A Cryptographic System Based on Blockchain and Attributes for Sharing Medical Data

Pavithra S
Department of Artificial Intelligence and Data Science
Nitte Meenakshi Institute of Technology, Bengaluru, India

Abstract — Medical information contains a great deal of personal data and is quite sensitive to privacy concerns. Given the increasing volume of information in the healthcare sector, medical data must be appropriately and safely kept in this big data era. However, sharing current medical information can be risky and challenging because of the potential for privacy violations. To solve these issues, this study proposes a blockchain framework-based storage solution for healthcare information security along with attribute-based access control. The concept uses attribute-based access management to enable dynamic and granular access to medical data, which can be made secure and impenetrable before being stored in the blockchain system by creating related crypto contracts. Moreover, IPFS technology is incorporated into this solution to ease the blockchain's storage burden. Experiments demonstrate that the suggested system in this study, which combines Demonstrations reveal that the scheme proposed in this paperwork on the combination of access control of attributes and blockchain technology will not only takes care of the storage and uprightness of medical data but also have more productivity while accessing the medical information.

Keywords: Attribute-Based Cryptosystem, Blockchain, Confidentiality, Electronic Medical Data, No Tampering. Medicine Information, IPFS

I. INTRODUCTION

Sharing of medical data in the current era results in the development of novel methods and medications for the treatment of numerous disorders. This can be accomplished by digitally archiving medical information and enabling remote accessibility. Patients are the sole owners of these records because the information contained in the electronic record was provided by them following their visits to the hospital. The amount of information kept in electronic records is growing, creating big data that can be applied to a variety of healthcare-related tasks. Due to the importance of data storage and sharing, numerous business entities have emerged to collect, process, analyze, and store data to share it with other authorized sectors. This trend causes more businesses to concentrate on data analytics, cloud storage, and processing, which makes it necessary for current businesses to rely on the availability of data to function and continue to exist. Several stakeholders made investments in cloud computing and storage to meet the heightened demand for big data storage. Data storage in cloud computing services was appealing to a wide range of customers, including patients, the healthcare sector, and the research industry. Also, controlled, cross- domain, and flexible data sharing are advantages that it provides. The biggest problem with data sharing and store- housing via the pall is the threat of data exposure to unasked third parties.

Telecare Medicine Information System has enabled the delivery of healthcare services to patients thanks to the fundamental advancements in information and communications technologies (TMIS). By discussing patients' illnesses with them and exchanging vital information with other medical specialists, the TMIS enables doctors to offer medical assistance from any distant location.

The TMIS can significantly lower the cost of treatment in this way. By using current medical history, this approach makes precise disease diagnosis decisions easier. The limitation of this situationstands out is the procedure of decision-making when there is an arrival of new patients whose health records and information related to medical history are not stored. To avoid this, it could be useful to use EHR, which provides all the information, including information about the patient, including billing information, scanning reports, clinicalrecords, sensor information, medication information, medical history, insurance information, and so forth applicabledata. Data sharing of this kind of information would present privacy and security risks. [2].

The IoT and wearable technology recently have evolved in the health industry. The cloud, which has access to a variety of health data and helpful forecasts, was used to store the data from each wearable gadget. To improve disease monitoring, diagnosis, and treatment, this data is connected to the EHR. [3].

A blockchain is made up of a continuous chain of blocks that each include all the entries, similar to a typical public ledger. A block is made up of a parent block, a child block, and a block header that contains the hash value of the preceding block. The uncle block hash information is also stored on the Ethereum blockchain. The genesis block is the name given to it initially. The Genesis block is devoid of any parents. For an EHR management system, blockchain technology offers a number of advantages, but it also has certain disadvantages. The system's processing components collide, and it's possible that blockchain engineering changed the chain structure. Members of the organisation would need to have some faith in a decentralized structure to benefit from it, Mining nodes would at the very least not want to compromise the blockchain's immutability.

Using a legitimate blockchain minimizes the motivation for third parties to link PHI because the transaction records are transparent. Furthermore, even if using a reliable blockchain lessens the motivation for third parties to correlate PHI, transaction records cannot be hidden. Nodes can now conduct negative network analysis. By examining a set of transactions, an adversary could learn details about a particular node's trips to the doctor, interactions with service providers, or social interactions.

Distributed systems are needed to perform cryptographic algorithms since they consume a lot of memory. As a result, the blockchain is unable to efficiently

store enormous amounts of data. Because the data will be stored elsewhere, it may still be exposed to outside attacks even if blockchains may handle data integrity and access control. The following sections make up the remainder of this study: A suggested technique is offered in Section 3, findings and analysis are shown in Section 4, and this documentation is wrapped up in Section 5. Section 2 explores related papers that discuss current methods for using blockchain to handle healthcare data.

II. RELATED WORK

Traditional identity management still relies on software certification, although researchers later suggested dynamic multi- factor authentication as a more effective method.

Public key infrastructure (PKI) has to be improved because it is security vulnerable, as shown by Lee et al.[12].

When using the elliptic curve principle for authentication and key creation, Xu et al. present a mutual authentication scheme based on two-factor authentication [13].

The difficulties that the multi-factor authentication method encountered when creating certificates for data sourceselliptic curve cryptography is used are highlighted by Zhang et al. [14]. By combining blockchains at the front with trustworthy hardware at the backend SGX, they also present new schemes for certificate generation.

Key authentication for the Session Initiation Protocol (SIP) was proposed by Tu et al. [15,18,37].

For the creation of wireless device certificates, Liu et al. described a bilinear method based on elliptic curves. However, this method is vulnerable to simulation attacks, so a new, improved system based on anonymous identity management was developed [16].

Decentralized blockchain design has advantages over traditional architecture, as shown by Lin et al. [17].

