Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

SECURED AND REVOCABLE AUTHENTICATION AND SHARING SYSTEM USING SMART-CONTRACTS FOR CLOUD DATA

Fatima Anjum[*1], Maheen Alia[2], Saima Farhan[3], Ayesha Iqbal[4], Kawish Habiba[5]

[*1,2,3,4]*Department of Computer Science, Lahore College for Women University, Lahore*
[5]*Department of Informatics and Systems, University of Management and Technology, Lahore.*

[*1]fatima.anjum@lcwu.edu.pk

DOI:https://doi.org/10.5281/zenodo.17511831

Keywords
Cloud Data, data sharing, security, electronic health records, authentication, encryption techniques, smart contracts, revocability

Article History
Received: 10 September 2025
Accepted: 16 October 2025
Published: 29 October 2025

Corresponding Author: *
Dr. Fatima Anjum

Abstract
In cloud environment, data is stored and shared among multiple nodes. This data is managed by third party, may have security, revocability and authenticity issues. Data sharing and exchanging services are being needed in every field i.e education, banking, health etc. In this case study medical dataset is used. As medical sector is more personal and crucial process, health records have a lot of medical and personal information of individuals. Electronic Health Records (EHRs), are digital format in which highly private information related to the diagnosis and treatment of patient is stored and it is also needed to share with peers. Hence, sharing of health records between participants is very challenging because the data might be leaked or tampered during the exchanging process. A secure and revocable data authentication system is proposed to overcome these issues in data sharing. Also modern Hybrid encryption techniques is implemented to share data via secure channel. The enhanced results and some comparisons are shown in the results section.

I. INTRODUCTION

As Internet of things (IoT) is a way of communication between devices and human Society. In this era everybody wants a comfortable lifestyle that is why internet has become necessity of life. The huge data collected from actuators and sensors is stored in cloud environment that is being exchanged between devices for sharing important information according to situations. Cloud environment has brought good approaches for recovering and sharing digital information, making the possibility of on-demand information sharing into the real world. Sharing the data among multiple peer nodes depending upon demand. In any situation, simple and fast access is repeatedly just equal to and cause security weakness, especially when it comes of the sharing of delicate material and information. Hence, the data security and authentication has become essential issue [1]. As we know with advancement, technologies are improving various sectors of life i.e business, education, finance, health and many more. The main benefits of advanced technologies are to enhance security, usability and more manners in medical sector. EHR (electronic health records) is digital format of storing and managing patient's medical data. Electronic health records have been promoted as to increase the quality of healthcare by improving efficiency of healthcare system. It has become emerging technology when compared with traditional paper-based medical records which have some

disadvantages like lost, availability issues etc [2]. But on demand of cloud computing the security requirements in sharing system is considerably developed. Many suggestions are recommended to establish the guarantee and safety of medical cloud data. During diagnosis and treatment procedure, the accessibility of entire EHRs on the cloud's benefits doctors check patient medical conditions and give proper prescription. But the medical records can be tempered, hacked or shared to others without any consent. That is why security and privacy issues also arise [3,4]. Further on the certainty and privacy of user's information are the most immediate boundaries while sharing data. Uncertified organizations may gain illegal control over records without consent, that has poor influence on confidentiality, integrity and security of data in the systems. It is therefore significant to have an efficient control mechanism solution for personal data sharing systems fig.1. In this case, owners of the data require to show the protection of the utilized data by using cryptography processes i.e, protecting information by codes [5,6]. Smart contracts are some instructions written in codes that execute the specific terms and conditions which are in contracts between different parties. The parties embed an agreed business logic in code. Parties can be individuals, organizations, governmental agencies or other administrative entities with a legal identity. These contracts are created on any step including authentication, verification and sharing while developing secure transmission system. The most common Smart contract platforms include. Hyper-ledger system where members do not fully confident on one another but know and identify one another [7,8]. Hyper-ledger framework where domain is the namespace building a network. Providers are responsible for making sure that all the peers in the network have executing transactions. When a transaction is proposed and agreed by a peer then organizations are the containers for the peers and respective certificate authorities. The certificate authority is responsible for creating user's certificates. It is used for verifying data ownership. The peers are nodes which are connected to clients and are responsible for executing transactions. Furthermore, privacy can be protected by checking and hiding the identities of all parties, it faces challenges to ciphertext improvement [9]. the data before it is exchanged. Orderly, attain adjustable access control to coded data, encryption based on attributes is an ongoing approach [10,11].

