Sana'a University Journal of Applied Sciences and Technology ISSN : 2958-9568
Vol. 1 | No. 2 | Page 131 – 146 | 2023 | https://journals.su.edu.ye/index.php/

A Hybrid Model for Using Cloud Computing and Blockchain Technologies to Protect Hospital Records

Ebtisam Ali Abdullah [1,*], Anwar Al-Shamiri[2] and Abdualmajed Ahmed Al-Khulaidi[3]
[1]Information Technology Department, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.
[2]Information Systems Department, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.
[3]Software Engineering, Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen.
***Corresponding author**: Ibt.alselwi@su.edu.ye

Article Info.
Article history:
Received: February 6, 2023
Accepted: March 30, 2023
Published: April 30 2023

Keywords
1. Cloud Computing
2. Blockchain
3. Healthcare
4. Electronic health record
5. Technological context
6. Organizational context

ABSTRACT: Cloud computing technology is one of the hottest trends in information technology (IT) today. It is an important alternative to ensure high data processing and exchange. Thus, this technology can be used in the health sector to exchange patient medical records and health-related information. However, there are fears of the leakage of confidential patient data. This research studied two main contexts, the technological and organizational contexts, to find out the concerns about the use of cloud computing technology in the health sector. The results indicated the desire of hospitals to use cloud computing because of its enormous benefits in the health sector, with concern about data security with cloud computing. For this reason, this paper propose a model for protecting and storing the patient's medical record using two technologies: cloud computing and blockchain. The model guarantees confidentiality, high protection, and privacy of patient information, and provides all beneficiaries of cloud computing with all the needed information when wanted.

Contents

1. Introduction

With the continual progression of technology and the information created by medical foundations, medical information has gone from the first paper medical records (PMRs) to the present electronic medical records (EMRs) [1]. There is no doubt that EMRs are easier to share, store, recover, and follow through eHealth systems, which can be generally partitioned into three classifications: traditional, cloud-based, and blockchain-based eHealth systems. Even though electronic records carry enormous comfort and advantages for medical services, the security of eHealth systems and the privacy protection of patients have forever been the common worry of the medical industry and academia [2] [3]. In traditional eHealth systems, EMRs are commonly stored separately in various medical foundations (e.g., clinics, hospitals, and health centers) that have their own databases. This is advantageous to the operation performance and data security of the whole medical foundation, yet it does not help share and connect other medical foundations. The fundamental reasons can be summed up as follows. First, the hardware and software of various medical foundations are inconsistent, resulting in incompatibility with each other. Second, access to data from other medical foundations requires previous authorization, which will without a doubt raise the time and cost. Third, the standards of EMRs are conflicting, and the required data may not be sound. For sure, the medical data is owned by each medical foundation. With the advancement of cloud computing and the extended utilization of cloud services, cloud-based eHealth systems arise as the times require. Not quite the same as the traditional way, EMRs are transferred to a cloud server, on which patients and medical foundations can get information through different intelligent terminals. This is a good solution for the information sharing and interaction issues of traditional eHealth systems, which further advance the improvement of medical service quality. Moreover, some work about access control [4], encryption [5], and authentication [6] has been considered to improve the security of cloud services and protect information privacy. Due to the server-centric structure and data managed by medical foundations' cloud service providers, cloud-based eHealth systems always have problems with a single point of failure and the inability to resist collusion attacks. From the above, it can be seen that EMRs in traditional or cloud-based eHealth systems are constrained by medical foundations, which are frequently lacking to safeguard the rights and interests of patients. This issue is put forward in work [7], which confirms the need for and significance of patients owning their medical data. Due to the transparency and openness of decentralization and non-tampering, blockchain technology and its applications have attracted high concern from companies, government departments, and scholars around the world in recent years [8]. In the meantime, blockchain-based eHealth systems are being investigated to resolve the issues in prior eHealth systems [9] [10] [11]. To our best knowledge, some of the existing work is patient-centric, and the utilization of data by medical foundations requires previous consent from patients. Although this protects the interests and rights of patients, it will seriously limit the practicality of eHealth systems.

To realize a better balance between patients and the medical foundations, the paper [12] proposed a blockchain-based access control scheme, in which patients are supervisors who permit the medical foundations to legally utilize their medical data without previous authorization but have the right to manage the medical data. Despite patients' ability to prohibit others from utilizing their medical data in the future, the proposed scheme guarantees the interests and rights of patients without influencing the normal diagnosis and research work of the medical foundations. In addition, an incentive mechanism is considered to encourage patients to share their medical data effectively.

Finally, a case study on Ethereum was performed to prove the feasibility and practicality of the proposed method [12].

1.1Cloud Computing

Cloud computing is a paradigm for enabling all-over-the-place, convenient, on-demand

network access to a shared gathering of configurable computing resources (e.g., storage, servers, network services, and applications) that can be quickly provisioned and appear with less management effort or service provider interaction [13].

1.1.1 Types of Cloud Computing

There are four deployment models for cloud computing.