AI To preserve quality, Bassam et al. developed a based on smart contracts authentication certificate solution that supports confidence between user identities and properties. They had acquired the authority to do X.509 user certification requirements identification however we were unable to. A decentralized architecture for sharing medical data based on the blockchain is presented by Asph Azaria et al., although the model's efficacy is poor [19]. Miners uphold data utilizing aggregation and reward mechanisms.

The constraints of using cloud storage technologies to implement data sharing were demonstrated by Esposito et al. as well as the limitations of cloud-based blockchain integration options for exchanging medical information. [20,29]. Li et al. describe an architecture focused on attribute-based encryption (ABE) technology for network-based access control and record storage. This plan ran into problems when the policy was changed because every time the policy was changed, the entire ledger had to be updated, which caused attribute revocation and encryption to cost more to process exponentially. Additionally, because blockchain engineering is tamperproof, the ledger could not be informed of these changes [21, 31].

Gu et al. developed the optimal encryption based on attributes (ABE) a technique to reduce computing costs, however, they were unable to fix the issue by changing the policy [22,32].

To ensure the authenticity of health records embedded in blockchain networks, Guo et al. developed an attribute- based multi-authority signature technique [23,34].

A distributed information monitoring system developed by Ferdous et al. Represents the use of access control, a common mechanism for dealing with data sharing issues, but cannot provide security. For the sake of authenticating users and blockchain networks, Nikola et al. proposed a unified trust management system using blockchain [25].

A transitively closed undirected graph- based identity management authentication system was introduced by Lin et al. to enable efficient data management and sharing based on identity identification and blockchains (TCUGA). This scheme uses node signatures, and hash functions, and does not require resigning on policy updates.

Li et al. suggested a prototype system that safeguards medical data and ensures its verifiability is built on the Ethereum platform and is trustworthy. [27],[36].

In their sparse matrix-based multiple-user identification scheme, Perera et al. provide an example of how multiple user activities can be recognized, controlled, and shared using multiple identities.

III. PROPOSED SYSTEM DESIGN

The six parties make up the medical data schema. Patients, hospitals, blockchain systems, CSPs, and users of medical data (medical institutions, insurance companies, etc.).

Appropriate Attribute Signing Keys SIKI; GIDs, Transformed Keys, and Private Keys are all provided primarily by the AAO to patients, medical data consumers, and hospitals, respectively. Patients draft and submit hospital accesscontrol policies. The patient then creates her LSSS-compliant medical information signature m0. The patient then sends her m0 to the data pool. The healthcare provider encrypts selected patient medical information.

A blockchain system consists of a consensus network, a blockchain, and a data pool. Medical data signatures, associated data, and cryptograms are contained in data pools. The device became advanced with the usage of the consort- team's blockchain to decorate the safety of scientific data. Coalitions including accounting nodes, hospitals, research institutes, and medical data users are working together to keep the blockchain up to date. Medical data will be tracked on the consortium's blockchain, which also ensures that the contents of the block cannot be changed. This includes addresses for encrypted medical data. Proof of Stake (PoS) technology is used in the consensus process of the consensus network to ensure the security of the blockchain ledger. Settlement nodes are initially selected by consensus nodes using the PoS mechanism. This allows broad consensus on the blockchain. The billing node then sends the encrypted medical data to the cloud and gets a data access address from there. Cloud- based medical data encryption text and medical- related data storage addresses are then added to the blockchain by accounting nodes. Blockchain offers decentralization, verifiability, and immutability properties that are important for solutions to distributed servers. CSP

mainly tracks the ciphertext of medical data and sends the ciphertext address to the blockchain. In addition, CSPs are authorized by data consumers to partially decrypt encrypted medical data. Medical data users initiate the process of seeking access to their data by uploading a collection of attributes to the blockchain system. If the verification is successful, the data consumer can obtain the ciphertext address of the medical data sent by the billing node. CSPs are authorized to partially decrypt the ciphertext of medical data after receiving an address and a transformed key from a data consumer. The medical data ciphertext is then fully decrypted by the user using the recovery key. CSP mainly tracks the ciphertext of medical data and sends the ciphertext address to the blockchain. In addition, CSPs are authorized by data consumers to partially decrypt encrypted medical data. The CSP primarily maintains the ciphertext for medical data and delivers the ciphertext's address to the blockchain. Additionally, the data consumers have given the CSP permission to partially decode the encrypted medical data. By sending their set of attributes to the blockchain system, medical data users start the process of requesting access to their data. Data consumers can acquire the medical data ciphertext address sent by the accounting node if the verification is successful. The CSP is then sent the address and transformed key by the data consumers, and it is permitted to partially decode the ciphertext of the medical data. The recovery key is then used by the users to fully decode the medical data ciphertext.

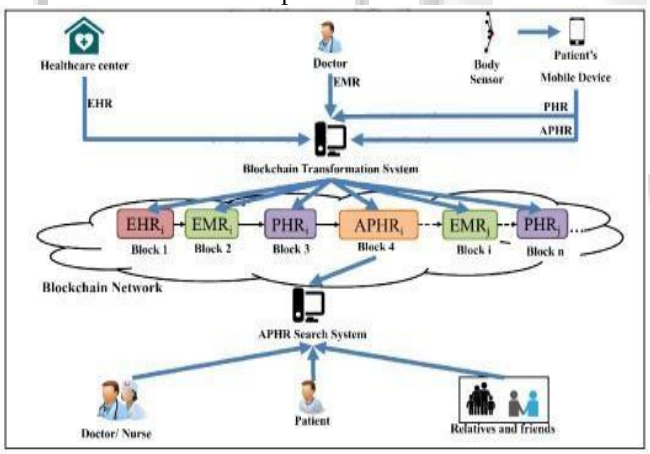


Fig. 1: The architecture of Blockchain-based data aggregation and group authentication scheme in electronic medical system

IV. PRELIMINARIES

A. Dual-linear map: Assuming that g is a generator of G, let G and GT be two multiplicative cyclic groups of prime order p. The map e: G G GT is referred to as a Dual-linear map if it satisfies the following requirements.

