electronics

Article

SEMRAchain: A Secure Electronic Medical Record Based on Blockchain Technology

Halima Mhamdi [1], Manel Ayadi [2], Amel Ksibi [2,*], Amal Al-Rasheed [2], Ben Othman Soufiene [3] and Sakli Hedi [1]

[1] MACS Research Laboratory RL16ES22, National Engineering School of Gabes, Gabes 6029, Tunisia
[2] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[3] PRINCE Laboratory Research, ISITcom, University of Sousse, Hammam Sousse, Sousse 4011, Tunisia
* Correspondence: amelksibi@pnu.edu.sa

Abstract: A medical record is an important part of a patient's follow-up. It comprises healthcare professionals' views, prescriptions, analyses, and all information about the patient. Several players, including the patient, the doctor, and the pharmacist, are involved in the process of sharing, and managing this file. Any authorized individual can access the electronic medical record (EMR) from anywhere, and the data are shared among various health service providers. Sharing the EMR requires various conditions, such as security and confidentiality. However, existing medical systems may be exposed to system failure and malicious intrusions, making it difficult to deliver dependable services. Additionally, the features of these systems represent a challenge for centralized access control methods. This paper presents SEMRAchain a system based on Access control (Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC)) and a smart contract approach. This fusion enables decentralized, fine-grained, and dynamic access control management for EMR management. Together, blockchain technology as a secure distributed ledger and access control provides such a solution, providing system stakeholders with not just visibility but also trustworthiness, credibility, and immutability.

Keywords: blockchain; smart contract; role-based access control; attribute-based access control; electronic medical record; multi-agents-system

Citation: Mhamdi, H.; Ayadi, M.; Ksibi, A.; Al-Rasheed, A.; Soufiene, B.O.; Hedi, S. SEMRAchain: A Secure Electronic Medical Record Based on Blockchain Technology. *Electronics* **2022**, *11*, 3617. https://doi.org/10.3390/electronics11213617

Academic Editors: Junaid Arshad, Jonathan Loo and Omair Shafiq

Received: 12 October 2022
Accepted: 4 November 2022
Published: 6 November 2022

1. Introduction

The global IoT medical device market is predicted to increase at a 4.5 percent compound yearly growth rate, reaching $409.5 billion in 2025 [1]. This technology may completely disconnect a patient from the hospital's centralized system while yet allowing them to speak with their doctor. In the healthcare sector, patient medical data are extremely sensitive, requiring effective privacy protection [2]. These data are typically kept in various places and are manipulated by many healthcare practitioners. With the advancement of technology such as the Internet of Things (IoT) [3] and artificial intelligence (AI) [4], health files are now saved electronically. The use of electronic health files allows for the secure storage of patients' personal information for the diagnosis of various conditions [5]. This entails digitizing this information and sharing them with healthcare experts, with the patient's permission, so that they may be updated in real-time in a safe and confidential way [6]. Therefore, the security of medical data is a criterion to be considered. Indeed, many cryptography-based approaches have been built to remedy the security problem and block attacks in healthcare applications using IoT [7].

The proposed schemes [8] provide patient data privacy with authentication. Others resort to the use of AI to develop a protocol and algorithm based on deep learning to ensure privacy and authenticate patient data [9]. For the same purpose, fog computing is leveraged in various other solutions [10]. The volume of transferred data in the offered solutions

is enormous, and the network's scale expands with each new user [11]. As a result, it is critical to secure the integrity and consistency of the intended system, which must fulfill several standards, including strong resilience to attack, respect for patient privacy, and control over access to these data [12].

In a peer-to-peer network, machines and devices connect to one another without the need for intermediaries, resulting in a decentralized network known as the Blockchain [13]. It is, in fact, a network of interconnected nodes that share and record transactions. To avoid a single point of failure, each node in the network stores a copy [14]. The blockchain's data are organized in blocks that are linked together to form a distributed ledger (DLT). Cryptographic functions protect the data's security and immutability. Satoshi Nakamoto first proposed the notion of blockchain in 2008 [15]. Blockchain technology is distinguished by several key characteristics, including decentralization, transparency, autonomy, security, and immutability [16,17]. These attributes raise the need for blockchain technology in a multitude of sectors [18,19]. For example, in the field of cyber-physical systems, authors discussed the use of this technology to ensure the confidentiality, integrity and availability of data transmission. They also discussed the concept of a consensus mechanism to ensure the security of these systems [20,21].

To overcome these challenges in decentralization, automation, security, and trust management of stakeholders in healthcare, the combination of blockchain technology and multi-agent systems is a key solution. Blockchain technology provides just such a solution in the form of a distributed and secure registry that allows patients not only to have visibility over their data but also to control access to it. Therefore, via Blockchain technology, we ensure the interoperability of the platform used by the various health actors. Similarly, for the emergency service, it can access patient data without the need to request it from the patient. The MAS allows for automating the interactions between the agents forming a fully decentralized system. Indeed, the MAS consolidates the efficiency and confidence of human/machine or machine/machine communication. It also ensures the security of the agents. The authors [22,23] have exploited the multi-agent system and proposed a trust management system between agents by using the technique of identification of agents via private and public keys. Based on smart contracts, the proposed solution consists in exploiting RBAC and ABAC access control techniques. This solution removes the central authority (CA) to reduce maintenance costs and eliminate legacy threats from centralized systems.

Integrated with the health domain, we intend to track the electronic medical record using blockchain technology. The main objective is to ensure security and trust between the agents in the system by establishing automated communication without human intervention via smart contracts. To guarantee the security of patient data, the following criteria must be taken into consideration: authentication and access control.

The main contributions of this paper can be summarized as follows:

- ❖ Proposing a blockchain-based platform for handling electronic patient records.
- ❖ Exploiting access control techniques namely ABAC and RBAC to access our system and avoid any external intrusion.
- ❖ Merging smart contracts and access control to guarantee the security and confidentiality of managed data.

The remainder of this document is organized as follows. Section 2 is devoted to the basic concept of blockchain technology and EMR. Section 3 presents the integration of blockchain in medical record management. The proposed system architecture is introduced in detail in Section 4. While Section 5 describes the simulation platform and the obtained results as well as the analysis and performance of the system. Finally, Section 6 concludes this paper and gives some hints for further research.

2. Basic Concept of Blockchain Technology and EMR

This section is dedicated to overview some basic notions related to blockchain technology as well as EMR systems and access control.

2.1. Blockchain Technology

The Bitcoin application introduced by Satoshi Nakamoto in 2008 endorsed Blockchain. Blockchain is based on the concept of a decentralized ledger, which allows for more secure transactions. From 2009 to 2013, Blockchain was used in digital currency transactions and was referred to as Blockchain 1.0. Later, in 2015, the use of Smart Contracts introduced Blockchain 2.0, which provided better authentication and a tamperproof transaction process. The Ethereum platform introduces Blockchain 3.0 and the concept of DApps. We are now living with Blockchain 4.0, which is bringing forward its application in business and industries [10].

- ❖ Blockchain features: Blockchain technology is characterized by many important features as illustrated in Figure 1. It is a decentralized P2P network in which data are stored in all nodes of the network. Thanks to a well-defined protocol, all nodes can manipulate, access and update transactions at the same time and without the need for an intermediary. These data are not all stored on the server of a central intermediary but are instead "distributed". This property eliminates the problems associated with a centralized system. It also promotes anonymity, i.e., the identity of users is not broadcast to other users, except to the one participating in the transaction. All transactions in the blockchain are time-stamped, meaning that all transactions have a start time, an end time, and the length of time they have been active. Once recorded in the blockchain, it is impossible to delete or modify a transaction since there are multiple copies in different nodes of the network. Therefore, blocks can be extended and not changed. This gives the blockchain a high level of security and makes it more difficult to attack blocks of information.