A. Public Cloud

It is also named the external cloud [14] because this kind of cloud is widely open and runs on the Internet, and then it can be accessed and resources can be saved by any client paying for the service. The major concern in this kind of cloud is data privacy and, because the infrastructure services for this kind of cloud can be accessed by the public and be multi-tenant, the infrastructure is owned by the institution that provides the cloud service [15] and is therefore managed and operated by cloud service providers.

B. Private Cloud

It is also named the internal cloud because it is marked in the scope of an entirely owned inner network by one institution [14], so the client manages and owns it and therefore has restricted access to clients who own the cloud and their partners.

This kind of cloud is the most secure way to use cloud computing, but it is expensive because its services are hosted in private data centers, IT infrastructure services, and individual leased environments.

C. Community Cloud

Cloud infrastructure is shared with a network of organizations, with infrastructure management by a third-party cloud service provider or institutions [16]. The aim of this cloud is to support the common tasks and goals of a specific community, and this kind of cloud is designed to meet the needs of the community. These communities have common concerns and are either jointly or individually rented.

D. Hybrid Cloud

The hybrid cloud was created from private and public clouds, providing access to clients, third-party networks, and partners [17], which are implemented by huge institutions that use cloud computing in multiple initiatives. These institutions also manage a few resources within their data centers that are provided externally, such as Microsoft HealthVault [18].

1.2 Blockchain Technology

As of late, research connected with blockchain and smart ledgers has gained popularity due to the emergence of cryptocurrencies like Bitcoin and Ethereum. Blockchain shares and stores data in a distributed, trusted, and unchanging way, eliminating intermediaries and the need for a centralized dependency for checking transactions [19] [20]. Transparency in blockchain provides a less sophisticated way for accessing ledger-based transactions across networks; it connects with various computing powers from multiplied nodes in the blockchain network, making it extremely strong concerning calculation speed [21]. The blockchain has different services and techniques, including Hash Cryptography, Consensus Protocol, Distributed P2P Networking, Immutable Ledger, and mining, which are currently presented in more detail:

•Consensus protocol: In a blockchain network, specific users have individual access rights to grant transactions that are updated in the system, known as consensus protocol;

• Hash cryptography: A blockchain utilizes the SHA256 hash for adding transactions. This was created by the NSA and is 64 characters in length. Hash algorithms incorporate features, like one-way cryptography, faster computation, determinism, and the avalanche effect, and must withstand collisions;

• Immutable ledger: All transactions in a blockchain network are recorded, while the shared ledger cannot be changed or tampered with;

• Distributed P2P network: All transactions are broadcast over the network to various users to update and distribute the data [22];
• Mining: Miners use blocks of nonce values to accomplish hash values in the network. This requires high computation speed to accomplish and acquire the reward.

It has the potential to duplicate a blockchain network at another site, e.g., inside the same healthcare delivery network or facility, or as part of a national or international data-sharing program. This ability makes it possible to share medical data with partner facilities and other interested parties, e.g., insurance providers or researchers. Blockchain is connected inside a network that shares information and guarantees that the information inside the network is reliable, accurate, and consistent. Thus, we can add information to a blockchain at one site and distribute it to one or more sites inside the same network. The new sites share the information inside the network, finally distributing the new information to the whole network and permitting site access to the most recent information.

1.2.1. Advantages of Blockchain Technology

Blockchain technology utilizes a distributed network, including information in tamper-resistant forms. Blockchain transactions are added or updated just through the making of new hash values; thus, current transactions cannot be modulated. To comprehend this, the possible utilization of blockchain technology should be described versus all the features that make the blockchain unique from others:

• Distributed ledger: Transactions are appended to a distributed system on the network, which creates system recovery by eliminating a single point of failure or centralized entity;
• Consensus mechanism: Transactions are only updated when all verified users in the network agree to the condition of the transaction;
• Provenance: The complete data or asset's history is available on the blockchain network;
• Immutability: Records on the network cannot be modified or tampered with; thus, all information is secure and trusted;
• Finality: When a transaction is committed on a blockchain, it cannot be modified or reversed; and
• Smart contract: The codes are created on a blockchain network, and the computer and nodes execute a triggered event. Hence, the codes are auto-executed within the time frame.

To this end, blockchain has the potential to reduce transparency and security issues, such as the trust of third parties at any stage of a transaction; this means that all intermediaries or third parties are eliminated with the advent of blockchain technology [9].

1.2.2 Types of Blockchain

A. Public Blockchain

This is a kind of blockchain that is available to all. Any user can associate with the public blockchain, and no authorization is required to join the network. On this type of blockchain, any client who connects to the network has access to read the transactions made onto the blockchain Any utilization connected with this blockchain has permission to make any legitimate variation to the blockchain or, on the other hand, if needed, to add any new transaction or block into the current chain of blocks. The greatest benefit of the public blockchain comes from the fact that it can contain any unknown client in the network. A public blockchain can be extremely useful in creating cryptocurrencies. The Ethereum and Bitcoin networks are the best models for a public blockchain. The disadvantages of the public blockchain are the scalability issues of the network and the transaction charge incurred for joining the blockchain network [1] **(see Figure 1).**

