109–4112. IEEE, 2011.

[7] Guicheng Shen and Bingwu Liu. The visions, technologies, applications and security issues of internet of things. In *E-Business and E-Government (ICEE)*, pages 1–4. IEEE, 2011.

[8] Miao Wu, Ting-lie Lu, Fei-Yang Ling, Ling Sun, and Hui-Ying Du. Research on the architecture of internet of things. In *Advanced Computer Theory and Engineering (ICACTE)*, pages 484–487. IEEE, 2010.

[9] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: The internet of things architecture, possible applications and key challenges. In *Proceedings of Frontiers of Information Technology (FIT)*, pages 257–260. IEEE, 2012.

[10] R. Abdmeziem and D. Tandjaoui. Internet of things: Concept, building blocks, applications and challenges. *Computers and Society*, Year.

[11] Maciej Haras and Thomas Skotnicki. Thermoelectricity for iot–a review. *Nano Energy*, 54:461–476, 2018.

[12] Patrick Fuhrer and Dominique Guinard. Building a smart hospital using rfid technologies. *IEEE Pervasive Computing*.

[13] F. TongKe. Smart agriculture based on cloud computing and iot. *Journal of Convergence Information Technology (JCIT)*, Jan 2013.

[14] ThingMagic. Rfid security issues - generation2 security.

[15] Yingshuai Wang, Garhan Attebury, and Byrav Ramamurthy. A survey on security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 8(2):2–23, 2006.

[16] V. Ashktorab and S.R. Taghizadeh. Security threats and countermeasures in cloud computing. *International Journal of Application or Innovation in Engineering and Management (IJAIEM)*, 1(2), October 2012.

[17] S Vishnu, SR Jino Ramson, and R Jegan. Internet of medical things (iomt)-an overview. In *2020 5th international conference on devices, circuits and systems (ICDCS)*, pages 101–104. IEEE, 2020.

[18] Nimra Dilawar, Muhammad Rizwan, Fahad Ahmad, and Saima Akram. Blockchain: securing internet of medical things (iomt). *International Journal of Advanced Computer Science and Applications*, 10(1), 2019.

[19] Shadab Alam, Mohammed Shuaib, Sadaf Ahmad, Dushantha Nalin K Jayakody, Ammar Muthanna, Salil Bharany, and Ibrahim A Elgendy. Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (iomt) integration. *Sustainability*, 14(22):15312, 2022.

[20] D Singh Rajput and Rakesh Gour. An iot framework for healthcare monitoring systems. *International Journal of Computer Science and Information Security*, 14(5), 2016.

[21] Nipuni Nanayakkara, Malka Halgamuge, and Ali Syed. Security and privacy of internet of medical things (iomt) based healthcare applications: A review. In *2019 IIER 750th International Conference on Advances in Business Management and Information Technology (ICABMIT)*, pages 1–18. Institute for Technology and Research, 2019.

[22] MM Kamruzzaman. Architecture of smart health care system using artificial intelligence. In *2020 IEEE international conference on multimedia & expo workshops (ICMEW)*, pages 1–6. IEEE, 2020.

[23] A Ravishankar Rao and Daniel Clarke. A fully integrated open-source toolkit for mining healthcare big-data: architecture and applications. In *2016 IEEE international conference on healthcare informatics (ICHI)*, pages 255–261. IEEE, 2016.

[24] Jiangfeng Sun, Fazlullah Khan, Junxia Li, Mohammad Dahman Alshehri, Ryan Alturki, and Mohammad Wedyan. Mutual authentication scheme for the device-to-server communication in the internet of medical things. *IEEE Internet of Things Journal*, 8(21):15663–15671, 2021.

[25] Lanfang Sun, Xin Jiang, Huixia Ren, and Yi Guo. Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application. *IEEE Access*, 8:101079–101092, 2020.

[26] Rajinder Tiwari. An overview of internet of things (iot): From literature survey to application implementation perspective. *International Research Journal of Engineering and Technology*, 4(1):575–582, 2017.

[27] K Uday Kumar Reddy, S Shabbiha, and M Rudra Kumar. Design of high security smart health care monitoring system using iot. *Int. J*, 8, 2020.

[28] Yu Pang, Zhen Yang, Yifan Yang, Xiaoming Wu, Yi Yang, and Tian-Ling Ren. Graphene based wearable sensors for healthcare. In *2019 International Conference on IC Design and Technology (ICICDT)*, pages 1–4. IEEE, 2019.

[29] Rakhi Bhardwaj, Shiv Narain Gupta, Manish Gupta, and Priyesh Tiwari. Iot based healthware and healthcare monitoring system in india. In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pages 406–408. IEEE, 2021.

[30] A Khanna and P Misra. The internet of things for medical devicesâprospects. *Challenges and the Way Forward, A white paper*, 2013.