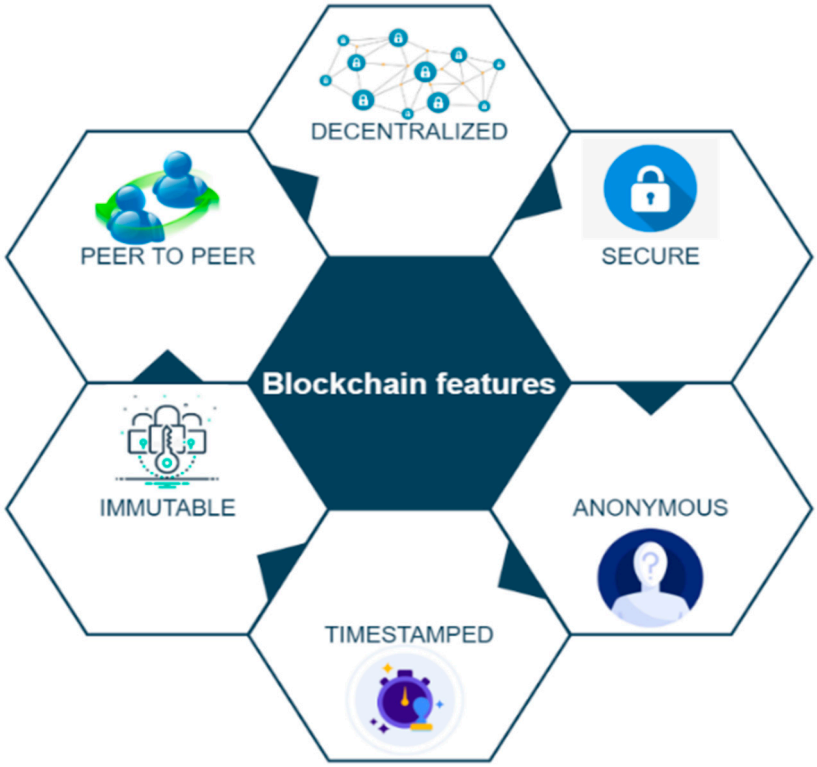

Figure 1. Blockchain features.

- ❖ Smart contracts: Nick Szabo, a computer scientist and cryptographer, pioneered the concept of smart contracts in the 1990s. The concept has recently been identified as being more useful in association with the progress of blockchain and DLTs. Smart contracts are digital forms of contracts that consist of a set of terms that must be met to carry out specific tasks, such as transferring assets or making a deposit.

Because smart contracts are scripted and fully automated, they do not require any counterparties. The concept is supposed to follow a simple logic and to be verified by cryptographic methods.

- Consensus mechanism: Blockchain consensus protocols create a system of irrefutable agreement between different parties within a distributed network while preventing malicious exploitation of the system. They allow the blockchain to be updated while ensuring that every block on the chain is valid. They also prevent a single entity from controlling the entire network, thus guaranteeing its decentralization. There are several mechanisms for validating a block. For example, proof of work (PoW), proof of stake (PoS), practical byzantine fault tolerance (PBFT), proof of authority (PoA) and proof of elapsed time (PoET).

2.2. Multi-Agents' System

A MAS is a self-contained distributed system comprised of multiple agents capable of carrying out their functions. Each agent in the system is an independent computational entity with one or more objectives, knowledge, and skills. To address challenges, the agents collaborate. MAS is also commonly used in the construction of distributed systems, with the goal of achieving high system dependability, availability, openness, resource sharing, and reusability [18].

2.3. Access Control

Access control is a technique for controlling user access to resources. It indicates the actions to be performed by each user and restrict illegal access to information. Authentication, identification, and authorization are the basis of the access control model. Among the most used types of access control is Discretionary Access Control (DAC), Attribute Based Access Control (ABAC), Role Based Access Control (RBAC) and Mandatory Access Control (MAC) [22].

- Discretionary Access Control: In DAC, the owner of a resource decides how it can be shared. He can choose to give read or write access to other users.
- Attribute Based Access Control: ABAC is a logical access control paradigm that regulates object access by assessing some stated control rule or policy against subject, object, action, and environment properties. The primary idea behind ABAC is to enable all authorization based on the subject's characteristics rather than assigning permissions directly between subjects and objects.
- Role Based Access Control: RBAC is called also non-discretionary access control. In this type, users are assigned a role and the role dictates access to a resource. It is, in fact, a set of rules that determines how subjects and objects interact.
- Mandatory Access Control: Access rights are governed by a vital force that is subject to varying levels of security. The needed authorization control includes distributing representations to structural resources as well as the privacy feature or operating framework. Access to assured assets is restricted to clients or devices that have the basic data exceptional status.

2.4. EMR Systems

According to the committee recommendation of 6.2.2019 on a European Electronic Health Record exchange format, EMR is defined as a patient file that contains the following data: patient records, electronic prescription/electronic dispensing, laboratory results, medical imaging and related reports, and hospital discharge reports [23]. Today's medical record systems are extremely vulnerable to data degradation, forgery, and loss because they are stored in various healthcare facilities and manipulated in a centralized way. In this case, many hospitals keep the data of their patients in a database through an agent. However, even in this case, the patient must bring his file with him if he changes doctor or the hospital. This is an unreliable way to manage such sensitive information [24].

3. Related Work

Blockchain technology provides an immutable, decentralized network in which all participating nodes can use consensus algorithms and smart contracts to validate transactions. Various healthcare systems [25,26] have used the blockchain because it is a dependable method for improving communication privacy and security. Table 1 to be used later on to highlight the research gaps and to report our own research motivations.

In [27], authors have exploited smart contracts to design a system for remote patient monitoring and alerting health specialists in case of emergency. This remote monitoring system guarantees the security and privacy of the patient through blockchain. The proposed system has three functions and three actors. The first function is the registration of patients and doctors on the platform. They access it via a smartphone and register their data such as their id, name, and age, in a secure way. They can also consult and update these data. For patient monitoring, processing will be done on the data received from the IoT sensor and then they will be stored by smart contracts in the blockchain. This step makes it easier for doctors to follow their patients in real-time. The last function concerns the company and the medical devices. When a device is purchased, a smart contract is established between the company and the patient to register it in his name. In this way, the patient's information retrieved by the IoT tool is registered in the care center.

MedChain is a platform proposed by S. Bingqing et al. [28]. It works on the same principle of sharing data by storing them immutably in the blockchain. The actors of Medchain are the patient, the physician, and the healthcare provider. They share data with each other using three approaches, namely blockchain technology, a P2P network, and a condensation chain. These approaches collaborate and provide a flexible and efficient data-sharing system.

In their paper [29], the authors exploit the notion of smart contracts and multi-agent systems to control and monitor logistics pharmaceutical activities. They propose a platform allowing the storage of transactions between the different actors of the system in the blockchain. Smart contracts ensure the management of these transactions without any third party. This makes the system less expensive and faster in terms of delivery time. However, to evaluate its performance and efficiency, it is necessary to develop a real prototype in parallel with empirical validation.