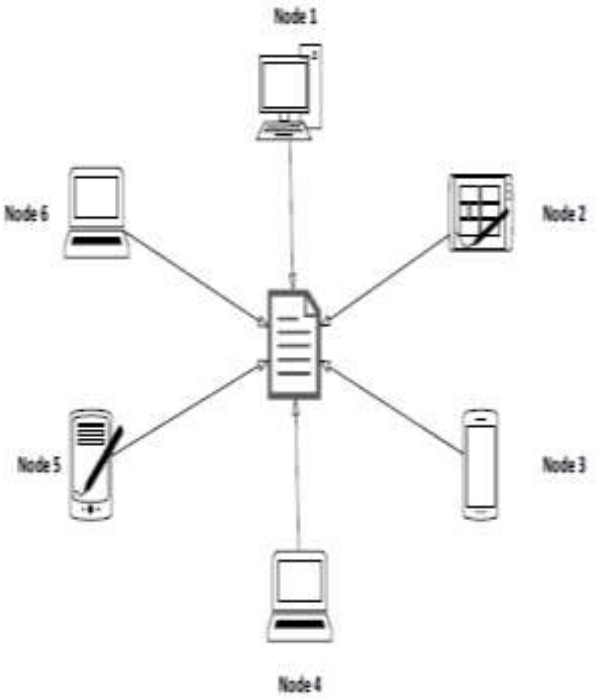

Figure 1: Public Blockchain Network [1]

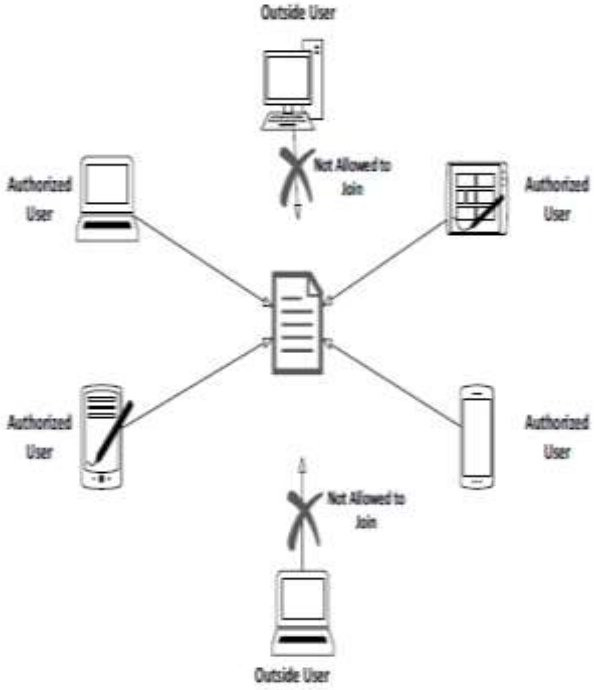

Figure 2: Private Blockchain Network [1]

B. Private Blockchain

In contrast to a public blockchain, on a private blockchain, any user who wants to join the network needs permission to be added. A private blockchain can be created by any organization **that wishes** to add only trusted users **to** the network, and no unauthorized **users** are permitted to join the network. In this type of blockchain, some finite clients **join** the network, and only authorized clients have access **to** the network. Differently from a public blockchain, the individual who makes the private blockchain network will be the administrator or validator of the network, who has the authority to add trusted clients to the network. The administrator or validator has access to the transactions of the network and can place rules on the network. Ripple and Hyperledger are the models for private blockchains [1] **(see Figure 2).**

C. Consortium Blockchain

A consortium blockchain is a hybridization of both private and public blockchains. A consortium blockchain permits users to enter the network without permission, such as on a public blockchain. However, when the users join the network, the ownership of the network does not become in the hands of an individual owner or a group, like in a private blockchain, where a few users out of every user can be assigned the task of administrators or validators who can validate the transactions proceeded by the users of the network and also hold the authoritative rules of the network [1]. The models of a consortium blockchain are Hyperledger Fabric [22], Corda, and Quorum [23].

2. Related Work

The previous studies were concerned with studying the factors that affect the use of cloud computing in hospitals to find out the barriers to using this technology.

Other studies relate to a way to solve the issue of concern about using cloud computing by using algorithms to protect the medical record, as well as using blockchain technology along with cloud computing to ensure stronger performance and high protection.

Various studies reveal different factors that influence the decision to use certain techniques. The researchers chose different methods to examine the factors that enable organizations to decide whether to use cloud computing.

Researchers in [14] studied the critical factors affecting the decision to adopt cloud computing in Taiwan hospitals. The results indicated that the top five factors were data security, perceived technical efficiency, cost, senior management support, and complexity. However, the study was not generalized to developing countries, and issues of technological readiness were not discussed.

The purpose of the research in [18] was to investigate the factors and barriers expected to affect the adoption of cloud computing in Indian hospitals. However, the study did not take into account some important factors such as availability, reliability, financial analysis, the strategic value of the cloud, and the decision maker.

In the research [19], the factors affecting the adoption of cloud computing in hospitals in Brazil were also analyzed. Results show that availability, security, and flexibility are factors of high importance.