[31] Z. Pang, J. Tian, and Q. Chen. Intelligent packaging and intelligent medicine box for medication management towards the internet of things. In *Proc. 16th International Conference on Advanced Communication Technology (ICACT)*, February 2014.

[32] Link Labs. Iot in health care: What you should know. Online.

[33] Warish D Patel, Chirag Patel, and Carlos Valderrama. Iomt based efficient vital signs monitoring system for elderly healthcare using neural network. *International Journal of Research*, 8(I), 2019.

[34] Chao Li, Xiangpei Hu, and Lili Zhang. The iot-based heart disease monitoring system for pervasive healthcare service. *Procedia computer science*, 112:2328–2334, 2017.

[35] Hui-Ru Cao and Choujun Zhan. A novel emergency healthcare system for elderly community in outdoor environment. *Wireless Communications and Mobile Computing*, 2018, 2018.

[36] Ankit Narendrakumar Soni. Smart devices using internet of things for health monitoring. *International Journal of Innovative Research in Science, Engineering and Technology*, 7(5):6355–6361, 2018.

[37] SM Riazul Islam, Daehan Kwak, MD Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. The internet of things for health care: a comprehensive survey. *IEEE access*, 3:678–708, 2015.

[38] Pawan Singh. Internet of things based health monitoring system: opportunities and challenges. *International Journal of Advanced Research in Computer Science*, 9(1):224–228, 2018.

[39] C Arcadius Tokognon, Bin Gao, Gui Yun Tian, and Yan Yan. Structural health monitoring framework based on internet of things: A survey. *IEEE Internet of Things Journal*, 4(3):619–635, 2017.

[40] M Shamim Hossain and Ghulam Muhammad. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. *Computer Networks*, 101:192–202, 2016.

[41] Naidila Sadashiv and SM Dilip Kumar. Cluster, grid and cloud computing: A detailed comparison. In *2011 6th international conference on computer science & education (ICCSE)*, pages 477–482. IEEE, 2011.

[42] Lena Griebel, Hans-Ulrich Prokosch, Felix Köpcke, Dennis Toddenroth, Jan Christoph, Ines Leb, Igor Engel, and Martin Sedlmayr. A scoping review of cloud computing in healthcare. *BMC medical informatics and decision making*, 15(1):1–16, 2015.

[43] Sanjay P Ahuja, Sindhu Mani, and Jesus Zambrano. A survey of the state of cloud computing in healthcare. *Network and Communication Technologies*, 1(2):12, 2012.

[44] Harshita Bhatia, Surya Narayan Panda, and Dimple Nagpal. Internet of things and its applications in healthcare-a survey. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pages 305–310. IEEE, 2020.

[45] Kamran Sattar Awaisi, Shahid Hussain, Mansoor Ahmed, Arif Ali Khan, and Ghufran Ahmed. Leveraging iot and fog computing in healthcare systems. *IEEE Internet of Things Magazine*, 3(2):52–56, 2020.

[46] Udit Jain, Abhinav Gumber, D Ajitha, GK Rajini, and Balaji Subramanian. A review on a secure iot-based healthcare system. *Advances in Automation, Signal Processing, Instrumentation, and Control: Select Proceedings of i-CASIC 2020*, pages 3005–3016, 2021.

[47] Prateeksha Varshney and Yogesh Simmhan. Demystifying fog computing: Characterizing architectures, applications and abstractions. In *2017 IEEE 1st international conference on fog and edge computing (ICFEC)*, pages 115–124. IEEE, 2017.

[48] Arjun Venkataraman. Edge computing: A primer for healthcare leaders. *Healthcare Informatics*, 2019.

[49] Behnaz Ghoraani, Hitesh Arora, Riyaz Wazirali, and Jinliang Yuan. Edge computing for remote patient monitoring: Opportunities and challenges. *IEEE Journal of Translational Engineering in Health and Medicine*, 7:1–11, 2019.

[50] Mohamed R. M. Rizk, Amani Abou-Elnour, Nashwa A. Ismail, Hala El-Sayed, and Sara A. El-Rahman. Telemedicine using smart mobile devices and edge computing technologies: A review. *IEEE Access*, 9:34702–34715, 2021.

[51] Feng Liu, Shanlin Yang, and Naixue Xiong. An edge computing-based telemedicine system for remote patient monitoring. *IEEE Journal of Biomedical and Health Informatics*, 24:2044–2054, 2020.

[52] Rafael Díaz-Granados, Rolando Trujillo-Rasua, and Jiajia Zhang. Edge analytics in healthcare: Opportunities and challenges. *Journal of Medical Systems*, 43:1–15, 2019.