1) Dual-linear: For each a, b belongs to p, there is e(a,b) = eg(a,b).
2) Non-degenerate: e(g, g) not equal to 1.
3) Calculable: An effective procedure for calculating e exists for any g1, g2 G. (g1, g2).

B. Plan for linear secret sharing:

The LSSS goal is a method for dividing secrets into manageable portions. Then, various people are in charge of each stake. One person cannot recover the buried knowledge; only a small group of people can do it. This is the precise description:

1) Secret distribution : The x row and j column of the X matrix are chosen by the secret distributor. Blockchain technology combined with attribute encryption is described by Yang et al. as A system for sharing medical data. Imagine the transposed matrix represented by the vector v = (s,r1,..., rn). where s Zp is the secret value to be revealed and r1,.,rj belong to the random elements of Zp.
2) Secret share ownership: The function is denoted in the kth row of matrix M and the secret share held by the kth member Uk is denoted as Mk v . If the kth member's secret share is her Uk Mk v, the secret distributor sends the shared secret value s to x members U1,...,Ux(k).
3) AND-Gate Policy A set of attributes is represented by N = 1,..., n, where the attribute I BELONGS TO N. Positive and negative attributes are indicated by the attributes +i and I respectively.

The InterPlanetary File System (IPFS), the Blockchain, the medical system (including doctors and system smart devices), and the data consumer are the four main components of our approach (DU). The IPFS will be used to store the medical system's data, guaranteeing its privacy, searchability, and verifiability.

1) Blockchain: Modern technologies like consensus processes, peer-to-peer transmission, decentralised data storage, and encryption algorithms are combined in the cutting-edge application paradigm known as blockchain. In this case, we record the process of storing and locating medical data using blockchain. No one has the authority to arbitrarily change the data stored on the blockchain since it is unchangeable. It might therefore be cited as support for the uniqueness and fluidity of the data.
2) Attibute-Based Cryptosystem: A form of public-key encryption called attribute-based encryption depends on attributes to determine both the ciphertext and the user's secret key.
3) InterPlanetary File System is a decentralized storage system (IPFS). Each file is given a distinct hash value based on its content so that we can quickly locate the files using the hash value. Different file types can be shared and stored permanently. Deduplication is a feature of IPFS that efficiently prevents data duplication and conserves storage space. In this paper, we use IPFS to store our medical records.
4) Medical System: A smart device is also part of the medical system, which includes doctors as one of its components. Doctors are responsible for storing and encrypting patient documents on our system. To encrypt the medical data and create keyword indexes, he first executes the Encrypt and Index algorithms. The ciphertext that was previously kept in the IPFS is then added to the blockchain together

with the hash of the medical records and the IPFS's returned hash address. The system smart device is largely in charge of enrolling and identifying each hospital staff (such as doctors, nurses, patients, researchers, etc.). Each registered employee is also given a secret private key linked to their attribute.

5) Data User (DU): An individual who uses data (DU) could be a patient, a researcher, a nurse, a doctor, etc. The system can assign a key pair that matches each DU's characteristics. DU must first receive authorization from the hospital to access a patient's records. The system smart device will return a token so it can search for the necessary medical data if it deems that its qualities comply with the access policies.

V. MODEL OF THE SYSTEM

Instead of the relevant patients, healthcare organizations have been in charge of managing the HER. Healthcare organizations have been in charge of managing the EHR instead of the relevant patients. Patients must therefore save their medical records for future use.

The blockchain makes it possible to store medical data and offers free access to the EHR through relevant websites and data suppliers. The suggested remedy creates an electronic health data security framework based on blockchain that permits access to many authorities in a networked system. The suggested structure for the storage and access of healthcare data is shown in flowchart form in Figure By using the suggested blockchain infrastructure, patients can download and exchange their data straight from their EHR. The multi-user system involves five participants. the client, the physician, the EHR server, the insurance broker, and the authenticator are those people. The following are the stages involved in storing and distributing patient medical and personal data:

The patient visits the doctor. The doctor has given the patient treatment. As a mining node, the EHR Server collects transaction data for the blockchain network and stores it in blocks. After being created, the EHR is validated by all nodes on the blockchain network. These transactions are stored in the node of each node and subsequently added to a memory pool that acts as a holding area for all transactions executed on each node. The miner node collects and arranges this transactional data into blocks. Such data can be validated using the hash, a 256-bit value that indicates unique data. After the verification is finished, the miner selects the verification results from the memory pool and adds them to a new block.

After then, the new block is uploaded to the blockchain. When it is claimed for insurance-related reasons, the treating physician will grant the insurance agent access to this data. The insurance agent can authorize the insurance payment to the patient and refer patients' EHRs exclusively to those who have claimed them. The patient then contacts the data verifier to request that their data be verified. The verifier delivers a verification result to the patients after concluding whether or not the provided data are secure and safe. Only patients can view their data in the EHR thanks to this framework. The doctor who treats the patient may also view the data with the patient's permission. In a similar vein, the insurance representative can only see the patient's information if they ask for the insurance payout.

Our plan creates a mechanism for accessing and storing electronic medical records that can be proven to be safe. In particular, when the patient registers on the hospital system, the doctor provides a diagnosis and creates a medicalrecord. For the patient and the researcher to have access to the records anytime they are needed, the doctor must save the records. Before being saved, the medical records must be encrypted because they deal with the patient's sensitive information. The doctor has signed and encrypted the medical records.