Many researchers have proposed and implemented different data sharing scheme for different environments. The data sharing is crucial issue and its demand is increasing with the time. To overcome privacy, security, confidentiality related issues in smart environment a proposed scheme is explained in next chapter.

II. RELATED WORK

Eiad Yafi1 *et al* suggested algorithm which is based on blockchain to handle privacy and incompetence of current devices. This hybrid technique was implemented to code the text while sharing this with organizations, also digital signatures of clients are generated and stored on blockchain. To test proposed framework a virtual cloud was also built. Data confidentiality and integrity were few factors applied to evaluated the performance of hybrid algorithm based on blockchain device on the virtual machine fundament. The vital role of their proposed framework is protecting privacy inside the cloud and fulfilling needs of service providers and clients. Results shows the efficiency of the proposed system compared with former [12]. Tianxu Li *et al* proposed an environmental monitoring cloud prototype system that inquires the data needed by the users and provide paid and unpaid data sharing. Data registration, data management, data querying, data processing and sharing modes were followed for data transferring. The authors had not highlighted the security issues and solutions in this setup [13]. *Mohammad Mousa Madine et al* provided Ethereum smart contracts based on blockchain for giving victims access upon their information in decentralized way. Their presented framework of system utilizes localized storage of interplanetary file systems (IPFS) and stand fast that depends on re-encryption oracles to securely store, and sent sufferer health data. They presented models as well as their complete deployment information and checked their proposed smart contracts using two significant performance measurements i.e; cost and correctness. Also, provided privacy examination along described generalize features of proposed system [14]. Liviu Hirtan *et al* paper explained a cooperative system that involves that the exchanging of health information among the health organizations as well as with additional institutions for instance research centers, insurance companies, etc. they have used techniques like blockchain and shared key methods. The design of scheme assures the non-disclosure about private data and notices the patient as the holder of

his/her security policies. Their workflow shows that trusted entities validate the health detail created by a medical unit [15]. Meng Shen *et al* presented a Blockchain based model which have data owners, miners, third parties these three different participants. The data was shared and recorded using blockchain and smart contacts among them. Private and public cloud was used for data sharing and acquiring among the participants. The authors also discussed about the reasons about security effect on data sharing and designed a sensible solution through distribution rules analysis. They proved that their scheme encourages data sharing and have positive effect on authentic data sharing in multiple clouds [16]. Chang *et al* proposed a secure file sharing system that promote a dispersed access authority and group key governance by the approval of the IPFS proxy. The file system which have a crucial role in the design adopted for taking responsibility over the control policies. The combination of the IPFS server and the blockchain network with the adoption of the IPFS proxy make a stable file exchanging system so the members on the system can create new groups or join different groups by their own choice. Although there is no accessing and controlling procedures in IPFS server and blockchain web, the secretly data sending system direct controls over access policies. The members access files only belong to the group they authorized [17].