The work of A. Saini et al. [30] is based on the use of the Ethereum private blockchain. It exploits the notion of smart contracts for managing the electronic medical record (EMR). The EMR contains sensitive patient data. Security must be considered when processing them. To this end, the authors have designed a model for sharing medical data between patients, hospitals and any other entity involved in this process. The smart contracts used ensure EMR privacy by using cryptographic and access control features, while the cloud allows medical data to be saved to eliminate network congestion. Real-time monitoring of the EMR in a decentralized and patient-centric manner is guaranteed by the proposed framework.

The authors of [31] suggested the BiiMed platform. This approach intends to share the patient's electronic health record across several actors. The blockchain provides data integrity and interoperability. The suggested architecture is divided into two components: the health information system (HIS) and the BiiMed blockchain. The HIS collects, stores, and distributes medical data, while the BiiMed platform maintains the shared data. It is built on the Ethereum blockchain and smart contracts. Interoperability and data integrity are hallmarks of electronic medical record exchange. The technology established using a decentralized trustworthy network ensures these qualities.

To maintain security, traceability and visibility in the pharmaceutical supply chain, the authors [32] designed a private blockchain platform to fight drug counterfeiting. These characteristics are assured by proof of ownership. Each actor in the pharmaceutical supply chain process: the manufacturer, distributor as well as retailer must have the authorization to distribute the pharmaceutical product.

The authors [33] address the issue of privacy and transparency of patients' medical data by developing a system that tracks patients' vital signs. Smart contracts and the

Hyperledger Fabric blockchain form the basis of this platform. The proposed system receives data from medical sensors and shares it in the blockchain network. These data are then tracked and processed by smart hospital actors via a web application based on HTML5 and JavaScript and facilitating data access. Performance is ensured by the traceability and security of the patient's vital parameters. Its features, such as low latency, simple interface, and high-speed transaction, make the presented prototype perform well. On the other hand, it suffers from security gaps, and this is due to the lack of authentication between the system components namely the server and the IoT sensors. The system can be improved by adding a part ensuring the communication between its distinct parts while considering the synchronization between IoT resources.

In their work [34], the authors exploited smart contracts to design a system for remote patient monitoring and alerting healthcare specialists in case of emergency. This remote monitoring system ensures patient security and privacy using blockchain. The proposed system has three functions and three actors. The first function is the registration of patients and doctors on the platform. They access it via a Smartphone and register their data such as their id, name, age, etc., in a secure way. They can also consult and update these data. For patient monitoring, processing will be performed on the data received from the IoT sensor, and then it will be stored by smart contracts in the blockchain. This step makes it easier for doctors to track their patients in real-time. The last function is about business and medical devices. When a device is purchased, a smart contract is established between the company and the patient to register it in their name. In this way, the patient's information retrieved by the IoT tool is registered with the healthcare center.

G. Srivastava et al. [35] have developed a protocol named GHOSTDAG that enables patient tracking. They use two public and private blockchains to ensure the security of medical data. The proposed system consists of a patient, a healthcare facility, the GHOSTDAG blockchain and smart contracts. Remote patient monitoring (RPM) devices collect the patient's vital parameters and send them to the smart device. These data are then encrypted and stored on a private blockchain via smart contracts. The latter also has the role of transmitting the information to a public blockchain that will be used by the healthcare institution. Alerts are also sent if the vital parameters exceed a predefined threshold. The model presented is characterized by its reliability and security, but its effectiveness must be verified by the implementation of an RPM prototype.

The authors proposed an electronic healthcare system [36]. Their architecture is based on blockchain technology and wireless body area networks (WBAN). The WBAN with the IEEE 802.15.6 standard provides the interaction between biomedical sensors and blockchain technology that enables data storage. The fusion of these two concepts provides a secure system that respects the privacy of the patient. Several actors are integrated into this system, including patients, hospitals, pharmacies, and doctors. To develop their prototype, the authors use the private blockchain HyperLedger Fabric and smart contracts. They also designed web interfaces for each actor. These interfaces facilitate access to medical records. Security, performance, and low hardware usage are the main contributors. The proposed system can be extended and scaled to support many participants and enormous amounts of medical data.

The authors [37,38] have developed a platform for exchanging clinical data between various users. They used a private blockchain to aggregate health information from various clinical sites. Smart contracts and RPC (Remote Procedure Call) servers are the basis of the proposed system. To facilitate its use, a web interface is required. The clinical data are collected and shared from various databases of different clinical sites. They are manipulated by smart contracts. The characteristics of blockchain, notably its immutability, transparency, and decentralization, encourage the development of platforms and systems for collecting and sharing patient data in clinical trials.

In their work [39], the authors have proposed an architecture named BIoMT to solve the problems encountered in the cloud-based one. Security is ensured through this architecture

thanks to the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) as well as proof of work as a consensus mechanism.

Table 1. Summarized Literature Review.

Refs.	Contribution	Blockchain			Performance			
		1	2	3	4	5	6	7
[27]	Design a system for remote patient monitoring and alerting health specialists in case of emergency.	*			*		*	*
[28]	Offer a MedChain platform to share data by storing it immutably in the blockchain.		*			*	*	
[29]	Use smart contracts and multi-agents' system to control and monitor logistics pharmaceutical activities.	*					*	*
[30]	Design a model for sharing medical data between patients, hospitals and any other entity involved in this process.	*		*				
[31]	To propose a platform named BiiMed. This solution aims to share the patient's electronic health record between different stakeholders.	*				*		
[32]	Design a private blockchain platform to fight drug counterfeiting and maintain security, traceability, and visibility in the pharmaceutical supply chain.		*				*	*
[33]	Develop a system that allows the monitoring of the patient's vital signs.	*		*			*	
[34]	Design a system to remotely monitor patients and alert healthcare specialists in the event of an emergency.	*					*	
[35]	To develop a protocol named GHOSTDAG allowing the follow-up of patients.	*			*		*	
[36]	Propose an electronic health system for medical records. Security, performance, and low hardware usage are the main contributions.	*			*		*	
[37,38]	Develop a platform for exchanging clinical data between various users.	*				*	*	
[39]	Propose BIoMT architecture based on the ECDSA algorithm and Proof of Work consensus protocol to secure medical data.	*	*		*	*		

1: Smart contract, 2: consensus mechanism, 3: Access control, 4: confidentiality, 5: Integrity, 6: privacy, 7: Authentication, *: criterion exists.

4. Proposed System

The proposed system, SEMRAchain, is a platform allowing the exchange and sharing of patient medical records. This solution combines blockchain technology and multi-agent systems. To ensure the security of the data manipulated by the different stakeholders, access control (ABAC and RBAC) as well as smart contracts are exploited. The system must also meet certain requirements. In the blockchain-based healthcare system, the identity of individuals with the right to participate in the electronic medical record management process must be verified. Indeed, participants must authenticate themselves to have access to resources. Additionally, each participant has a predefined role in the processing of the patient's file. In fact, they have access only to the resources necessary to accomplish their tasks. The data exchanged in healthcare are large and the scale of the network evolves each time a user is added, so scalability must be considered. For all users to benefit from the required medical data service, an electronic medical record system should include a flexible user interface that allows for the efficient and simplified use of resources. The application must meet the CIA triad (confidentiality, integrity, availability). Patient data require protection from viewing or other unauthorized access or modification to ensure reliability and accuracy. It is also available to authorized users who need it.