Create keyword indexes after that, as described in step 1, and upload the data to the IPFS for storage. As can be seen in step 2, IPFS gives the doctor the hash address of the saved file.

The doctor hashes the patient's medical records and their index using the SHA256 hash function after receiving the hash address, as shown in step 3, encrypts the hash address using a random integer, and stores both the hash value and the encrypted hash address on the blockchain by broadcasting a transaction. A transaction ID will be returned by the blockchain, as demonstrated in step 4 of the procedure. Data storage is finished once the blockchain supplies the transaction ID.

The patient must first call up the earlier medical records before returning the next time to examine his record. The DU submits a keyword-rich access request to the hospital, the smart device in the system checks to verify if the DU has access rights, and if the DU confirms, it sends the DU a search token.

The following two steps show this. Based on the block ID obtained in the search token, the DU can get the corresponding hash value from the blockchain and, as demonstrated in steps 7 and 8, compare it to the corresponding hash address on the blockchain to determine whether the hash address discovered in the token was hacked. To access authentic medical records, DU also uses its private key to decipher the ciphertext. Finally, DU checks to see if its hash value agrees with the blockchains.

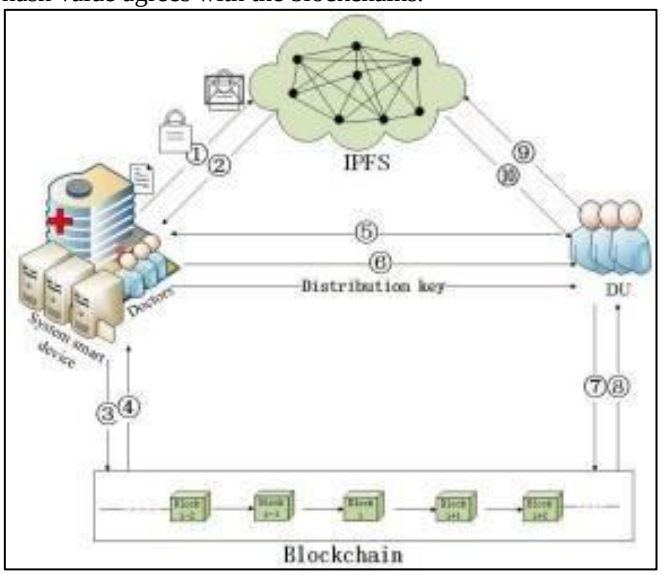


Fig. 2: System Model

A. Data Sharing Scheme

System Configuration: The AAO selects a bilinear map, a generator g of G, and two prime p multiplicative cyclicgroups, C and CT.

$$g\hat{}: (C)(C) = CT \quad (1)$$

Key generation: When a user registers with the system, the AAO will generate a private key with appropriate attributes. This private key can be obtained from the AAO. The steps are detailed below.

$$si \Rightarrow Zp, \text{where} i = [1, n] \quad (2)$$

Generation of private key:
Generation of Signature key
d = D^, (Di, Ei)(3)
S = P^, (S i, Pi)(4)
Example: Consider retrieved relevant context D,P,E,S used to generate key messages such that is based on:
D: Decryption text;
P: Private key generation;
S: Signature key generation;
E: Encryption text;

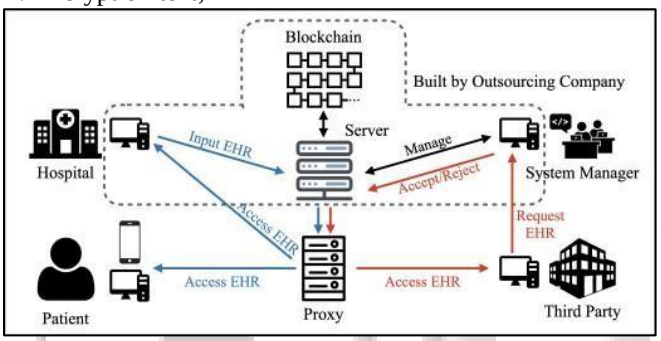


Fig. 3: Framework for Healthcare Data Storage and Access on the Blockchain.

Details of the planned system's operation Each system entity creates a public-private key pair PR; PU and registers on the Blockchain using their public keys by sending a registration transaction to the Registry Contract that is signed by their private key. The group of authorities employ a threshold signature to sign user data submitted to the Blockchain in order to ensure privacy. This protects consumers from associations with service providers that could put them at risk for privacy linkage attacks. To do this, the system's miners are represented by a single public key, and portions of the associated private key are discreetly distributed among them. As a result, a system public key PUs and system private key PRs key are generated initially, and each miner is given a part of the private key. Notably, in addition to the system key, miners also own a key pair that is comparable to that of regular users. While the users' unique key is used to carry out their private transactions, such requesting user data from another care provider, the system key is used to safeguard the users' privacy when data is recorded on the Blockchain.

Algorithm 1: Patient Blockchain creation and addition

Input: Patient Blockchain creation and addition:
Output: creating new blocks for the patient blockchain and adding them Begin
Give the EHR access to the patient's medical information
Create secret and public keys using the RSA encryption method.
while Not end of user session do
The doctor and insurance agent use the private key to decrypt the encrypted data while the patients use the public key toencrypt data.
Utilize the HMACSHA1 technique to create the encrypted EHR hash. Create a bilinear map for the encrypted EHR using the patient's ID.
Make a genesis block for the patient using the name, ID, and password provided. Block with the Added Bilinear Hash and Encrypted EHR
To the patient blockchain, include this block.
end while
END

The creation and expansion of the patient blockchain are offered by Algorithm 1. To increase the security of the suggested architecture, a bilinear map is used. The bilinear map is a function that joins two vectors to create a new vector and has the following mathematical definition:

$$B : VXW = X \quad (5)$$

Here,
V: Encrypted EHR
W: Patient ID
X: Bilinear Map

The bilinear map was created using identity-based encryption. As demonstrated in Figure, the genesis block of thepatient blockchain comprises the patient's name, ID, and password. The treatments for the patients have been rolled out one by one like new blocks. Data saved on the patient blockchain is only accessible by the patient; no one else hasaccess to it.