[53] Pooyan Asgari, Mohammad Pourhomayoun, and Xiaonan Wang. Predictive analytics in healthcare: A review of current applications and trends. *IEEE Access*, 9:24216–24229, 2021.

[54] S. S. Nadar, N. Rathi, B. Anjum, and V. Laxmi. Edge computing for medical imaging: A review. *IEEE Journal of Translational Engineering in Health and Medicine*, 6:1–8, 2018.

[55] V. K. Saini, P. Kumar, and B. Lohani. Smart medical imaging: An edge-cloud deep learning solution for remote medical diagnosis. *IEEE Access*, 9:57794–57802, 2021.

[56] Mahadev Satyanarayanan. How we created edge computing. *Nature Electronics*, 2(1):42–42, 2019.

[57] Ejaz Ahmed, Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Imran Khan, Abdelmuttlib Ibrahim Abdalla Ahmed, Muhammad Imran, and Athanasios V Vasilakos. The role of big data analytics in internet of things. *Computer Networks*, 129:459–471, 2017.

[58] Muhammad Habib ur Rehman, Ibrar Yaqoob, Khaled Salah, Muhammad Imran, Prem Prakash Jayaraman, and Charith Perera. The role of big data analytics in industrial internet of things. *Future Generation Computer Systems*, 99:247–259, 2019.

[59] Wazir Zada Khan, Ejaz Ahmed, Saqib Hakak, Ibrar Yaqoob, and Arif Ahmed. Edge computing: A survey. *Future Generation Computer Systems*, 97:219–235, 2019.

[60] Yuyu Yin, Lu Chen, Yueshen Xu, Jian Wan, He Zhang, and Zhida Mai. Qos prediction for service recommendation with deep feature learning in edge computing environment. *Mobile networks and applications*, 25:391–401, 2020.

[61] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78:680–698, 2018.

[62] A Varshney, N Garg, KS Nagla, TS Nair, SK Jaiswal, S Yadav, and DK Aswal. Challenges in sensors technology for industry 4.0 for futuristic metrological applications. *Mapan*, 36(2):215–226, 2021.

[63] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, 135:62–75, 2019.

[64] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee, 2017.

[65] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. *arXiv preprint arXiv:1906.11078*, 2019.

[66] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. Where is current research on blockchain technology?âa systematic review. *PloS one*, 11(10):e0163477, 2016.

[67] Marianna Belotti, Nikola Božić, Guy Pujolle, and Stefano Secci. A vademecum on blockchain technologies: When, which, and how. *IEEE Communications Surveys & Tutorials*, 21(4):3796–3838, 2019.

[68] Myles Snider, Kyle Samani, and Tushar Jain. Delegated proof of stake: features & tradeoffs. *Multicoin Cap*, 19, 2018.

[69] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. 2018.

[70] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[71] Peng Zhang, Douglas C Schmidt, Jules White, and Gunther Lenz. Blockchain technology use cases in healthcare. In *Advances in computers*, volume 111, pages 1–41. Elsevier, 2018.

[72] Garry Gabison. Policy considerations for the blockchain technology public and private applications. *SMU Sci. & Tech. L. Rev.*, 19:327, 2016.

[73] Asger B Pedersen, Marten Risius, Roman Beck, et al. A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive*, 18(2):99–115, 2019.

[74] Juan M Roman-Belmonte, Hortensia De la Corte-Rodriguez, and E Carlos Rodriguez-Merchan. How blockchain technology can change medicine. *Postgraduate medicine*, 130(4):420–427, 2018.

[75] Tushar Dey, Shaurya Jaiswal, Shweta Sunderkrishnan, and Neha Katre. Healthsense: A medical use case of internet of things and blockchain. In *2017 International conference on intelligent sustainable systems (ICISS)*, pages 486–491. IEEE, 2017.

[76] Zonyin Shae and Jeffrey Tsai. Transform blockchain into distributed parallel computing architecture for precision medicine. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pages 1290–1299. IEEE, 2018.

[77] Polina Mamoshina, Lucy Ojomoko, Yury Yanovich, Alex Ostrovski, Alex Botezatu, Pavel Prikhodko, Eugene Izumchenko, Alexander Aliper, Konstantin Romantsov, Alexander Zhebrak, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*, 9(5):5665, 2018.

[78] Mohammed Shuaib, Noor Hafizah Hassan, Sahnius Usman, Shadab Alam, Surbhi Bhatia, Arwa Mashat, Adarsh Kumar, and Manoj Kumar. Self-sovereign identity solution for blockchain-based land registry system: a comparison. *Mobile Information Systems*, 2022:1–17, 2022.

[79] Christophe Schinckus. A nuanced perspective on blockchain technology and healthcare. *Technology in Society*, 71:102082, 2022.

[80] Edward H Shortliffe. The evolution of electronic medical records. *Academic Medicine*, 74(4):414–9, 1999.