Various agents, as shown in Figure 2, have access to patient data. These data are aggregated and stored on the blockchain. The consultations as well as the update of the EMR are controlled by a smart contract. Each agent must be authenticated to be

able to manipulate, in a limited time, the information that suits them. After examining a patient, the doctor agent writes prescriptions and adds scans and test results which are all recorded as operations. The pharmacy dispenses medications and records the transaction on the blockchain. The same goes for analyses from the laboratory. Via smart contracts, patients use electronic tokens for the payment of online consultations or when purchasing medication.

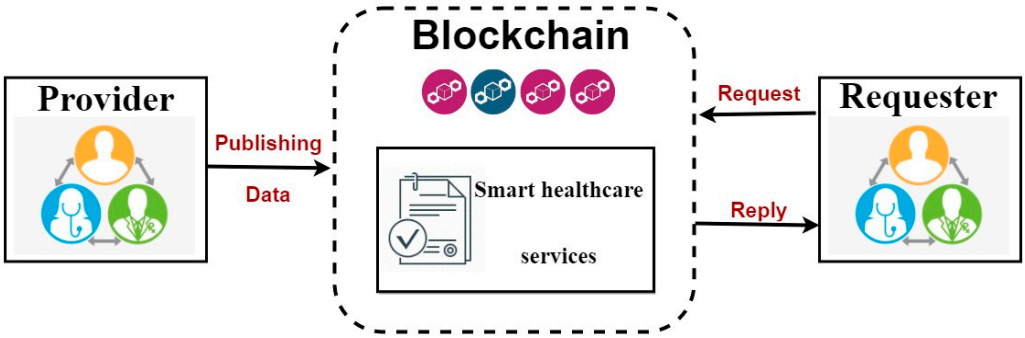

Figure 2. Smart healthcare services.

4.1. Proposed System Model

In the EMR system and as shown in Figure 3, several agents exchange information between them. They access a web application to provide or request health information. To access it, they must be authenticated. Depending on the type of user, the smart contract adds the automatic and secure aspect of this transfer. Data that are saved on the blockchain are then displayed on the appropriate interface. Therefore, we try to assign each user an access role thanks to the transparency and immutability of the blockchain to maintain the security of the patient's data against attacks.

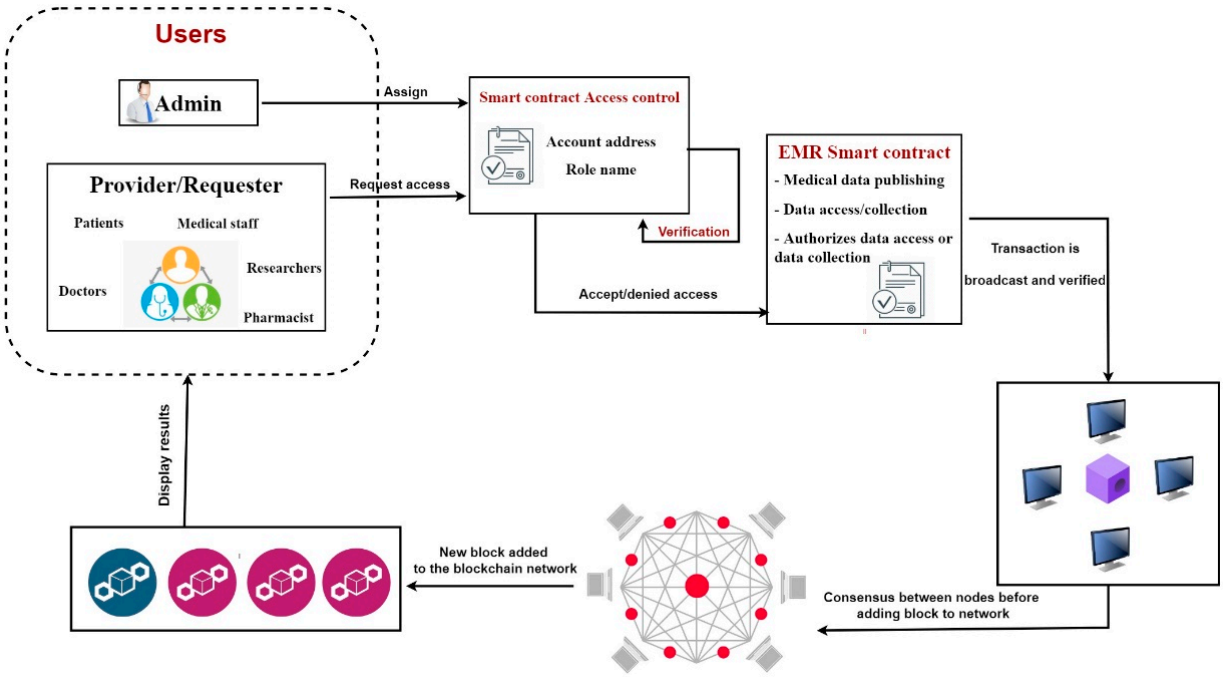

Figure 3. Smart healthcare services based on blockchain technology.

The architecture of the system is composed of two main parts: MAS allows communication between agents and a public blockchain network (BC) allows storing all transactions and smart contracts. The proposed model is based on three main concepts:

- ❖ Smart contract: Smart contracts are the most important component of any blockchain framework as they fulfill basic functions. For the design of our framework, the first step is the deployment of different smart contracts either for system stakeholder enrollment or for authentication to manipulate and check EMR.
- ❖ Authentication: Access to the system requires user authentication through Ethereum addresses for each agent. After authentication, the patient and healthcare specialist agent can consult and communicate with each other.
- ❖ Access control: Access control is a process that allows only authorized entities to manage information and control this information. In our case, to access and update the patient's medical data, the healthcare professional agent sends an access request via the smart contract that verifies the identity and rights of the requester and then authorizes him to send a request to the appropriate service.

4.2. System Model Process

The communication process between our system's agents is divided into four stages: Agent registration, Agent enrollment, Agent authentication, and EMR management. These steps are explained, respectively, in Figures 4–6.

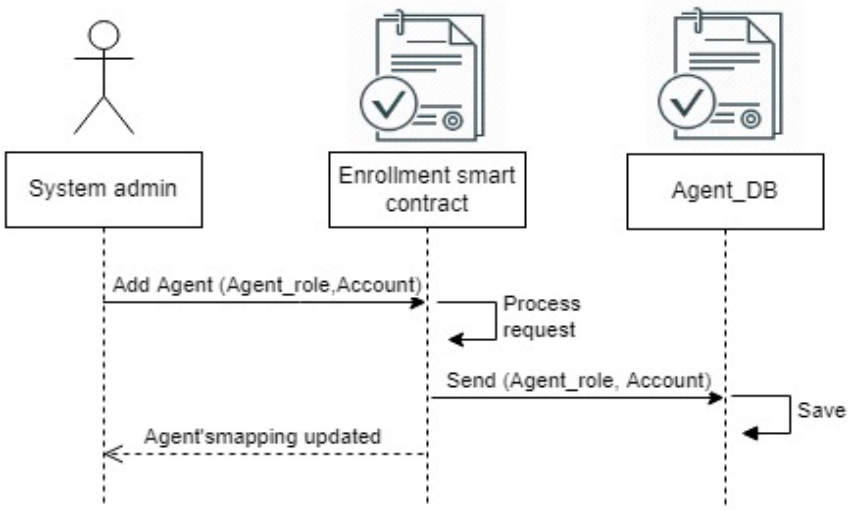

Figure 4. Agent registration.

