IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 June 2024, accepted 28 June 2024, date of publication 4 July 2024, date of current version 15 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3423714

RESEARCH ARTICLE

A Secure Medical Data Sharing Framework for Fight Against Pandemics Like Covid-19 by Using Public Blockchain

SEVAL CAPRAZ, (Member, IEEE), AND ADNAN OZSOY
Graduate School of Science and Engineering, Hacettepe University, 06800 Ankara, Turkey

Corresponding author: Seval Capraz (seval.capraz@hacettepe.edu.tr)

ABSTRACT The global impact of the COVID-19 pandemic was huge, and it showed that reporting and collecting accurate healthcare data are crucial operations for governments. Not only the test results but also the vaccination information of people should be shared correctly by trusted systems between countries. Now it is possible with the integration of new practices like blockchain and cryptology with the help of secure, transparent, and privacy-centric methods. There are a lot of recent studies focusing on blockchain usage in healthcare in literature. However, they still have flaws in granting full authorization to individuals, ensuring the security of personal information, speed, and scalability. They mostly use private or consortium blockchains. However, in a public blockchain, a system that everyone can participate in and follow provides more reliable information. At the same time, heavy and slow encryption techniques were used in the models proposed in the literature. Our study focuses on the usage of blockchain in combating pandemics by ensuring privacy and maintaining reliable medical data sharing during pandemics. The proposed system is implemented by leveraging public blockchain on Ethereum with smart contracts, IPFS for decentralized storage, and robust and fast encryption techniques like ChaCha20. In addition to existing techniques, the framework introduces innovative methods, such as storing encrypted keys alongside encrypted data in IPFS, which enhances security and scalability. We also eliminate the usage of doctors' private keys. The framework grants patient's full ownership of their medical data, aligning with GDPR requirements. Patients can grant or revoke access to their data, enhancing their control over personal information. The use of smart contracts to manage access rights ensures that only authorized parties can access the data, and patients can easily manage these permissions through a decentralized platform. We aim to implement a framework which is fast, easy to use and differs in terms of storing and sharing medical data with different encryption methods and protocols by using a public blockchain. We ensure novel management of COVID-19 medical records that are personal data.

INDEX TERMS Blockchain, distributed ledgers, cryptography, smart contracts, COVID-19, contact tracing, vaccine.

I. INTRODUCTION

The COVID-19 pandemic has underscored the importance of secure and efficient sharing of medical data. Historically, hospitals have maintained ownership of medical records for many years. The process of requesting a hospital to transfer these records can be time-consuming, often taking days, and in some cases, proves to be challenging, especially when attempting to transfer records across different countries. Emerging technologies such as blockchain present a transformative opportunity to address this trust deficit, enabling secure and precise sharing of medical information while ensuring robust anonymization for the protection of private data. Blockchain's capabilities in spreading accurate information, ensuring traceability for records, monitoring COVID-19 test results can help to combat pandemics. Blockchain technology offers a decentralized and secure alternative. Blockchain's inherent features of decentralization,

The associate editor coordinating the review of this manuscript and approving it for publication was S.K. Hafizul Islam.

immutability, and transparency can address challenges in healthcare data management, ensuring patient privacy and data integrity. In literature, blockchain solutions for healthcare have been proposed more and more in recent years. However, proposed methods use heavy cryptographic algorithms, cloud servers and doctors' signature in procedures which cause the system to slow down. While scalable, cloud solutions can become expensive with increasing data storage needs. They are still subject to the limitations of centralization. Adding more security layer or complexity decreases system performance much. Also, in some publications, the confidentiality of the data is not fully ensured. In addition to this, most publications use private or consortium blockchains to gain speed and scalability that makes registering the system centralized and difficult to track blockchain activities. Private chains have centralized control and governance, and they are exclusively utilized within a single organization. They are not proper for global usage. On the other hand, using public blockchain provides more trust and ease of usage.

Pandemic data like COVID-19 is simpler than other types of medical data since it is small and easy to store as json file. We can use public blockchains for medical data sharing of pandemic data with acceptable latency. This study explores the development of a secure and decentralized framework using public blockchain with strong encryption methods tailored for COVID-19 medical data sharing. There are many enhancements in this study for security and decentralization that are handled by blockchain, peer-to-peer storage IPFS and strong cryptography. The key features of our framework and main contributions are as follows:

- Firstly, because of the security of personal data, off-blockchain is used. Off-blockchain activities typically involve processes that are not recorded directly on the blockchain itself. It helps a lot with interoperability between different blockchain networks. InterPlanetary File System (IPFS) is used since it is a peer-to-peer decentralized file storage and retrieval system.
- Secondly, we tested the system on Ethereum with a Solidity smart contract. Ethereum is the most popular blockchain development environment among scientists. It is easy to use and provides security. This study uses Ethereum as a public blockchain. Any user can register the system as a patient and has full control over his/her medical data which is uploaded by hospitals.
- Thirdly, we used current cryptology algorithms proven to be powerful and fast. They are AES, ChaCha20 and RSA. We used them to create strong security in the fastest way. Our framework implements novel techniques, including the storage of encrypted keys alongside encrypted data in IPFS, which improves both security and scalability. This approach eliminates cloud server operations and doctors' signing process.
- Lastly, we designed an access protocol to grant access to data for users. Patients can grant or revoke access since the true owner of the data is patient. If the patient does not allow a hospital, they cannot decrypt the patient's medical data and read it as a plain text. We created a full system to ensure privacy.

In this study, proposing a stronger and faster alternative medical data sharing framework to fight against pandemics such as COVID-19 is aimed. For this purpose, we used Ethereum as a public blockchain. We created user interfaces with React for users. Our react client connects with smart contract via Web3 API. Fig. 1 shows the technologies used and Fig. 2 shows overall framework design. The proof-of-concept implementation and test data are given in a GitHub public project as well as installation guide.[1] The proposed framework contributes to the literature in terms of technology and method. Our main contributions are using strong and fast cryptology algorithms and designing a system in which data ownership is totally given to the personal data owner. A comprehensive examination of blockchain technology and its application in sharing medical data is presented within the context of strategies to combat pandemics.

II. RELATED WORKS

The emergence of Bitcoin in 2008 further popularized blockchain technology, with Nakamoto publishing a white paper [1] on Bitcoin in 2009 which has since inspired numerous applications in healthcare. Between 2013 and 2015, Vitalik Buterin conceptualized Ethereum, introducing features like smart contracts. Ethereum's development marked a significant moment in blockchain history, enabling the creation of decentralized applications. Ethereum stands out as the leading blockchain platform for executing smart contracts, utilizing the Turing-incomplete programming language Solidity. In this study, we used Ethereum platform for permissionless blockchain.

The literature on blockchain-based solutions for healthcare data management and sharing is extensive and diverse. There are many studies which use blockchain and IPFS to store medical data. In an early study, in 2018, Wang et al. [2] developed a framework on Ethereum with attribute-based encryption (ABE) methods. They use a secret key generator on a trusted system to use it for access control. They encrypt the file with AES encryption and store it on IPFS. Then the system encrypts the secret key and stores it on the blockchain. Requestors who meet the access criteria first decrypt the encrypted secret key then download the encrypted file from the IPFS. In our study, we keep the encrypted key in IPFS next to the encrypted data, not on the blockchain. This is important to keep block size small and for security. Our design makes it more scalable and secure.

In 2019, Luo et al. [3] advocated for blockchain's use in secure clinical data sharing. Xu et al. [4] proposed Healthchain that is another blockchain-based solution for medical data sharing. Their design is based on usage of two private blockchain. In 2020, Hasan et al. [5] presented a solution leveraging blockchain technology to create digital medical passports and immunity certificates for managing

[1] https://github.com/svlzx/PandemicBlockchain

COVID-19 information. In their approach, IPFS is used to store encrypted test results and all medical documents. The encrypted key is stored on a blockchain. The private key is sent to the receiver as an encrypted package. In our design, it eliminates password storage on the blockchain as explained in the following sections.

In 2020, Christodoulou et al. [6] introduced a health information exchange framework that leverages blockchain technology. Blockchain offers features like immutability and decentralization. To create a user-centric approach, they utilize smart contracts, granting data control to the owner. After encrypting the data, it's stored on a peer-to-peer (p2p) file storage system using IPFS Clusters. The blockchain stores the address of the data, while access control is managed through smart contracts. The researchers implemented and tested their proposed system on the Ethereum blockchain platform. They used doctors' public keys to encrypt the medical data. Patients use their private key to sign the hash of the encrypted data. This approach needs doctors' public and private keys. In our method we generate symmetric keys to encrypt and decrypt data, so we do not need private keys of doctors. Our design is simpler and more reliable.

In 2021, Vardhini et al. [7] explored electronic medical health records management using smart contracts on Hyperledger Fabric. They proposed using zero-knowledge proof to prove the owner of the data. Their proposed system is slow and not scalable. Panwar and Bhatnagar [8] presented another blockchain-based solution which uses cryptographic curve hash signature (BC-CCHS). Their solution is based on pre-shared private keys between patients and hospitals. This raises another problem: sharing private keys in a secure way. Qin et al. [9] introduced a secure method for storing and sharing electronic medical records related to strokes, utilizing a consortium blockchain. Most proposed studies rely on private or consortium blockchains. Our design is based on public blockchain with better security.