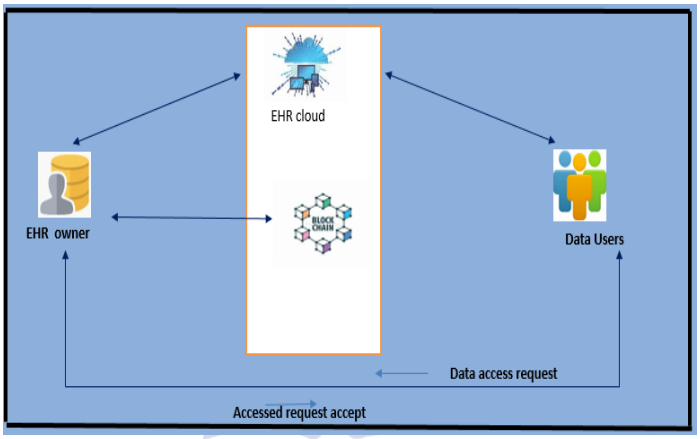


Figure 1: Data sharing existing system [22, 23]

Dagang *et al* aimed two issues, traditional data sharing and key management system for which they designed meta key and secure proxy re-encryption system. They also focused on reliability and availability of data along with encoded data transfer using encryptions. Authors focused on the illegal and deceitful free property of the cryptographic protocol and worked on it [18]. Sita Kumari Kotha *et al* described various issues and challenges for implementing a dynamic group data sharing platform. Their paper present user and service provider problems involving data confidentiality, security, privacy, performance and briefly summarized the prosed solutions for such problems. Their paper would help future scholars in developing secure data sharing mechanisms for smart environment [19]. XIA *et al* proposed a medical data sharing among data users in non-trustable domain. Their system is implemented using smart contracts for user access along with control over the data. Also the results were compared with existing system [20]. K. R. Sajay and Sasidhar described a hybrid technique in which blowfish encryption is used for data security. their major focus was security and storage. The limitations and security issues were discussed in this paper [21].

III. PRELIMINARIES

Socket

Sockets are application programming interface used for Inter-processing communication. This interface is used by developers for implementation network communication. Socket programs can be written in different languages refers as socket programming. These languages can be Python, C, C++, JavaScript etc running on different platform. For socket programming the Socket module is used in python library for system setup.

1)Socket Types

Two types of transport service provided by sockets that is connection oriented socket (TCP) and connectionless datagram socket (UDP)

o Datagram Stream ()
o Stream Socket ()

Domain is the group of protocols used in socket functions. It represents the data/file that the users requesting or accessing.
AF_INET6
AF_UNIX
AF_NET
PF_NET6

Hostname
It is a label assigned to a device/node for its identification

IP address
It is internet protocol address having series of numbers that identifies a device over the network. Such as 192.0.1.2.

Port number
Both sockets require port number. These are 16 bits' that identifies the processes involve in socket.

Socket Class
By importing socket library, the Socket class is used by developers to create socket objects.

Functions
Few socket programming functions are described below. By using which the secure transmission channel would be created.

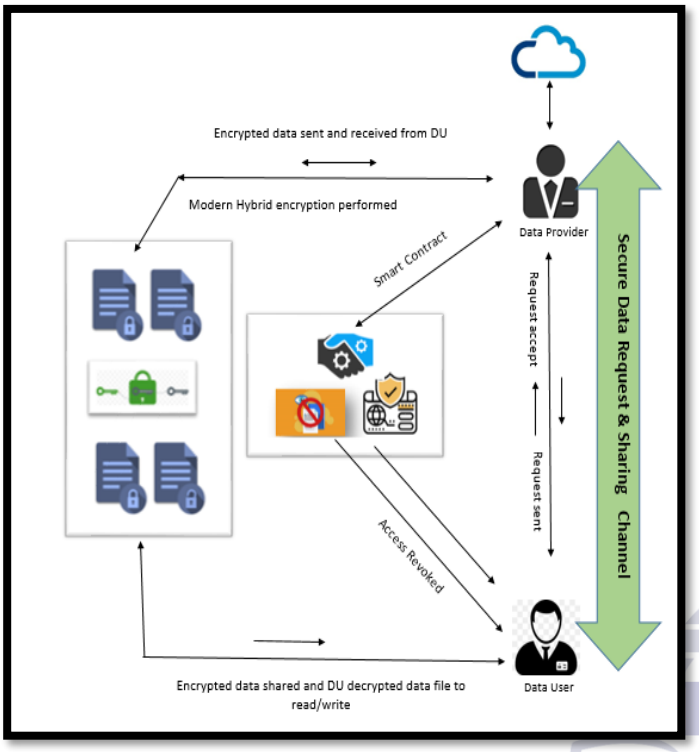
2)Smart Contracts
Smart contract are digital contracts between data users and data providers. The contracts can be for authentication, access, transaction purposes. These contract can be implemented in different languages. For python, SmartPy is python library used to create smart contracts. Variables, conditional statement can be used for creating these contracts.