[81] SoonHyeong Jeong, Jun-Hong Shen, and Byeongtae Ahn. A study on smart healthcare monitoring using iot based on blockchain. *Wireless Communications and Mobile Computing*, 2021:1–9, 2021.

[82] Adrien Bécue, Eva Maia, Linda Feeken, Philipp Borchers, and Isabel Praça. A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, 10(13):4482, 2020.

[83] Michael Schluse, Marc Priggemeyer, Linus Atorf, and Juergen Rossmann. Experimentable digital twinsâstreamlining simulation-based systems engineering for industry 4.0. *IEEE Transactions on industrial informatics*, 14(4):1722–1731, 2018.

[84] Michael Grieves. Digital twin: manufacturing excellence through virtual factory replication. *White paper*, 1(2014):1–7, 2014.

[85] Edward Glaessgen and David Stargel. The digital twin paradigm for future nasa and us air force vehicles. In *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference*, page 1818, 2012.

[86] Fei Tao, Fangyuan Sui, Ang Liu, Qinglin Qi, Meng Zhang, Boyang Song, Zirong Guo, Stephen C-Y Lu, and Andrew YC Nee. Digital twin-driven product design framework. *International Journal of Production Research*, 57(12):3935–3953, 2019.

[87] Lihui Wang, Weiming Shen, Helen Xie, Joseph Neelamkavil, and Ajit Pardasani. Collaborative conceptual designâstate of the art and future trends. *Computer-aided design*, 34(13):981–996, 2002.

[88] Radhakisan Baheti and Helen Gill. Cyber-physical systems. *The impact of control technology*, 12(1):161–166, 2011.

[89] Anderson Luis Szejka, Osiris Canciglieri Júnior, Eduardo Rocha Loures, Hervé Panetto, and Alexis Aubry. Proposal of a model-driven ontology for product development process interoperability and information sharing. In *Product Lifecycle Management for Digital Transformation of Industries: 13th IFIP WG 5.1 International Conference, PLM 2016, Columbia, SC, USA, July 11-13, 2016, Revised Selected Papers 13*, pages 158–168. Springer, 2016.

[90] Michael Grieves and John Vickers. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. *Transdisciplinary perspectives on complex systems: New findings and approaches*, pages 85–113, 2017.

[91] Cordelia Mattuvarkuzhali Ezhilarasu, Zakwan Skaf, and Ian K Jennions. Understanding the role of a digital twin in integrated vehicle health management (ivhm). In *2019 IEEE International Conference on Systems, Man and Cybernetics (SMC)*, pages 1484–1491. IEEE, 2019.

[92] Stefan Boschert and Roland Rosen. Digital twinâthe simulation aspect. *Mechatronic futures: Challenges and solutions for mechatronic systems and their designers*, pages 59–74, 2016.

[93] Radhya Sahal, Saeed H Alsamhi, and Kenneth N Brown. Personal digital twin: a close look into the present and a step towards the future of personalised healthcare industry. *Sensors*, 22(15):5918, 2022.

[94] Yujun Ma, Yulei Wang, Jun Yang, Yiming Miao, and Wei Li. Big health application system based on health internet of things and big data. *IEEE Access*, 5:7885–7897, 2016.

[95] Bo Jin, Tran Hoai Thu, Eunhye Baek, Sung Hwan Sakong, Jin Xiao, Tapas Mondal, and M Jamal Deen. Walking-age analyzer for healthcare applications. *IEEE journal of biomedical and health informatics*, 18(3):1034–1042, 2014.

[96] Ying Liu, Lin Zhang, Yuan Yang, Longfei Zhou, Lei Ren, Fei Wang, Rong Liu, Zhibo Pang, and M Jamal Deen. A novel cloud-based framework for the elderly healthcare services using digital twin. *IEEE access*, 7:49088–49101, 2019.

[97] Bergthor Björnsson, Carl Borrebaeck, Nils Elander, Thomas Gasslander, Danuta R Gawel, Mika Gustafsson, Rebecka Jörnsten, Eun Jung Lee, Xinxiu Li, Sandra Lilja, et al. Digital twins to personalize medicine. *Genome medicine*, 12:1–4, 2020.

[98] Radhya Sahal, Saeed H Alsamhi, Kenneth N Brown, Donna OâShea, Bader Alouffi, et al. Blockchain-based digital twins collaboration for smart pandemic alerting: decentralized covid-19 pandemic alerting use case. *Computational Intelligence and Neuroscience*, 2022, 2022.

[99] Mustafa A Al-Sheikh and Ibrahim A Ameen. Design of mobile healthcare monitoring system using iot technology and cloud computing. In *IOP conference series: materials science and engineering*, volume 881, page 012113. IOP Publishing, 2020.