Additionally in 2021, Abouali et al. [10] introduced a blockchain framework for secured on-demand patient health records sharing. They used both doctors and patients' encryption keys with Ursulas. We are inspired by their re-encryption method during which healthcare entities encrypt personal health records and upload them to IPFS. We used their encryption method in a simple way and adopted our design. Hasan et al. [11] developed blockchain-enabled telehealth services using smart contracts. They used a permissioned Ethereum blockchain. Ricci et al. [12] conducted a systematic review on blockchains for COVID-19 contact tracing and vaccine support. They proposed usage of re-encryption keys to share medical data. Xu et al. [13] introduced BPDST, a blockchain-based approach for privacy-preserving data sharing on thin clients for health data, utilizing a consortium blockchain. They used consortium blockchain.

In 2022, Jain et al. [14] presented a detailed review of contributions to data management using blockchain techniques and implemented a full system with Ethereum. The technology behind the implementation is the same as us, however they do not use secure encryption. Kumar [15] addressed granular privacy approaches and scalable healthcare frameworks utilizing blockchain and IPFS technology. The Ethereum network employs the ECDSA algorithm for data encryption purposes. Within that study, the patient's data, along with a hash of corresponding data and the sender's signature, are all encompassed within the transaction. Abid et al. [16] presented NovidChain, a blockchain-powered platform designed to safeguard privacy while managing COVID-19 test and vaccine certificates. The proposed infrastructure of NovidChain relies on Ethereum permissioned blockchain (private blockchain).

In 2023, Sheeraz et al. [17] presented a blockchain system on Hyperledger Fabric for trustless healthcare data sharing. In their study, a private or permissioned blockchain is used and they do not encrypt the data before storing it to IPFS. Abdelgalil and Mejri [18] developed HealthBlock, a blockchain-based framework for collaborative sharing of healthcare data. Their approach to access control delegation relies on Indy and Hyperledger Fabric. Indy is a decentralized database system offering resources such as tools, libraries, and reusable elements to facilitate the establishment and utilization of autonomous digital identities. Lakhan et al. [19] presents a novel framework aimed at enhancing the efficiency, security, and scalability of healthcare applications within the Industrial Internet of Things (IIoT) paradigm. The framework uses a public blockchain to maintain data processing workflows across multiple computing nodes, ensuring data security and integrity. They use this approach for healthcare tasks across mobile, fog, and cloud nodes with Q-Learning and Deep Reinforcement Learning. Ahmad et al. [20] present a high-level design with three blockchain-based systems to assist governments and medical professionals in managing health emergencies more effectively. That study explains Ethereum, a public platform, offers restricted privacy for transactions and limited throughput, processing around twenty transactions per second. In contrast, private blockchain platforms are regarded as faster and more secure, capable of managing several thousand transactions per second, for instance Hyperledger can manage 2000 transactions per second. Reegu et al. [21] proposed usage of blockchain for healthcare to enable secure and decentralized medical data sharing based on EHR standards such as HIPAA and HL7. It is a literature review. They focus on interoperability, so the framework can run on either Ethereum or Hyperledger. Ghosh et al.

[22] reviewed the literature which uses blockchain for healthcare in 2018-2021. They listed the studies based on their approach. Studies have issues of performance and scalability, and lack of proof-of-concept. Wenhua et al. [23] reviewed the blockchain solutions on healthcare based on security issues. Adding more security layers to blockchain solutions increases energy costs and

TABLE 1. Evaluation of related works.