Figure 2. Smart contracts

3)Cryptography technique
In this system for the data encryption and decryption process two layered cryptography techniques that is Modern Hybrid Encryption is implemented. It comprises of two RSA and AES encryption algorithms. RSA (Rivest-Shamir-Adelman) RSA is asymmetric encryption algorithm in which two different key are generated and data encryption process is performed. AES (Advanced Encryption algorithm is symmetric algorithm where one secret key is generated that is used for future process. I have implemented a modern hybrid technique by merging both the encryption techniques for better data security and transmission. In python AES and RSA libraries are imported for key generation and encryption/decryption process.

4) CouchDB

CouchDB is open source NoSQL database that provides many different formats to store and retrieve data. Widely use in healthcare, financial services, social media and many more services. It is developer friendly. CouchDB is flexible, fast and same structure document can be stored in it. Widely, supported by different languages and framework.



5) Dataset:

For this research Electronic health records are being used. Data can be in any form i.e, image, video, text etc that can be encrypted and shared over the network. In this research my focus is personal data [22][23].

IV. SYSTEM MODEL

A secure and reliable five steps data sharing mechanism is proposed by merging encryption techniques on both the data provider and user side. This scheme is useful for accessing personal data especially related to medical and financial information in centralized systems. To calculate the results EHR dataset is used. In cloud environment data is in any form text, images and videos. This Data is encrypted with a Modern Hybrid Encryption Algorithm written in python code and encrypted data is then sent to data user in through secure channel. After this secure transmission of data, at users' end, data is decrypted by authorized users according to the smart contract. Users can make any changes required in the data and send back after encryption to the data provider for updating in the cloud. After this whole process the access would be revoked for the users. This two-way data sharing architecture is shown in figure 3.

Figure 3: System Model

1) Communication Setup

In first step a secure transmission channel is buildup by connecting the two end users. For this case study I have used data provider (DP) and data user(DU). By using socket, the communication channel is created.

2) Authentication Contract and Data Request

In this phase user registration, data request and authentication is performed for giving access to the data file.

3) Key-Generation

Four keys are generated and used in this frame.

Public key (Pk)

Private key (Pr2) for data provider

Private key (Pr2) for data user

Master Key(MK)

4) Modern Hybrid Encryption/Decryption

Modern Hybrid Encryption techniques is implemented here for encrypting and decryption the data at both the side (DP and DU)

5) Data Update and Revocability

After sending back the changed data by DU. The data is updated in database and key's access would be revoked under smart contract.

A. IMPLEMENTATION

The proposed system is implemented in python language using PyCharm framework. Socket programming is used to make a connection for sending and receiving users. Smarts contracts for authentication and revocability is created in python also. Cryptographic methods is used for data encryption and decryption so that the file could share securely via socket. CouchDB is used to retrieved and updated the data.

i)Connection Phase

A secure channel is created for DP and DU for communication and data transmission. Algorithm 1 represents secure network channel.