Algorithm 2: Emergence and expansion of Doctor

Input: A patient block referenced by the patient blockchain. Creating a Doctor Blockchain and Adding Blocks
Output: Form an insurance agency blockchain and add blocks to it Begin
Physicians and insurance agents download data from patient blocks transferred using private keys to their own blocks
while Not end of user session do
The block is hashed to produce a bilinear map, an encrypted EHR, and a hash. Decrypt encrypted EHR with private key
Physicians and insurance agents can access the EHR
Use the doctor's name, ID, and password to create a Genesis block for the doctor, and the insurance agent's information to do the same.
Add hash with encrypted EHR and bilinear map to block. Add this block to the Doctor and Insurance Agent blockchains.
The insurance amount for the treatment is transferred to the patient block
end while
END

The creation and expansion of a blockchain of medical professionals and insurance brokers is guided by algorithm 2. The Doctor blockchain, seen in Figure, is made up of Genesis blocks that store the names, IDs, and passwords of doctors. Over time, more blocks were added that contained information on how to treat illnesses. Blocks

are only accessible to doctors with patient permission. The blockchain for an insurance agent is depicted in Figure, and it is made up of Genesis blocks that contain the password, ID, and name of the insurance agent. Over time, more blocks were added that contained information on how to treat illnesses. Insurance agents are only permitted to view blocks with patient consent.

No one can access the data from the EHR because it is all encrypted on the blockchain. Finally, for the purpose of ensuring its security, the Data Verifier will validate the Patient Blockchain. Algorithms deliver the procedures needed for blockchain validation. The necessary block for the data verifier to validate will be present in the blockchain. A new hash will be produced for it after the encrypted EHR has been decrypted using the HMAC-SHA1 method and the hashwith bilinear map. If both the new Hash value and the new Bilinear Map match, the matching Block is considered to be a Safe Block; if not, the connected Block is considered to be a non-Safe Block.

VI. RESULTS

The respective doctors get access to view the patient's EHR only those who have got permission from the CSP. This is done to stop unauthorized users from getting access. The results of comparing the suggested method's suggested time requirements for accessing EHR in a blockchain to those of current centralized storage techniques are shown in Figure. Requests for data access have been made to the EHR, and the time needed to get the requested data has been recorded. Centrally hosted on a server will be the Electronic Health Record (EHR). The patient should ask for access to such papers by sending an EHR request with the relevant annotations to the central server. The central server checks for the availability of the needed data after receiving the EHR request and then transmits it to the patient. This procedure will be documented as:

$$\text{Timeconsupmption} = T\,2 - T\,1 \quad (6)$$

Where,

T2=Decrption time

T1= Encryption time

Additionally, the size of the EHR would have a direct impact on the amount of time needed to search for and access the data. It indicates that the amount of time required varies depending on the size of the electronic health record, i.e., the length of time required shall be decreased if the EHR is small and higher if the EHR is large. The comparison result demonstrates that centralized storage requires more time than the suggested blockchain method.