In the other study, the researchers proposed [24] a data categorization approach founded on data confidentiality. The K-NN data categorization technology has been altered in the virtual cloud environment. The reason for utilizing K-NN was to categorize data based on its security needs. They categorized the data into two classes: non-sensitive and sensitive data. After categorizing the data, they determine what data does not need security and what data does require security. They utilized the RSA algorithm to encrypt sensitive data to remain secure. The results of their work showed that this approach is convenient when contrasted with storing data in the cloud with no comprehension of the security requirements of the data. In the research, they categorized the data generally, and the study was not specific to the data related to the health record of the patient. They utilized one algorithm, saved and encrypted the data without doing decryption, did not apply a hybrid technique, and did not ensure the privacy of sensitive data or prevent unauthorized people from accessing this data. This differs from our hybrid approach, which will provide double encryption by merging two algorithms for better and stronger security performance, and which will provide better encryption by using blockchain technology. It also differs in terms of the privacy of the patient's medical record, as in our hybrid approach, the record cannot be accessed except after obtaining permission from the patient.

In another study [25], the researcher designed a hybrid approach for encrypting the data on the cloud. The researchers designed a hybrid approach for encrypting the data in the cloud. They used the RSA algorithm to encrypt the private key and the AES algorithm to encrypt the data. Encryption and decryption of the key and the data were done utilizing two different techniques. In any case, the issue is that the hybrid technique is not fully utilized to protect the data. In addition, its performance is not as good as the method proposed by us because they have used one algorithm for data encryption and another one to encrypt the key, not the data. We will encrypt the data using algorithms (AES, RSA) and provide better security using blockchain technology.

The researchers in [26] proposed a hybrid layered approach to protecting user data along with the association of lattice-based security techniques. In their proposed model, a new

approach to checking roles and responsibilities is incorporated using a lattice model.
In the research, the content requestor can get the record based on the access control policy. The storage and retrieval of documents are additionally protected using the two-layer approach for encryption and decryption (RSA and AES). The hybrid approach prevents unauthorized disclosure. Lattice-based access control provides a classification of access policies based on the owner of the document and different roles in the hospital for those who are eligible to access the document. In this way, the security controls for each classification are also achieved. This research was not expanded as they used unstructured electronic health care (CHR) records that took longer encryption time, and they also did not use the communication cost scale to reduce the time of sending and receiving medical records to improve health care services. This differs from our hybrid approach consisting of both algorithms (RSA and AES), but we will use a structured electronic health record (EHR) that reduces encryption time, in addition to using blockchain technology to ensure stronger protection and better performance.
The researchers in [27] introduced a secure protocol for sharing medical data between hospitals, patients, and medical data consumers. They used attribute-based encryption methods with blockchain technology. The researchers applied two types of attribute-based encryption: KP-ABE and CP-ABE, to fine-grain access control of patients' private medical data and used blockchain technology to transmit medical data in real-time, increasing network efficiency more effectively. To revoke access in attribute-based encryption, medical data in MedSBA is encrypted by the AES algorithm and its encryption key by the ABE algorithm based on preferred features. Moreover, the data was stored on cloud storage systems.

As a result of comparing their scheme with previous work, their proposed scheme demonstrated appropriate security for sharing medical data using the BAN logic. They also investigated the security of the KP-ABE and CP-ABE cryptography methods used in their proposed scheme.
In summary, few existing studies employing AES and RSA algorithms provide better performance in terms of security. In some of the studies, one algorithm is used to encrypt and another one is used to decrypt, which leads to implementation overhead.

In this research, we will first conduct a study on the critical factors regarding the use of cloud computing in hospitals and take into account two contexts: the technological context and the organizational context. The technological context includes two important factors: availability and reliability. The organizational context includes two factors: technological readiness and perceived barriers that include the factor of protection and privacy of confidential patient data. This research proposes a model to solve the problem of concerns about the use of cloud computing in hospitals. The research model will provide more security for medical records on the cloud using a hybrid approach and also control access to the patient's medical record after taking strict permission from the patient to protect the privacy and confidentiality of patient data. This powerful protection will let the patient store their private files in the cloud without worrying about data leaking into the wrong hands or security threats.
No one can guess the key or the ciphertext due to the hybrid approach, which includes two algorithms: AES and RSA. Thus, access to confidential data by unauthorized persons will be impossible. The model will save the cost of communication (the time from requesting the

medical record to receiving the record), which will improve the quality of medical services provided during the emergency period.

3. Problem Statement

Cloud storage plays an important role in the medical information system. By storing EHR data in the cloud, and when users store EHR data in the cloud, the data will suffer a variety of security threats, including data privacy, data integrity, and data authentication. It can be seen that electronic medical records in traditional or cloud-based electronic health systems are under the control of medical institutions, and often inadequate protection of privacy and secure storage of medical data are critical issues in medical services. Safe storage and full utilization of personal medical records have long been a matter of concern to the general population. The emergence of blockchain technology brings a new idea to solve this problem.