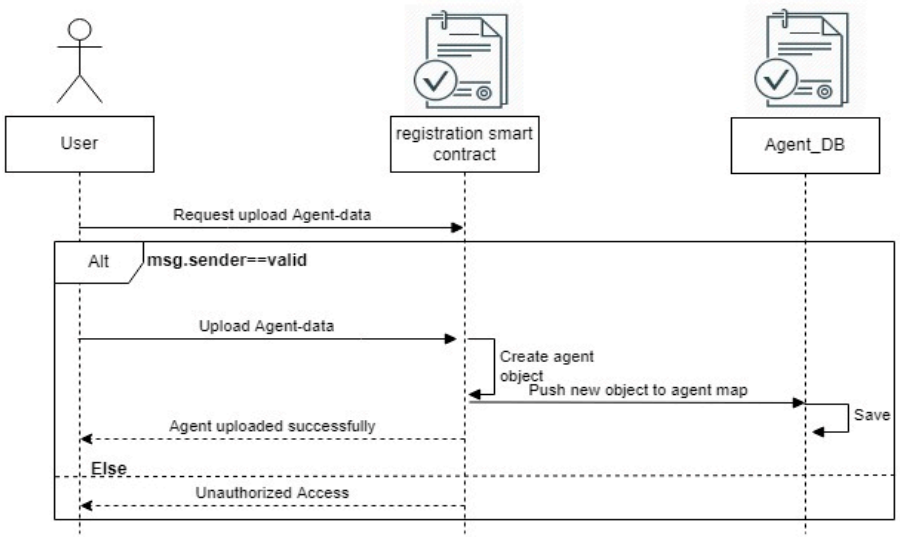

Figure 5. Agent enrollment.

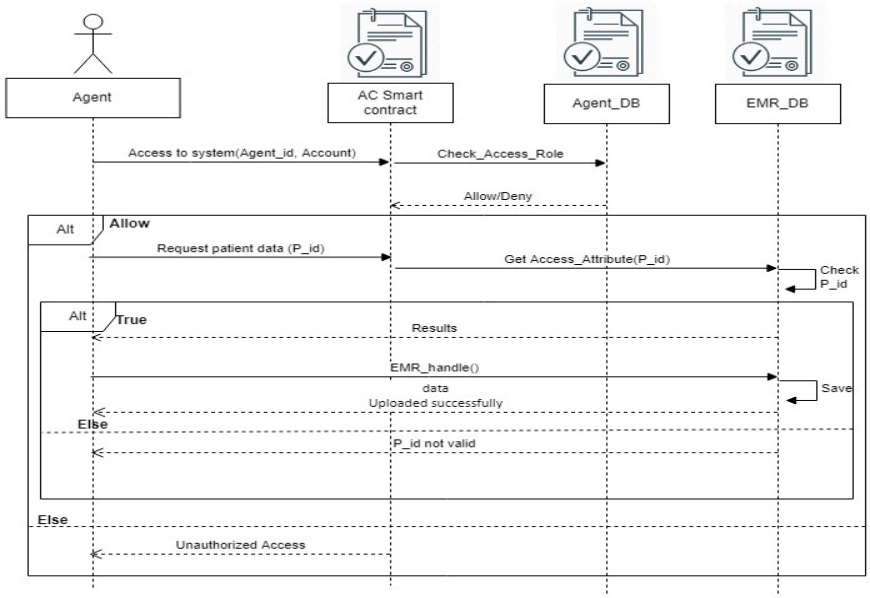

Figure 6. EMR management Based RBAC and ABAC.

- Agent registration: In this step, the system administrator assigns each agent an account and a role. This designation is recorded in a hash table via a smart contract. The added role is then used when adding an agent or in the handling of transactions in the communication process. However, the deployment of different smart contracts required by our system was the object of this step.
- Agent enrollment: The registration step consists of adding the agents to the system. After verifying the account address, the agent information can be added to the Agent_DB through a smart contract. In this phase, the smart contract saves the characteristics or attributes of each agent, especially the identifier and account. Upon successful registration, agents are allowed to join the blockchain.
- Agent authentication: To use our system, registered agents authenticate themselves. Two types of access control are used: Role-Based Access Control and Attribute-Based Access Control. The use of the "msg. sender" variable of the OpenZeppelin library allows for identifying and validating the agent's address. On the other hand, during EMR management, it is necessary to control access to patient data.
- EMR management: to access and update the patient's medical data, the healthcare professional agent sends an access request via the smart contract that verifies the identity and rights of the requester and then authorizes them to send a request to the appropriate service.

5. Simulation and Results

In this section, simulation results for cost consumption are discussed. Ethereum blockchain is used in this system; for that, the cost of smart contracts and their functions are calculated in terms of gas usage. Furthermore, the ether value is also checked for each gas unit. Further sections describe the simulation environment and the cost consumption of each smart contract and its functions.

5.1. Simulations Setting

To validate our system, all the simulations are performed on Intel Core i5, CPU 2.60 GHz with 8 GB RAM, running on Windows 10. Furthermore, we used the Ethereum blockchain. Indeed, Ethereum can manage the implementation of smart contracts written in solidity language. Each agent has an account in the Ethereum blockchain. To access this account, we use the web3.js library through an HTTP connection in JSON RPC format. The Truffle development environment is used to compile and migrate smart contracts to the blockchain.

Metamask is used to implement Ethereum wallet functions that allow participants to control the Ethereum account information and make transactions. Any changes sent to the transactions are recorded on the blockchain network.

5.2. EMR Smart Contract Deployment

We use a personal blockchain, Ganache, to implement our smart contracts. It enables the deployment of smart contracts, the development of Dapp, and the execution of tests. Ganache offers ten Ethereum accounts, each with a balance of 100 ether, as well as a graphical interface for examining everything that happens on this network.

Figures 7–10 depict the compilation and migration of smart contracts to the blockchain ganache. Four smart contracts are compiled and deployed in the "development" blockchain: EMR.sol, Registration.sol, Auth.sol and Migration.sol. The entire cost of this transaction, as shown by the migration result, is 0.01751596 ether, which is the equivalent of £ 58.61. This conversion was conducted on 28 March 2022. Following the transfer of our smart contract, we will build a local virtual server holding the client-side application using the truffle framework. To join our blockchain network, we need to connect to our Metamask portfolio.

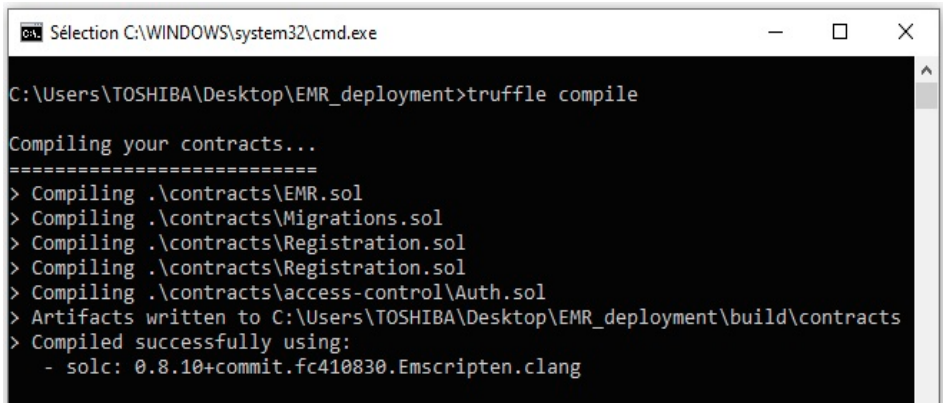

Figure 7. Compilation.