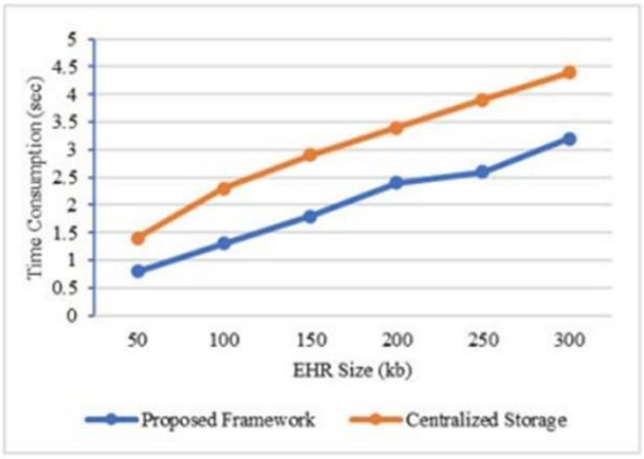


Fig. 4: Time Consumption

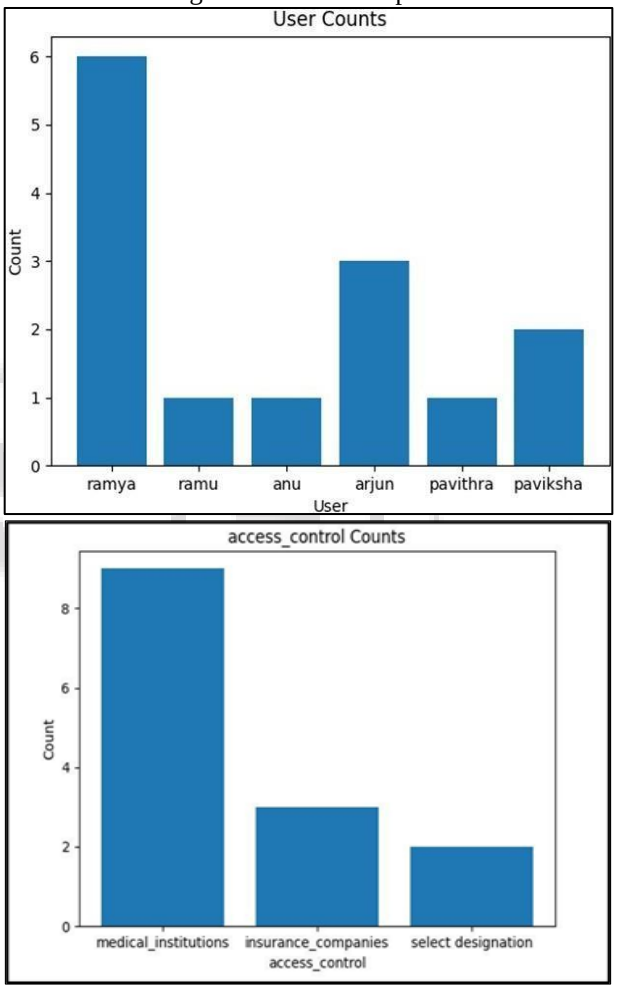
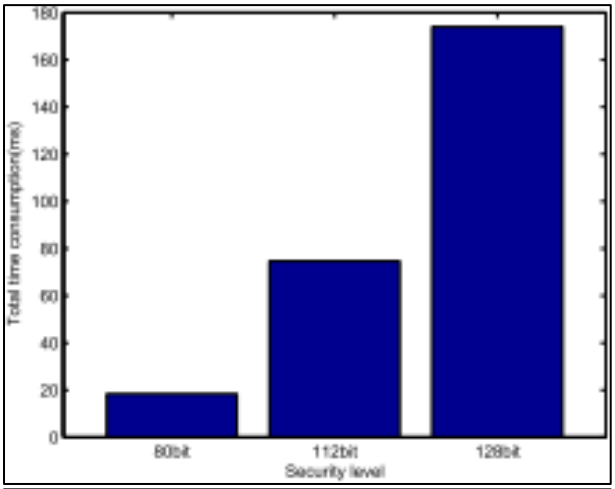


Fig. 5: (a)user counts; (b) Acccess counts



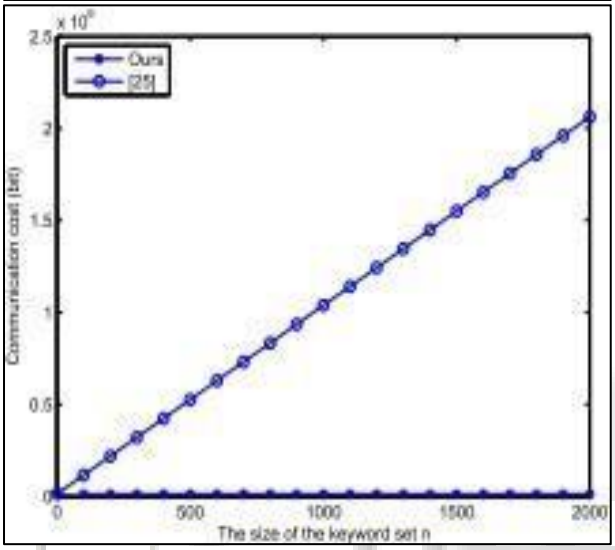
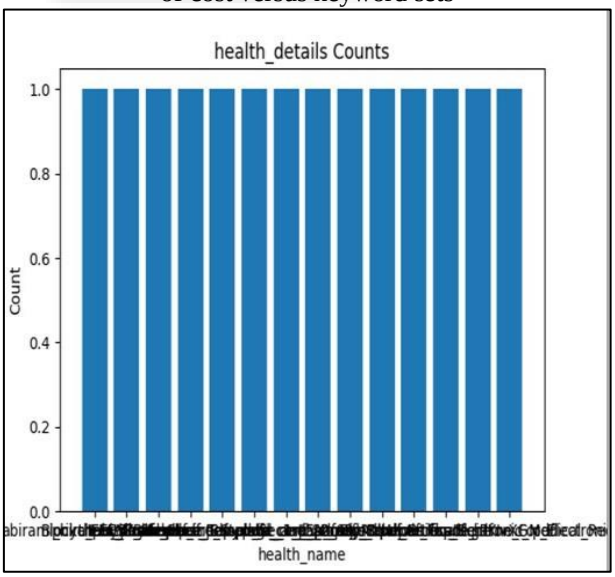


Fig. 6: (a) The total computational cost of experiments of the proposed scheme with security levels.; (b) Comparison of cost versus keyword sets



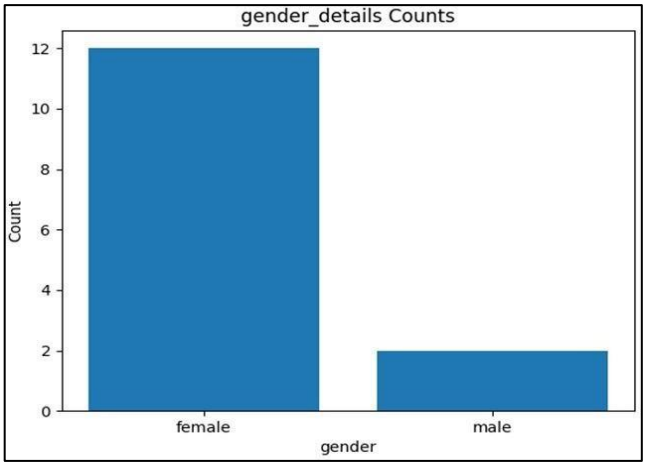
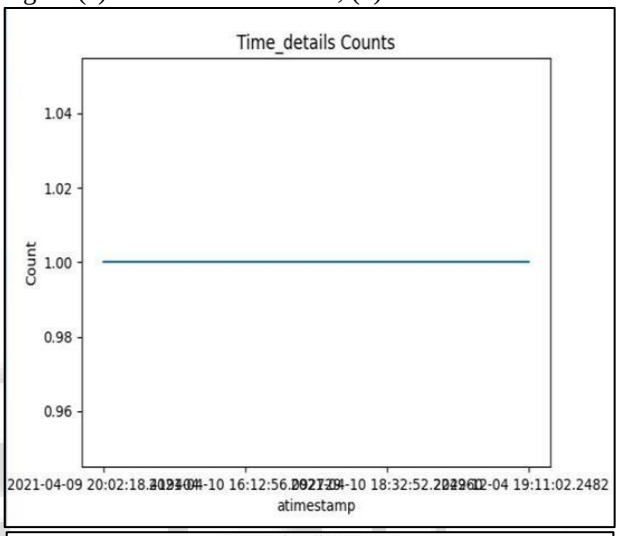