However, the blockchain has its limitations, such as low storage capacity and high processing time and cost, so the blockchain can be used for protection and cloud computing for storage.

This research built a cloud computing model that provides high security of the patient's health record using blockchain technology and ensures high privacy of confidential patient data by preventing access to the record only after obtaining permission from the patient at a lower cost and lower execution time.

4. Objectives

1. Studying the factors that help the use of cloud computing in hospitals.
2. The main purpose of this research is to introduce and implement a cloud-based model that allows for:

- Security of a patient's medical record using blockchain technology before this record is shared between medical units.
- Provides high privacy for confidential patient data.

5. Contribution

After the implementation of this model, you will achieve:

1. Security of a patient's medical record before this record is shared between medical units. This robust protection will allow patients to store their private files in the cloud without worrying about data leaking into the wrong hands or security threats.
2. Provides high privacy for confidential patient data by not allowing access, addition, or sharing of a patient's medical record except after obtaining permission from the patient.
3. Safe medical data management to promote rapid access to emergency medical records.
4. Obtaining the patient's medical record within a short period and at a lower cost of communication leads to improving the quality of medical services provided during the emergency period and saving patients' lives.

6. Research Work

This research studied two main contexts, i.e., the technological and organizational contexts, to find out the concerns about the use of cloud computing technology in the health sector. In addition, this research proposed a model for protecting and storing the patient's medical record using two technologies: cloud computing and blockchain. The model guarantees confidentiality, high protection, and privacy of patient information.

6.1. Technological and Organizational Contexts

A. Technological Context (TC)

This context indicates the external and internal technologies used in the institutions. Internal technology refers to the technologies already utilized to improve the productivity of institutions. External technology indicates that

it is available on the market but has not been utilized by institutions yet [17]. This context indicates the following factors:

- **Availability**: Health services in cloud computing have to be available continuously, uninterrupted, or minimized in performance.
- **Reliability**: Data and health services must be consistent, error-free, and in a valid state, regardless of any hardware, software, or network failure.

B. Organizational Context (OC)

This context indicates the characteristics and resources of the institutions [17]. It indicates:

-Technological Readiness: indicates the readiness of infrastructure, human resources, and information technology that impact the use of new technology [20].
-Perceived Barriers: refer to the barriers that influence the use of cloud computing technology, such as privacy and security [19].

6.2. The Proposed Model

6.2.1. Description of the Proposed Model

The proposed model for implementing cloud computing in hospitals provides security for confidential patient data through the use of blockchain technology, which ensures strong security of the patient's medical record at a lower connection cost.
The patient data (the patient's medical record) is transferred using medical data collection devices. Then, the collected data is transferred to the blockchain technology located within the cloud computing system of the hospital attended by the patient. The blockchain records, updates, and analyzes the medical record information with the creation of an index for each health record, then encrypts the patient's health record using encryption algorithms (AES and RSA). Due to the problem of limited storage on the blockchain, the blockchain maintains an index of the patient's health record information, while the encrypted information of the patient's medical record is saved in the private cloud computing of the hospital attended by the patient.
Patients can allow their data to be shared, added, or downloaded to a center or hospital using the index on the blockchain.
The proposed model consists of a simple and inexpensive public cloud with large storage capacity as needed. This cloud needs little management, as medical record information for hospitals that do not have private clouds is stored and managed in this cloud. In addition, the patient's health records are stored in medical departments that are not found in any hospital.

In the proposed heterogeneous model, the public cloud is linked to several private blockchains owned by private hospitals, medical care centers, and public hospitals that are linked to each other in a decentralized manner. In the hospital blockchain attended by the patient, confidential patient data is processed, updated, and encrypted. Backup copies are made to prevent this data from being lost and sent to the public cloud for storage. The patient's data is only processed after obtaining permission from the patient to give the authorized persons in the hospital access to and control of his medical data. The hospital or medical center sends a request to other hospitals to search for the patient's medical record using a special index of this record to reduce the cost of communication and searching to share the record after getting the patient's permission. If there is an update to the data on the private blockchain, a new block is created and stored in the cloud at the Ministry of Health (see Figure 3).