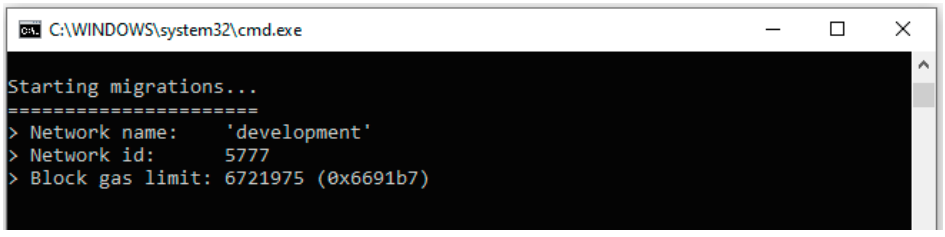

Figure 8. Migrate.

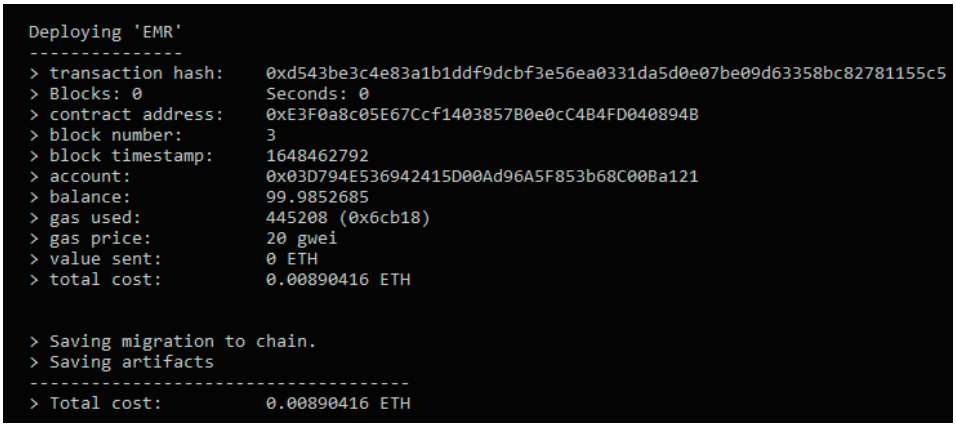

Figure 9. EMR smart contract deployment.

```
Deploying 'Registration'
------------------------
> transaction hash:    0x0446d4d7d7f2d41865d357482dd01e7c0709173787e8d3c872ba872e355acf00
> Blocks: 0            Seconds: 0
> contract address:    0x3394f3F43442442432D1095a9CA58cF635F1FD2e
> block number:        5
> block timestamp:     1648462798
> account:             0x03D794E536942415D00Ad96A5F853b68C00Ba121
> balance:             99.97610644
> gas used:            430590 (0x691fe)
> gas price:           20 gwei
> value sent:          0 ETH
> total cost:          0.0086118 ETH


> Saving migration to chain.
> Saving artifacts
-------------------------------------
> Total cost:          0.0086118 ETH
```

Figure 10. Registration smart contract deployment.

5.3. Cost Consumption

In the Ethereum blockchain, the proposed platform is evaluated through the cost consumed by the smart contracts. These are the units of gas to execute a transaction and smart contract functions. Otherwise, it is the transaction cost as well as the execution cost. The transaction cost is the fee for transferring the smart contract code to the Ethereum blockchain. It is limited by the thickness of the smart contract. The smart contract's size is determined by the basic operations it performs. While the execution cost is the cost of storing global variables and smart contract method calls. It is also affected by the calculation operations performed during transaction execution.

To calculate the gas fees for each transaction in our system, we apply the following equation:

$$\text{Transaction Fee} = \text{gasUsed} \times \text{gasPrice} \tag{1}$$

where gasUsed is defined depending on the storage and processing quantity for each transaction and gasPrice denotes the amount of gwei necessary for the transaction.

Let us take the example of the addUser function which allows assigning to each agent a role and account. As mentioned in Figure 11 the function gasUsed is 112,883 and gasPrice is 20 Gwei. So,

$$\text{Transaction Fee} = 112{,}883 \times 20 = 2{,}257{,}660 \text{ Gwei} = 0.00022 \text{ Ether} \tag{2}$$

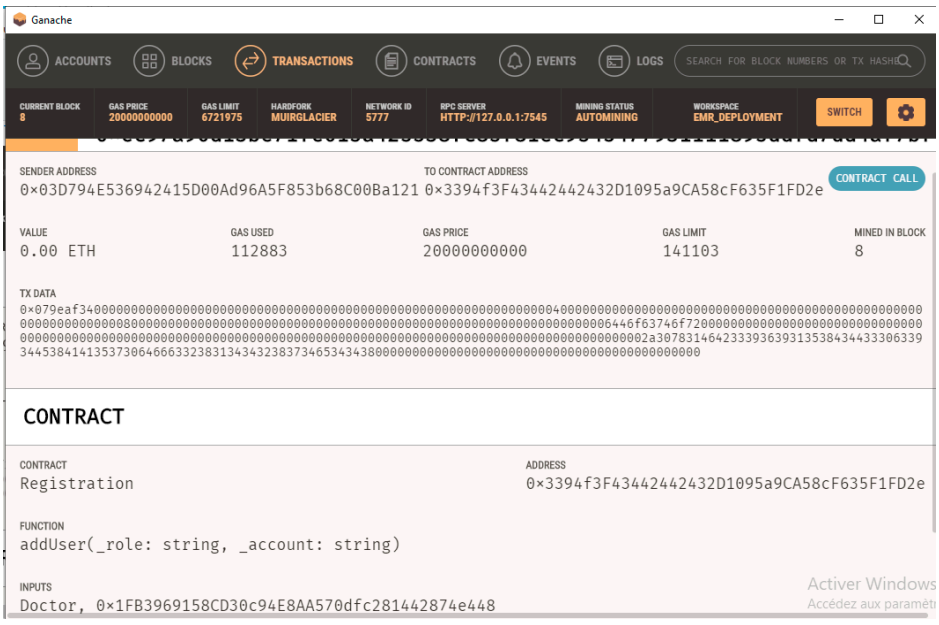

Figure 11. Registration smart contract deployed in Ganache.

5.4. Smart Contracts Cost

After deploying the smart contracts in our system and as shown in Figure 12, we calculated the cost of each smart contract. The results obtained are in Ether. The execution cost for the EMR management contract is 0.00890416 ETH while the cost for the registration contract is 0.0086118 ETH and for the agent enrollment contract is 0.008752 ETH. We notice that the cost of the EMR_management contract is higher than the other contracts. This contract contains the main functions of the system, such as adding patient analyses as well as the access control functions ABAC and RBAC. While the registration contract occupies less gas consumed since it just assigns a role to the agents in a table containing the accounts and roles. Agent_enrollment contract takes care of adding the relevant information to each agent.