Fig. 7: (a) Health details counts; (b) Gender details counts



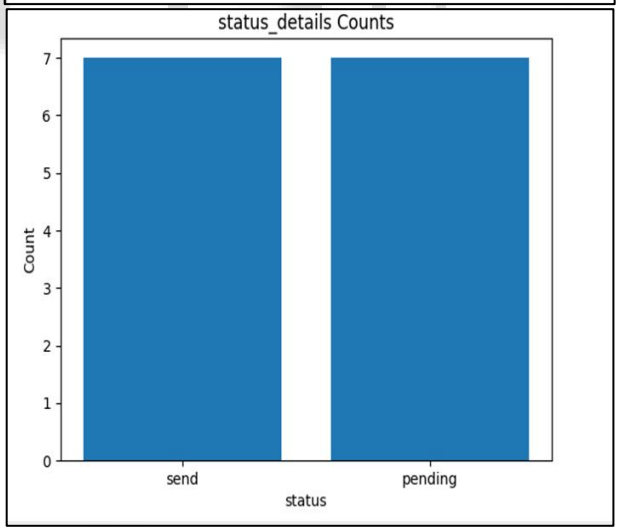
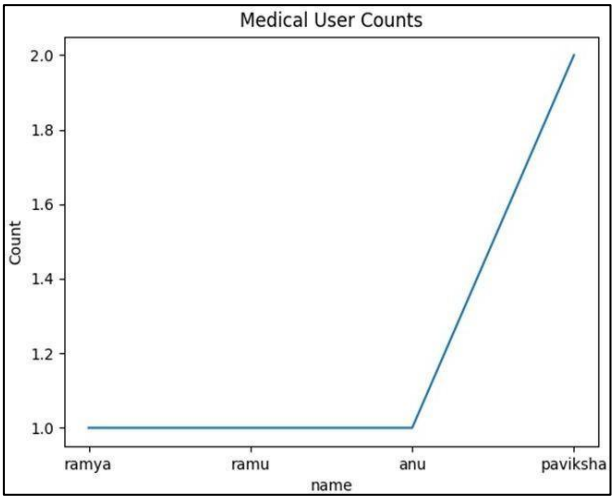


Fig. 8: (a) Time Detailscounts; (b) Status Details counts



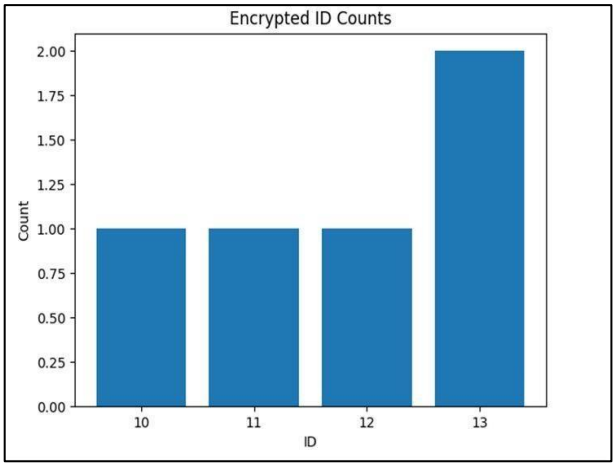
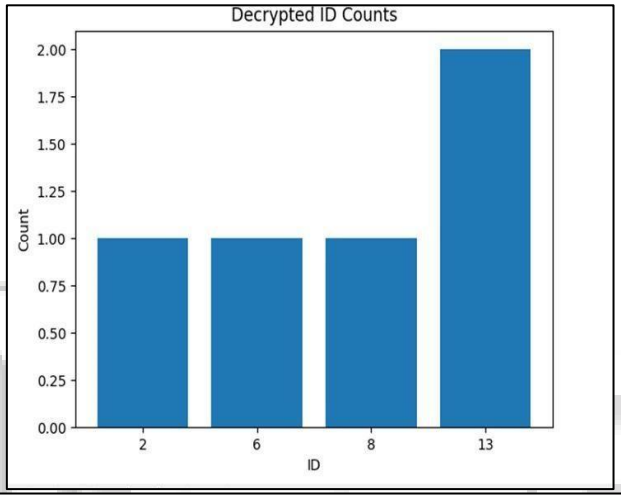