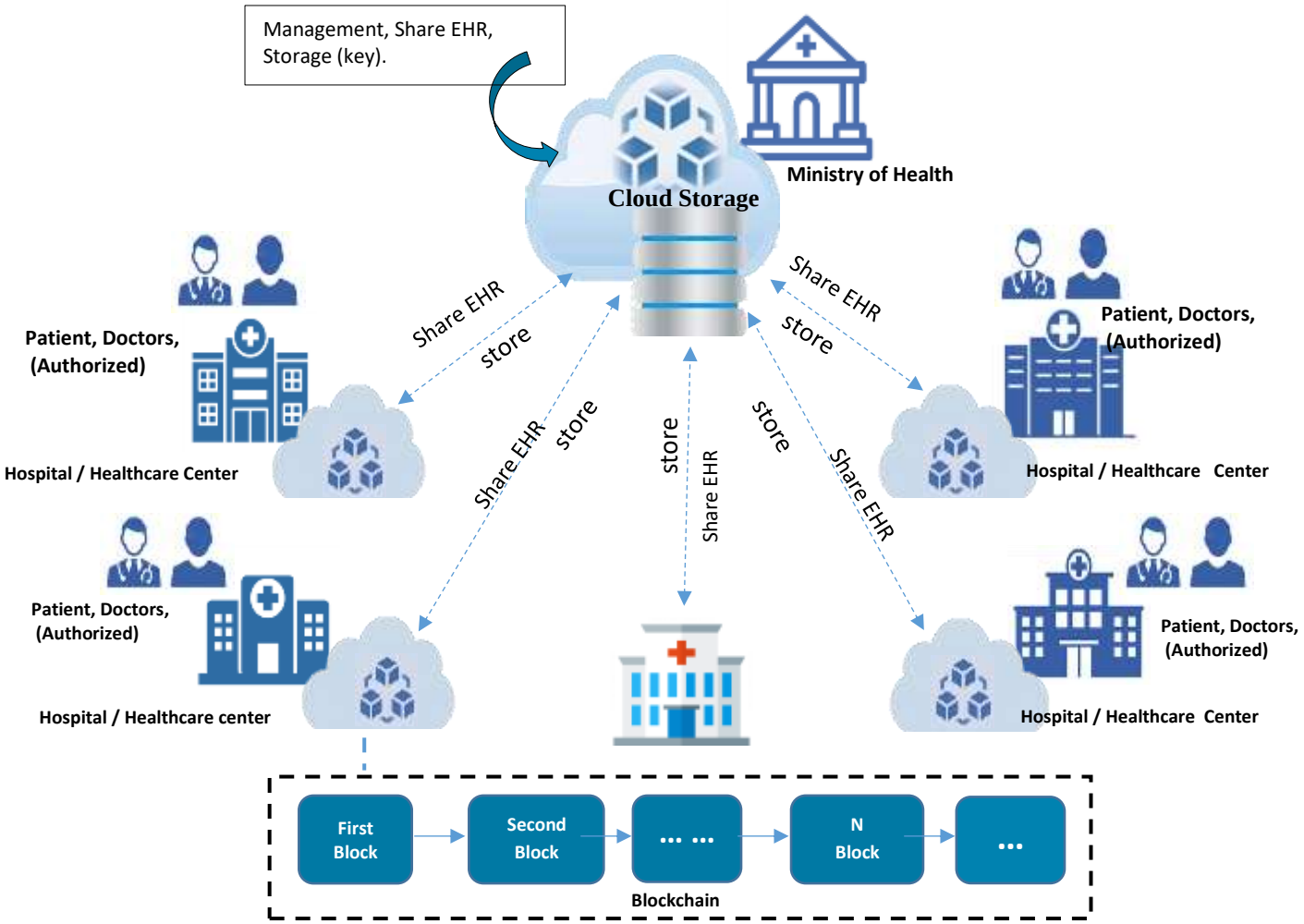

Figure 3: The Proposed Model

7. Methodology

This research was conducted in private hospitals in the Republic of Yemen. The target environment was 32 hospitals in the Capital Secretariat, Sana'a, in addition to the Ministry of Public Health.

Data collection was conducted. 364 surveys were hand-delivered. The purposive sample of the study consisted of IT and administrative staff and health professionals (doctors, pharmacists, nurses, and lab physicians) from 32 private hospitals. In addition, the questionnaires were distributed to the administrative staff from the Information Technology Department at the Ministry of Public Health (see the questionnaires in the Appendix**)**.

The reason for choosing private hospitals was because they are more cooperative and responsive to the researcher.

To find out the factors that cause fears of leaking confidential patient data. These factors were as follows: availability, reliability, perceived barriers, and technological readiness.

7.1 Methods of Statistical Analysis

The data are processed statistically using the Social Statistical Package (SPSS) software.

Each of the following statistical metrics is calculated:

1) Frequency and percentage are used to describe the demographic characteristics of respondents in the following aspects: gender, age, education, years of experience, and position.

2) Calculation of the mean and the standard deviation to determine the respondents to the different variables of the study.
3) Correlation analysis is an indication of the nature of the relationship between two variables.

8. Results

• Demographic Data Analysis

The following section presents the demographic characteristics of the respondents according to gender, age, education, position, and years of experience.

Table 1. Frequency Distribution – Demographic of Respondents

	Items	Frequency	Percent
Gender	Male	161	67.4%
	Female	78	32.6%
	25 years or less	75	31.4%
Age	26 - 35 years	110	46.0%
	36 years or more	54	22.6%
Education	Diploma	35	14.6%
	Bachelor	139	58.2%
	Higher Education	65	27.2%
Position	IT Manager	22	9.2%
	IT staff	63	26.4%
	General director	7	2.9%
	Manager financial	13	5.4%
	Director of Human Resources	4	1.7%
	Other administrators	21	8.8%
	Doctor	41	17.2%
	Physician Assistant	17	7.1%
	Pharmacist	25	10.5%
	Lab physician	23	9.6%
	Other health care professional	3	1.3%
Years of Experience	4 years or less	104	43.5%
	5 - 10 years	76	31.8%
	10 years or more	59	24.7%

• Descriptive Statistics

To represent numerical or mathematical methods to collect data, summarize or shorten it, and display it in tables.