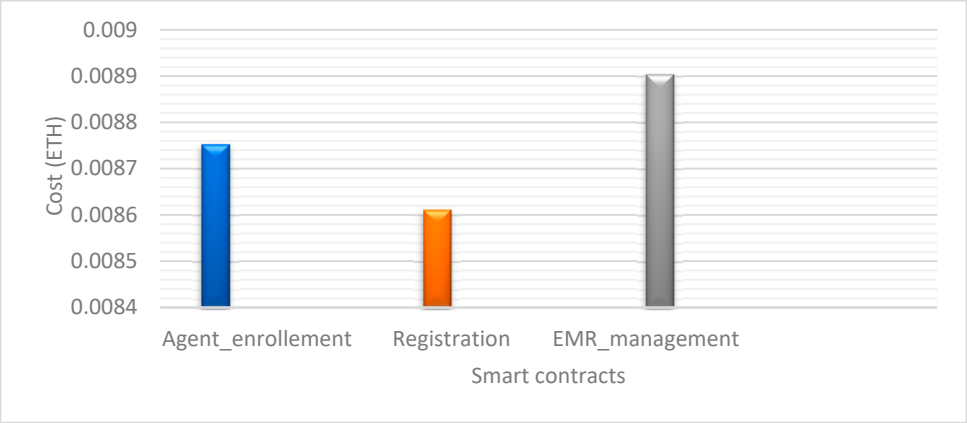

Figure 12. Smart contracts cost.

5.5. Functions Cost

We have calculated the transaction costs of different smart contract functions. Note, that the transaction cost for reading data from the blockchain, such as the "getPatientData", "getPrescription" and "getResults" functions, is null. Since mining is not required while getting messages from blocks, and no changes are required for the smart contract, this function does not incur any extra costs. The following Table 2 gives an overview of the cost of some transactions in our system.

Table 2. Gas price of some transactions of our proposed system.

Function	Transaction Cost	Price ($)
addUser	0.00022	0.74
uploadAgentData	0.00038	1.28
addEMRdata	0.00033	1.11

6. Comparison of Proposed System with Related Work

This section is dedicated to a comparison between this work and some studies previously summarized in Section 3. This comparison (Table 3) is based on some criteria deemed important such as blockchain-based, access control and security. In [34], K. Syeda et al. satisfied the Cr 1, Cr 2, and Cr 3 criteria while Srivastava et al. and Junchao et al. in [35,36] took into consideration the Cr 1 and Cr 4. Moreover, it is shown that in [38] authors took into account Cr 1, Cr 3 and Cr 4. Finally, according to this analysis, it is clear that only our work took into account all these comparison criteria.

Table 3. Comparison of proposed system with related work.

Criterium ID \ Reference	[34]	[35]	[36]	[38]	Our System
Cr 1	√	√	√	√	√
Cr 2	√	X	X	X	√
Cr 3	√	X	X	√	√
Cr 4	X	√	√	√	√
Cr 5	X	X	X	X	√

Cr 1: Blockchain-based; Cr 2: Access Control-based; Cr 3: Security; Cr 4: Integrity; Cr 5: Multi-agent system-based; X: Not supported; √: supported.

- Security: The use of the RBAC and ABAC mechanisms ensures the security of our proposed framework. So, no third party is allowed to access the system. Let us not forget also that blockchain is protected with mechanisms and protocols. Therefore, agent data can be handled reliably and confidentially. Only trustworthy persons have access to these data. The system denies access to any untrusted third party attempting to access the system.
- Confidentiality: EMR contains patient information such as electronic prescribing/delivery, laboratory results, medical imaging and related reports, and hospital discharge reports. To ensure the confidentiality of these data, unauthorized manipulation by third parties must be avoided. The use of smart contracts, by rejecting access to the system by any untrusted third party, ensures patient privacy, trust, and accuracy. The information saved in the system is immutable and cannot be modified by third parties thanks to the use of blockchain technology. This guarantees the confidentiality of the data handled.
- Trustfulness: Trust is maintained with access control via user registration as well as restricting access to the data of our system stakeholders. Furthermore, the information saved in the system is immutable and cannot be modified by third parties thanks to the use of blockchain technology. This guarantees the confidentiality of the data handled.

7. Conclusions

When COVID-19 appeared, it was necessary for doctors to turn to telemedicine to limit the transmission of the epidemic. However, this scenario promotes the risk of disclosure of patient data. Thus, blockchain technology is combined with multi-agent systems and access control in this study to solve this problem. The primary goals of this system are trust and security. To ensure that these features are implemented, various smart contacts are strategically placed. The proposed framework includes multiple access control smart contracts. These smart contracts go through three stages, validation of access request, policy check, and misconduct check. To evaluate the proposed system, smart contract costs and function costs are calculated. The entire cost of this transaction is 0.01751596 ether which is the equivalent of £ 58.61. The cost of each smart contract is, respectively, as follows: the execution cost for the EMR management contract is 0.00890416 ETH while the cost for the registration contract is 0.0086118 ETH and for the agent enrolment contract it is 0.008752 ETH. A deep analysis of related work was performed according to five categories of criteria. The first one concerns blockchain technology. The second category of criteria is relative to access control. The third and fourth criterium are, respectively, security and integrity. The last one represents a multi-agent system based. The results obtained show that the developed platform is characterized by security, availability, and privacy.

In future work, we will extend our system to design a platform consisting of three important parts. This platform contains a list of hospitals, EMRs and a network of connected ambulances. The three parts are linked together by a blockchain network. This extension allows the road user to find the nearest medical service and the nearest ambulance to their location in case of an accident.

Author Contributions: Conceptualization, methodology, writing—original draft, results analysis, H.M.; data collection, data analysis, writing—review and editing, results analysis, M.A.; methodology, writing—review and editing, design and presentation, references, A.K.; methodology, writing—review and editing, A.A.-R.; methodology, writing—review and editing, B.O.S.; methodology, writing—review and editing, S.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was financially supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R235), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used during the current study are available from the corresponding author on reasonable request.

Acknowledgments: This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R235), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