Algorithm 1: Secure Channel

Input: network socket
Output: Connection successful

1. Import socket
2. Create a socket for DP and DU
3. Bind IP and Port bind
4. Connect DU. socket (addr)
5. Connection is built

Print: Connection Successful

ii)Registeration and Authentication

A smart contract is created and used for this phase. algorithm3, 4 are explained below

Algorithm 2: DU registration

Input: DU id, name, password
Output DU registeration

1. while true do
2. DU is new user
3. function REGISTERDATAUSER (DU name, DU id, password)
4. Insert to Registration table
5. end function

end

Algorithm 3: Authentication Contract

Input: Check DU authentication

1. request for file
2. Verify entered password
3. if
4. password match in the registeration table
5. create auth_code, code =rand_code '8'
6. send code to DU id
7. DU will enter the code
8. if
9. entered code= auth_code
10. user authenticated
11. else
12. authentication failed
13. else
14. wrong access

iii)Secure Data Sharing phase

In this phase two algorithms explains the key generation and encrypted data sharing procedure between two parties. Algorithm 5, 6 are given

Algorithm 5: key generation

Input: import AES, RSA
output: Mk key, Pk, Pr1, Pr2

1. Create Mk key using aeskey random bytes
2. then create two RSA keys using
3. random = Random. new().read
4. private1 = RSAkey. exportKey() for DP
5. private2 = RSAkey. exportKey() for DU

Algorithm 6: Sharing phase

Input: data file, encryption
Output: data file share to DU

1. Get Mk, Pk keys
2. encrypt data file using Mk
   e_data = aescipher.encrypt_and_digest(data)
3. then encrypt Mk using Pk
   e_aeskey = rsacipher.encrypt(aeskey)
4. share this bundle. enc file to DU
5. If
6. DU make changes in file and share with DP
   re_encrypted file
7. then
8. decrypt data file using Pk2
9. compare the data file with previous
10. Update the data file in db

iv)Revocation

After secure completing data exchanging steps the users access session would be expired. Algorithm 7 is given below.

Algorithm 7: Revocation Contract

Input: nonce
Output revoke user access

1. Create smart contract for revoking access
2. get nonce () for sharing session
3. return nonce used
4. session expired

After system architechture and implementation the results were calculated

V. PERFORMANCE ANALYSIS

Previously smart environments used different cryptography methods to secure and share data. The proposed system results are compared with few of the existing systems performance.

A. Encryption time

The encryption and decryption time is calculated and shown below. The results of Modern hybrid encryption and decryption is shown in figure 4

Table 1: Encryption and Decryption Results of Modern Hybrid Algorithm

File (Mb)	Encryption time(s)	Decryption Time(s)
2	0.5	1
5	1.3	3.5
10	2.7	5.3
20	4.3	7.6
60	10	14.71

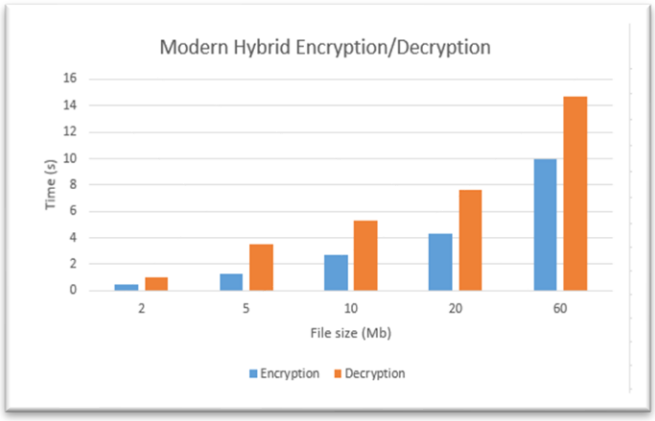


Figure 4: Results of encryption and decryption

B. Encryption time comparison

From table 3 and figure 45we can analyze the difference between encryption time of two different algorithms using different file size.