Table 2. Descriptive Statistics

Items	Mean	Std. Deviation	Percentage	Verbal Result
Adoption of Cloud Computing	4.23	0.596	84.6%	Strongly Agree
Availability	4.08	0.643	81.6%	Agree
Reliability	4.15	0.533	83.0%	Agree
Technological Readiness	3.6	0.836	72.0%	Agree
Perceived Barriers	3.58	0.830	71.6%	Agree

- **Correlation Analysis**

Correlation is an indication of the nature of the relationship between two variables. The relationship can be positive, negative, weak, moderate, strong, or any logical combination. “A Pearson correlation matrix will indicate the direction, strength, and significance of the bivariate relationships among all the variables that were measured at an interval or ratio level. The correlation is derived by assessing the variations in one variable as another variable also varies.

Table 3 shows the correlation analysis between the dependent variables and the independent variables.

Table 3 shows the correlation analysis			
Variables		Person correlation	P value
Using of Cloud Computing	Availability	.549**	.000
	Reliability	.230**	.000
	Technological Readiness	.401**	.000
	Perceived Barriers	-.228-**	.000

9. Discussion

The following section discusses two contexts in detail. Table 4 shows that.

A. Technological Context

The results show that the technological context is the first dimension in the use of cloud computing in hospitals in Yemen and represents a mean of 4.12. This context is represented by two technical factors: reliability and availability.

The results showed that there is an important positive impact between availability and the use of cloud computing. The results also show that there is an important positive impact between reliability and the use of cloud computing.

B. Organizational Context

The results show that this context is the second most important dimension in the use of cloud computing in Yemeni hospitals and represents a mean of 3.59. This context is represented by two factors: perceived barriers and technological readiness.

The results show that there is an important positive impact between technological readiness and the use of the computing cloud. Moreover, the results show that there is an important positive impact between perceived barriers and the use of cloud computing.

Table 4. Overall Statistical Results of the Research Variables

The result of this study shows a serious concern about security, privacy, and confidentiality of patients' data.

10. Conclusion

This research studied two main contexts: the technological and organizational contexts, to find out the concerns about the use of cloud computing technology in the health sector. The results indicated the desire of hospitals to use cloud computing

because of its enormous benefits in the health sector, with concern about data security with cloud computing. In addition, this research proposes a model for protecting and storing the patient's medical record using two technologies: cloud computing and blockchain. The model guarantees high protection, confidentiality, and privacy of patient data and provides all beneficiaries of cloud computing

Table 4. Overall Statistical Results of the Research Variables						
Context	**Context Ordinary**	**Variables**	**Mean**	**SD**	**Percent**	**Verbal Result**
Technological (mean=4.12)	1	Availability	4.08	0.643	81.6%	Agree
		Reliability	4.15	0.533	83.0%	Agree
Organizational (mean=3.59)	2	Technological Readiness	3.6	0.836	72.0%	Agree
		Perceived Barriers	3.58	0.830	71.6%	Agree

with all the necessary information when needed. In the future, we will implement a research model.

11. References

[1] Sharma, Y. and B. Balamurugan, A survey on privacy preserving methods of electronic medical record using blockchain. Journal of Mechanics of Continua and Mathematical Sciences, 2020. 15(2): p. 32-47.

[2] Chenthara, S., et al., Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 2019. 7: p. 74361-74382.

[3] Zhang, A. and X. Lin, towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems, 2018. 42(8): p. 1-18.

[4] Premarathne, U., et al., Hybrid cryptographic access control for cloud-based EHR systems. IEEE Cloud Computing, 2016. 3(4): p. 58-64.

[5] Li, H., et al., Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data. IEEE Transactions on Cloud Computing, 2017. 8(2): p. 484-494.

[6] Mehmood, A., et al., Anonymous authentication scheme for smart cloud based healthcare applications. IEEE access, 2018. 6: p. 33552-33567.

[7] Kish, L.J. and E.J. Topol, Unpatients—why patients should own their medical data. Nature biotechnology, 2015. 33(9): p. 921-924.

[8] Zhu, Q., et al., Applications of distributed ledger technologies to the internet of things: A survey. ACM computing surveys (CSUR), 2019. 52(6): p. 1-34.

[9] Tanwar, S., K. Parekh, and R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 2020. 50: p. 102407.

[10] Gordon, W.J. and C. Catalini, Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal, 2018. 16: p. 224-230.

[11] Esposito, C., et al., Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 2018. 5(1): p. 31-37.

[12] 1Gan, C., et al., Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor. Multimedia Tools and Applications, 2021. 80(20): p. 30605-30621.

[13] Mell, P. and T. Grance, The NIST definition of cloud computing. 2011.

[14] Paiti, T., What are the opportunities and challenges of cloud computing technology in the healthcare information systems. 2013.

[15] Buyya, R., C. Vecchiola, and S.T. Selvi, Mastering cloud computing: foundations and applications programming. 2013: Newnes.