Fig. 9: (a) Medical User counts; (b) Encrypted ID counts



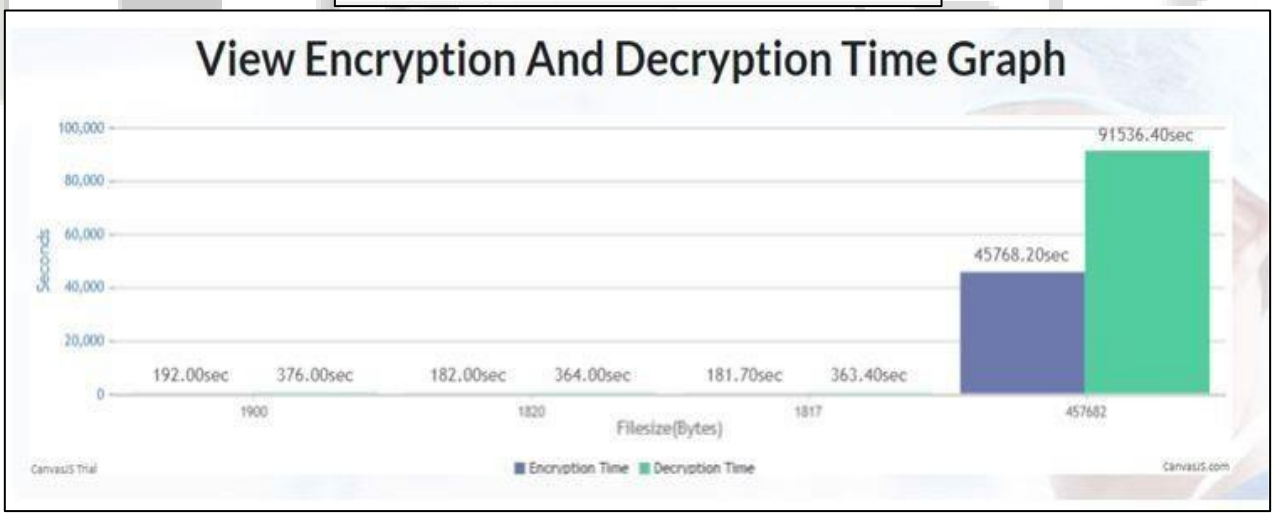


Fig.10: (a) Decrypted ID Counts; (b) Encryption and Decryption graph

VII. Conclusion

The proposed framework goes into considerable detail concerning the potential applications of blockchain technology for the storage and dissemination of EHR data in the healthcare industry. This approach overcame the limitations of the pre-existing supply chains and data models. The results of this paper's discussion of access control, the amount of time required to request and search data in an EHR blockchain, and feature comparison demonstrate that the suggestedsolution performs better than the current systems in every conceivable way.

The suggested methodology makes it abundantly clear that integrating blockchain into healthcare data management lowers the possibility of data breaches and erroneous invoicing while boosting privacy, security, and transparency. Blockchain-based data exchange also makes it possible for authorized third parties to share information securely and safely. The secure management of healthcare at all levels, including those of patients, doctors, hospitals,

insurance companies, and pharmaceutical companies, is ensured by this medical data science plan.

REFERENCES

[1] —Blockchain: Opportunities for health care — Deloitte US.‖ [Online].
[2] —Types of Blockchains amp; DLTs (Distributed Ledger Technologies).‖ [Online].
[3] W. J. Gordon and C. Catalini, —Blockchain Technology for Healthcare: Facilitating the Transition to Patient- Driven Interoperability,‖ Comput. Struct. Biotechnol. J., vol. 16, pp. 224–230, 2018.
[4] X. Zheng, A. Vieira, S. L. Marcos, Y. Aladro, and J. Ordieres-Mere´, —Activity-aware essential tremor evaluation using deep learning method based on acceleration data,‖ Park. Relat. Disord., 2018.
[5] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, —FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,‖ Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, 2018.
[6] I. Radanovic´ and R. Likic´, —Opportunities for Use of Blockchain Technology in Medicine,‖ Appl. Health Econ. Health Policy, 2018.
[7] H. Wang and Y. Song, —Secure Cloud- Based EHR System Using Attribute- Based Cryptosystem and Blockchain,‖ J. Med. Syst., vol. 42, no. 8, 2018.
[8] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, —Blockchain-Based Data Preservation System for Medical Data,‖ J. Med. Syst., vol. 42, no. 8, pp. 1–13, 2018.
[9] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, —MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain,‖ J. Med. Syst., vol. 42, no. 8, pp. 1–11, 2018.
[10] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, —Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,‖ IEEE CloudComput., vol. 5, no. 1, pp. 31–37, 2018.
[11] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, —How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational Concept,‖ J. Diabetes Sci. Technol., p. 193229681879028, 2018.
[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, —MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain,‖ IEEE Access, vol. 5, no. c, pp. 14757–14767, 2017.
[13] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, —A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval,‖ Comput. Struct. Biotechnol. J., p. pagerange, 2018.
[14] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, —Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,‖ J. Med. Syst., vol. 42,no. 7,pp. 1–7, 2018.
[15] — Blockchain: Opportunities for health care — Deloitte US.‖ [Online]. —Types of Blockchains amp; DLTs (Distributed Ledger Technologies).‖ [Online].
[16] W. J. Gordon and C. Catalini, —Blockchain Technology for Healthcare: Facilitating the Transition to Patient- Driven Interoperability,‖ Comput. Struct. Biotechnol. J., vol. 16, pp. 224–230, 2018.
[17] X. Zheng, A. Vieira, S. L. Marcos, Y. Aladro, and J. Ordieres-Mere´, —Activity-aware essential tremor evaluation using deep learning method based on acceleration data,‖ Park. Relat. Disord., 2018.
[18] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, —FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,‖ Comput. Struct. Biotechnol. J., vol. 16, pp. 267–278, 2018.
[19] I. Radanovic´ and R. Likic´, —Opportunities for Use of Blockchain Technology in Medicine,‖ Appl. Health Econ. Health Policy, 2018.
[20] H. Wang and Y. Song, —Secure Cloud- Based EHR System Using Attribute- Based Cryptosystem and Blockchain,‖ J. Med. Syst., vol. 42, no. 8, 2018.
[21] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, —Blockchain-Based Data Preservation System for Medical Data,‖ J. Med. Syst., vol. 42, no. 8, pp. 1–13, 2018.
[22] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, —MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain,‖ J. Med. Syst., vol. 42, no. 8, pp. 1–11, 2018.
[23] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, —Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,‖ IEEE CloudComput., vol. 5, no. 1, pp. 31–37, 2018.
[24] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, —How to Use Blockchain for Diabetes Health Care Data and Access Management: An Operational