Table 2: The Encryption time of proposed and existing scheme

	Modern Hybrid Encryption	Blowfish- Rsa
File (Mb)	Encryption time(s)	Encryption time(s)
2	0.5	9
5	1.3	12.2
10	2.7	13.5
20	4.3	14.24
60	10	40.8

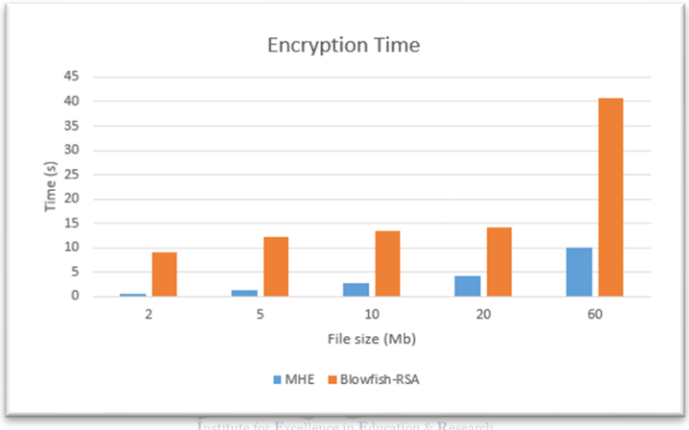


Figure 5: Represents encryption time of between proposed and existing scheme

The proposed architecture time is better from the existing algorithm [21] in encryption processes. The analysis shows that makes proposed system bit faster and secure.

C. Decryption Time Comparison

The decryption time of Modern hybrid algorithm is calculated and shown in figure

Table 3: Decryption time calculations

	Modern Hybrid Encryption	Blowfish- Rsa
File size (Mb)	Decryption time(s)	Decryption time(s)
2	1	5
5	3.5	10.43
10	5.3	20.5
20	7.6	65.24
60	14.71	110.67

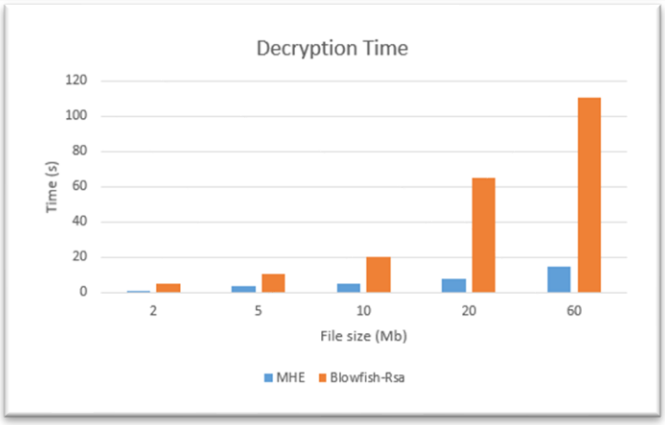


Figure 6: Represents decryption time of between proposed and existing scheme

From table 2 and figure 5 we can analyze the difference between decryption time of two different algorithms using different file size. The proposed architecture time is better from the existing algorithm [21] in decryption processes. The analysis shows that makes proposed system bit faster and secure.

D. Latency

Latency per number of requests is shown in figure and table below.

Table 4: The latency per user requests compared with two existing algorithms

No of requests	MHE	Med Share	Med block
5	40	83.4	53.4
10	61.09	122.51	145.26
15	78.3	146.7	178.24
20	95.34	188.7	226.78
30	130.45	305	351.3

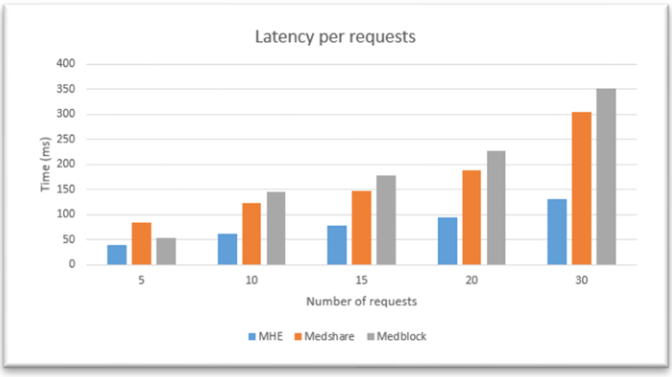


Figure 7: Represent the latency per user requests comparison

The latency of proposed scheme is low as compared to the other two architectures [17] [19] as shown in table 4 and figure 7.