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

References

1. Goyal, S.; Sharma, N.; Bhushan, B.; Shankar, A.; Sagayam, M. IoT Enabled Technology in Secured Healthcare: Applications, Challenges and Future Directions. In *Cognitive Internet of Medical Things for Smart Healthcare. Studies in Systems, Decision and Control*; Hassanien, A.E., Khamparia, A., Gupta, D., Shankar, K., Slowik, A., Eds.; Springer: Cham, Switzerland, 2021; Volume 311. [CrossRef]
2. Mhamdi, H.; Soufiene, B.O.; Zouinkhi, A.; Ali, O.; Sakli, H. Trust-Based Smart Contract for Automated Agent to Agent Communication. *Comput. Intell. Neurosci.* **2022**, *2022*, 5136865. [CrossRef] [PubMed]
3. Ben Othman, S.; Almalki, F.A.; Chakraborty, C.; Sakli, H. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. *Comput. Electr. Eng.* **2022**, *101*, 108025. [CrossRef]
4. Bharadwaj, H.K.; Agarwal, A.; Chamola, V.; Lakkaniga, N.R.; Hassija, V.; Guizani, M.; Sikdar, B. A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications. *IEEE Access* **2021**, *9*, 38859–38890. [CrossRef]
5. Gope, P.; Millwood, O.; Sikdar, B. A Scalable Protocol Level Approach to Prevent Machine Learning Attacks on PUF-based Authentication Mechanisms for Internet-of-Medical-Things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 1971–1980. [CrossRef]
6. Ahmed, I.; Jeon, G.; Piccialli, F. A Deep-Learning-Based Smart Healthcare System for Patient's Discomfort Detection at the Edge of Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 10318–10326. [CrossRef]
7. Almalki, F.A.; Soufiene, B.O. EPPDA: An Efficient and Privacy-Preserving Data Aggregation Scheme with Authentication and Authorization for IoT-Based Healthcare Applications. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5594159. [CrossRef]
8. Almalki, F.A.; Ben Othman, S.; Almalki, F.A.; Sakli, H. EERP-DPM: Energy Efficient Routing Protocol Using Dual Prediction Model for Healthcare Using IoT. *J. Health Eng.* **2021**, *2021*, 9988038. [CrossRef]
9. Soufiene, B.O.; Bahattab, A.A.; Trad, A.; Youssef, H. PEERP: An Priority-Based Energy-Efficient Routing Protocol for Reliable Data Transmission in Healthcare using the IoT. *Procedia Comput. Sci.* **2020**, *175*, 373–378. [CrossRef]
10. Raoof, S.S.; Durai, M.A.S. A Comprehensive Review on Smart Health Care: Applications, Paradigms, and Challenges with Case Studies. *Contrast Media Mol. Imaging* **2022**, *2022*, 4822235. [CrossRef]
11. Wang, Y.; Nazir, S.; Shafiq, M. An Overview on Analyzing Deep Learning and Transfer Learning Approaches for Health Monitoring. *Comput. Math. Methods Med.* **2021**, *2021*, 5552743. [CrossRef]
12. FKraemer, F.A.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Fog Computing in Healthcare–A Review and Discussion. *IEEE Access* **2017**, *5*, 9206–9222. [CrossRef]
13. Awaisi, K.S.; Hussain, S.; Ahmed, M.; Khan, A.A.; Ahmed, G. Leveraging IoT and Fog Computing in Healthcare Systems. *IEEE Internet Things Mag.* **2020**, *3*, 52–56. [CrossRef]
14. Ijaz, M.; Li, G.; Lin, L.; Cheikhrouhou, O.; Hamam, H.; Noor, A. Integration and Applications of Fog Computing and Cloud Computing Based on the Internet of Things for Provision of Healthcare Services at Home. *Electronics* **2021**, *10*, 1077. [CrossRef]
15. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 25 August 2022).
16. Tasca, P.; Tessone, C.J. A Taxonomy of Blockchain Technologies: Principles of Identification and Classification. *Ledger* **2019**, *4*, 1–39. [CrossRef]
17. Kaur, M.; Khan, M.Z.; Gupta, S.; Noorwali, A.; Chakraborty, C.; Pani, S.K. MBCP: Performance Analysis of Large Scale Mainstream Blockchain Consensus Protocols. *IEEE Access* **2021**, *9*, 80931–80944. [CrossRef]

18. Mhamdi, H.; Zouinkhi, A.; Sakli, H. Multi-agents' system of vehicle services based on Blockchain. In Proceedings of the 2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Monastir, Tunisia, 20–22 December 2020; pp. 291–296. [CrossRef]
19. Mhamdi, H.; Zouinkhi, A.; Sakli, H. Smart contracts for decentralized vehicle services. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Harbin, China, 28 June–2 July 2021; pp. 1846–1851. [CrossRef]
20. Bhattacharjya, A.; Wisniewski, R.; Nidumolu, V. A holistic research on major Blockchain's Consensus Protocols' working mechanisms with security aspects of CPS. *Electronics* **2022**, *11*, 2760. [CrossRef]
21. Bhattacharjya, A. A holistic study on use of Blockchain technology in CPS and IoT architectures with focus on maintaining CIA triad of data communication. *Int. J. Appl. Math. Comput. Sci.* **2022**, *32*, 403–413.
22. Cho, C.; Seong, Y.; Won, Y. Mandatory Access Control Method for Windows Embedded OS Security. *Electronics* **2021**, *10*, 2478. [CrossRef]
23. Recommendation on a European Electronic Health Record Exchange Format. Available online: https://digital-strategy.ec.europa.eu/fr/node/2138 (accessed on 31 July 2022).
24. Nishi, F.K.; Shams-E-Mofiz, M.; Khan, M.M.; Alsufyani, A.; Bourouis, S.; Gupta, P.; Saini, D.K. Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. *J. Sensors* **2022**, *2022*, 7299185. [CrossRef]
25. Mhamdi, H.; Othman, S.B.; Zouinkhi, A.; Sakli, H. Blockchain Technology in Healthcare: Use Cases Study. In *Intelligent Healthcare*; Chakraborty, C., Khosravi, M.R., Eds.; Springer: Singapore, 2022. [CrossRef]
26. Mhamdi, H.; Othman, S.B.; Zouinkhi, A.; Almalki, F.A.; Sakli, H. Blockchain Technology in Healthcare: A Systematic Review. In *Blockchain Technology in Healthcare Applications: Social, Economic, and Technological Implications*, 1st ed.; Bhushan, B., Rakesh, N., Farhaoui, Y., Astya, P.N., Unhelkar, B., Eds.; CRC Press: Boca Raton, FL, USA, 2022. [CrossRef]
27. Kazmi HS, Z.; Nazeer, F.; Mubarak, S.; Hameed, S.; Basharat, A.; Javaid, N. *Trusted Remote Patient Monitoring Using Blockchain-Based Smart Contracts*; BWCCA 2019, LNNS 97; Springer Nature Switzerland AG 2020L: Berlin/Heidelberg, Germany, 2020; pp. 765–776.
28. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient Healthcare Data Sharing via Blockchain. *Appl. Sci.* **2019**, *9*, 1207. [CrossRef]
29. Casado-Vara, R.; Briones, A.G.; Prieto, J.; Rodríguez, J.C. Smart Contract for Monitoring and Control of Logistics Activities: Pharmaceutical Utilities Case Study. In *Chapter in Advances in Intelligent Systems and Computing*; Springer: Cham, Switzerland, 2019.
30. Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2020**, *8*, 5914–5925. [CrossRef]
31. Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 310–317. [CrossRef]
32. Raj, R.; Rai, N.; Agarwal, S. Anticounterfeiting in pharmaceutical supply chainby establishing proof of ownership. In Proceedings of the TENCON 2019–2019 IEEE Region 10 Conference (TENCON), Kochi, India, 17–20 October 2019; pp. 1572–1577.
33. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef] [PubMed]
34. Ahmad, R.S.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Ellahham, S.; Omar, M. The role of blockchain technology in telehealth and telemedicine. *Int. J. Med. Inform.* **2021**, *148*, 104399. [CrossRef] [PubMed]
35. Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. Data Sharing and Privacy for Patient IoT Devices Using Blockchain. In *Smart City and Informatization. iSCI 2019. Communications in Computer and Information Science*; Wang, G., El Saddik, A., Lai, X., Martinez Perez, G., Choo, K.K., Eds.; Springer: Singapore, 2019; Volume 1122. [CrossRef]
36. Wang, J.; Han, K.; Alexandridis, A.; Chen, Z.; Zilic, Z.; Pang, Y.; Jeon, G.; Piccialli, F. A blockchain-based eHealthcare system interoperating with WBANs. *Futur. Gener. Comput. Syst.* **2019**, *110*, 675–685. [CrossRef]
37. Zhuang, Y.; Sheets, L.R.; Shae, Z.; Chen, Y.W.; Tsai, J.J.P.; Shyu, C.R. Applying Blockchain Technology to Enhance Clinical Trial Recruitment. *AMIA Annu Symp Proc.* **2020**, *2019*, 1276–1285.
38. Zhuang, Y.; Sheets, L.; Shae, Z.; Tsai, J.J.P.; Shyu, C.-R. Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials. *AMIA Annu. Symp. Proc. AMIA Symp.* **2018**, *2018*, 1167–1175.
39. Bhattacharjya, A.; Kozdrój, K.; Bazydło, G.; Wisniewski, R. Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. *Electronics* **2022**, *11*, 2560. [CrossRef]