[16] Barthelus, L., Adopting cloud computing within the healthcare industry: opportunity or risk? Online Journal of Applied Knowledge Management (OJAKM), 2016. 4(1): p. 1-16.

[17] Hwang, K., J. Dongarra, and G.C. Fox, Distributed and cloud computing: from parallel processing to the internet of things. 2013: Morgan kaufmann.

[18] Kuo, M.-H., A. Kushniruk, and E. Borycki, Can cloud computing benefit health services?–a SWOT analysis, in User Centred Networked Health Care. 2011, IOS Press. p. 379-383.

[19] Mistry, I., et al., Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical systems and signal processing, 2020. 135: p. 106382.

[20] Kabra, N., et al., MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions. Future Generation Computer Systems, 2020. 102: p. 574-587.

[21] Vora, J., et al. BHEEM: A blockchain-based framework for securing electronic health records. in 2018 IEEE Globecom Workshops (GC Wkshps). 2018. IEEE.

[22] Androulaki, E., et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. in Proceedings of the thirteenth EuroSys conference. 2018.

[23] Al Mamun, A., S. Azam, and C. Gritti, Blockchain-based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. IEEE Access, 2022.

[24] Attaran, M., Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 2022. 15(1): p. 70-83.

[25] Singh, N. and P.D. Kaur, A hybrid approach for encrypting data on cloud to prevent DoS attacks. International Journal of Database Theory and Application, 2015. 8(3): p. 145-154.

[26] Saravanan, N. and A. Umamakeswari, Lattice based access control for protecting user data in cloud environments with hybrid security. Computers & Security, 2021. 100: p. 102074.

[27] Pournaghi, S.M., M. Bayat, and Y. Farjami, MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing, 2020. 11(11): p. 4613-4641.

[28] Kuo, M.-H., Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 2011. 13(3): p. e67.

[29] Alharbi, F., A. Atkins, and C. Stanier, Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations. Complex & Intelligent Systems, 2016. 2(3): p. 155-171.

[30] ghaleb, Y., Adopting cloud computing in the yemeni public sector, Opportunities and challenges. 2016.

[31] Ayoobkhan, A.L.M. and D. Asirvatham, Adoption of cloud computing services in healthcare sectors: special attention to private hospitals in Colombo district, Sri Lanka. 2017.

[32] Oliveira, T., M. Thomas, and M. Espadanal, Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. Information & Management, 2014. 51(5): p. 497-510.

[33] Alshaibani, M., Cloud Computing Framework for Yemeni Universities. 2017.

Appendix: Measurement items			
Constructs	**Items**		**Adapted source**
Availability (AV)	AV1	Cloud computing in hospital provides its services consistently and uninterruptedly.	[28]
	AV2	Providing patient data is critical to healthcare providers in hospital who cannot work effectively unless such data is available.	[28]
	AV3	The cloud computing continuously provides health services without a decline in performance.	[28]
	AV4	Cloud computing in hospital need to make serious judgments to interact quickly and efficiently to ensure the continuity of service.	[28]
Reliability (RB)	RB1	The use of cloud computing in hospital requires assurances of the good reliability of the services provided.	[28]
	RB2	All health services and data require to be consistent and error-free.	[28]
	RB3	Data in cloud computing in hospital requires to in good condition regardless of any software, hardware or network failure.	[28]
	RB4	There are some cases where cloud computing services suffer from unreliability for technical reasons.	
	RB5	The provision of reliability and security requires to accept the application of cloud technology software in the medical field.	
Technological Readiness (TR)	TR1	The hospital provides Internet access to all its staff.	[29]
	TR2	The hospital has hardware that has the capabilities to adopt cloud computing technology.	[30]
	TR3	The hospital has software that has the capabilities to adopt cloud computing technology.	[30]
	TR4	The hospital has a network to adopt cloud computing technology.	
	TR5	The hospital has a technical staff ready to deal with cloud computing.	
	TR6	The hospital has sufficient training and education for staff to adopt cloud computing technology.	[31]
	TR7	The hospital management benefits from information technology to achieve its goals.	[29]
Perceived Barriers (PB)	PB1	There is a concern about data security in cloud computing.	[30]
	PB2	Using cloud computing reduces data privacy.	[32]
	PB3	There is concern about denial of data access at sometimes instance.	
Adoption of Cloud Computing (ACC)	ACC1	Adopting cloud computing technology in the hospital is a useful technological option.	[33]
	ACC2	Adopting cloud computing technology in the hospital is a useful economic option.	[33]
	ACC3	The adoption of cloud computing technology in the hospital increases the efficiency and quality of the medical services provided to the beneficiaries.	[33]
	ACC4	The adoption of cloud computing technology in the hospital increases the efficiency of hospital staff.	[33]

	ACC5	The adoption of cloud computing technology in the hospital increases the satisfaction of beneficiaries.	**[33]**
	ACC6	The adoption of cloud computing technology in the hospital increases the protection and security of information and data.	**[33]**
	ACC7	The adoption of cloud computing technology improves the performance of medical services.	**[33]**