VI. DISCUSSION

Cloud Data Security is always a first priority for any healthcare, education or industrial side. The data is stored in cloud can be used and required for many purposes. In this research a secure data sharing scheme is proposed to exchange information in a safe way where data hacking, tampering and loss issue is overcome. The process is implemented using Modern Hybrid Encryption method. So that during the data sharing or exchange process it is in secure form i.e cipher-text that is unreadable by any un authorize person. The authentication process is performed before sharing any data to specific peer and the revocation mechanism is also used to make the data more secure. Revocation is used to revoke access of user after sharing mechanism is completed so that the data file is not accessible until the data user requests for the file. This architecture makes the data access, sharing a bit faster and confidential as well.

REFERENCES

[1] M. N. P. Bachhav Bhavana, "Data Management for Internet of Things: A Survey and Discussion," *International Research Journal of Engineering and Technology*, vol. 04, 2017.

[2] Q. U. SHAHNAZ AYESHA, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, 2019.

[3] Q. U. Usmana Muhammad, "Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology," *Science Direct*, vol. 174, 2020.

[4] X. W. Z. J. C. L. F. &. L. G. Liu, "A Blockchain-Based Medical Data Sharing and Protection Scheme," *IEEE Xplore*, vol. 7, 2019.

[5] D. C. P. P. N. D. M. &. S. A. Nguyen, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, 2019.

[6] e. a. Eltayieba Nabeil, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *Journal of Systems Architecture*, vol. 102, 2020.

[7] K. a. Scott Clemens, "Security Techniques for the Electronic Health Records," *Springer*, vol. 127, 2017.

[8] F. Andressa and R. V. e. al, "Scalable Architecture for sharing EHR using the Hyperledger Blockchain," *IEEE International Conference*, 2020.

[9] W. N. e. a. Sukhwani Harish, "https://ieeexplore.ieee.org/abstract/document/8548070," *IEEE International Symposium on Network Computing and Applications*, 2018.

[10] D. S. ,. X. Z. Chen Yi, "Blockchain-Based Medical Records Secure Storage and Medical," *Journal of medical systems*, 2019.

[11] M. X. e. al, "Trusted data sharing with flexible access control based on blockchain," *Computer Standard and Interfaces*, vol. 78, 2021.

[12] A. D. M. Y. Eiad, "Decentralizing Privacy Implementation at Cloud Storage Using," *Arabian Journal for Science and Engineering*, 2020.

[13] L. T. e. a. Xiao Shuo, "Cloud platform wireless sensor network detection system based," *Cluster Computing*, 2019.

[14] e. a. A MADINE MOUSS MOHAMMAD, "13. Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for giving patients control over their medical records. IEEE Access, 8, 193102-193115.," *IEEE Access*, 2020.

[15] e. a. Hirtan Liviu, "Blockchain-based approach for e-health data access," *IEEE*, 2019.

[16] S. Meng and D. Junxian, "Blockchain-Based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds," *IEEE Xplore*, vol. 38, 2020.

[17] C. S. T. e. a. Huang Shan Hsiao, "A Secure File Sharing System Based on IPFS and Blockchain," *IECC Proceedings of the 2020 2nd International Electronics Communication Conference*, 2020.

[18] S. B. E. A. O. K. G. J. XIA QI, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," *IEEE* , vol. 5, 2017.

[19] S. B. S. Sajay . R.K, "Enhancing the security of cloud data using hybrid encryption," *Journal of Ambient Intelligence and Humanized Computing*, 2019.

[20] B. O. Liu Xing, "A Comparison of the Definitions for Smart Sensors,Smart Objects and Things in IoT," *IEEE Xplore*, 2016.

[21] D. R. ROUHANI SARA, "Security, Performance, and Applications of mart Contracts: A Systematic Survey," *IEEE Access*, vol. 7, 2019.

[22] "https://www.kaggle.com/datasets/imdevskp/corona-virus-report," [Online].

[23] "https://www.kaggle.com/datasets/karimnahas/medicaldata," [Online].