Study	Year	Platform/Technology	Pros/Cons
Wang et al. [2]	2018	Ethereum, IPFS	Encrypted files are stored on IPFS. The encryption key of the file is first encrypted by the ABE (Attribute-based encryption), then encrypted with the AES together with other information (file location hash) and stored on the blockchain.
Xu et al. [4]	2019	Two private blockchain, IPFS	Data duplication between two private blockchain to handle doctor and patient keys.
Hasan et al. [5]	2019	Ethereum, IPFS	Encrypt files using symmetric key and store to IPFS. The encrypted key is stored on a blockchain.
Christodoulou et al. [6]	2020	Ethereum, IPFS	Doctors' public keys to encrypt the data. Patients use their private key to sign the hash of the encrypted data.
Vardhini et al. [7]	2021	Hyperledger Fabric	Zero-knowledge proof is suggested. Lack of data encryption.
Panwar et al. [8]	2021	Hyperledger	Cryptographic curve hash signature (BC-CCHS). Pre-shared private keys between patients and hospitals.
Qin et al. [9]	2021	A consortium blockchain	Improved PBFT. There is no fine-grained access control.
Abouali et al. [10]	2021	A consortium blockchain on Ethereum, IPFS	Medical data is encrypted using NuCypher decentralized network. They use doctors' public key.
Hasan et al. [11]	2021	A permissioned blockchain on Ethereum, IPFS	Lack of data encryption.
Xu et al. [13]	2021	Hyperledger Fabric, Cloud storage	Medical data is signed by doctors, encrypted, and stored on cloud storage. The storage addresses are stored on blockchain. They use the DPOS consensus.
Kumar [15]	2022	A consortium blockchain on Ethereum, IPFS	Patient's data, along with a hash of corresponding data and the sender's signature, are within the transaction.
Abid et al. [16]	2022	A permissioned blockchain on Ethereum, IPFS	Medical data is encrypted and stored on IPFS. Healthcare providers sign the medical data. Therefore, they manage the data.
Sheeraz et al. [17]	2023	Hyperledger Fabric, IPFS	Lack of data encryption.
Abdelgalil et al. [18]	2023	Hyperledger Fabric, Hyperledger Indy, IPFS	Doctors have a role as verifier in the system. They provide scalability.
Lakhan et al. [19]	2023	Ethereum, Mobile Fog Cloud	Not support real-time healthcare applications and will incur overhead at different nodes.
Reegu et al. [21]	2023	Ethereum or Hyperledger, Document base database	Document-oriented databases. Identity attributes along with the hash of whole health data stored on chain.
Jafari et al. [27]	2024	Ethereum	Lack of data encryption.
Niranjana et al. [28]	2024	ChaCha20-Poly1305 encryption, cloud server	Storing encrypted data on blockchain.
Wahyudi et al. [29]	2024	Ethereum	Vaccine tracking.
Masood et al. [31]	2024	Ethereum	Vaccine tracking.
Wang et al. [33]	2024	Ethereum	Incremental updates without changing block.
Haque et al. [34],[35]	2024	Delegated Proof of Stake (DPoS) consensus	Scalable blockchain.

decreases performance. Behnaminia and Samet [24] reviewed patient tracking systems for Covid-19. They also emphasize the scalability and performance issues. In addition to this, Andrew et al.

[25] presented a survey about blockchain solutions for healthcare and they found out the performance of the proposed studies are low. Key generation causes a computational cost alongside costs of encryption methods.

In 2024, numerous studies highlighted the potential of blockchain technology to revolutionize healthcare. Akram et al. [26] investigated the benefits, challenges, and lessons learned from employing blockchain to improve food supply chains during the COVID-19 pandemic. They emphasized that an eco-friendly blockchain platform is needed that is energy efficient and sustainable. Jafari et al. [27] investigated the development of an immutable COVID-19 vaccination certificate utilizing blockchain technology. They used Ethereum and they stored patient information on smart contracts and blockchain. This approach has privacy problems. Niranjana et al. [28] suggested using blockchain-based Storj mechanism instead of IPFS for health data records. Storj network provides high security by dividing the data into pieces and distributing it to different nodes. They used ChaCha20-Poly1305 symmetric encryption before uploading to the cloud server. They increase the security by splitting files into 80 separate parts. To reconstruct the original file, 29 of these parts are needed. This mechanism provides a decentralized and secure storing system however it is slower than IPFS. Wahyudi et al. [29] introduced a mobile-based vaccine tracking system leveraging Ethereum blockchain and QR codes. Their data is not personal medical data, so their system does not concern privacy. Ishengoma [30] emphasized the potential of blockchain to tackle the challenges posed by the COVID-19 pandemic in African developing countries. Masood and Faridi [31] proposed an innovative blockchain-based system for vaccine tracking and certification on the Ethereum blockchain. Bisht et al. [32] conducted a comprehensive survey on using searchable encryption and blockchain for storing and sharing personal health records. According to their survey, establishing a universal standard for the format of personal health records (PHRs) is essential, as it would facilitate the sharing of PHRs between various medical institutions and third parties. Moreover, there is a need for searchable encryption (SE) schemes that support more complex queries beyond single keyword searches while ensuring PHR security. Additionally, SE schemes should utilize the benefits of parallel computation. Wang et al. [33] developed a blockchain-based medical data sharing scheme for incremental updates by maintaining privacy. Haque et al. [34] proposed a scalable blockchain framework for efficient IoT data management. They provide scalability with lightweight consensus like Delegated Proof of Stake (DPoS). In their another study [35], they presented a scalable EdgeIoT blockchain framework using EOSIO. They investigated scalable blockchain to exhibit low latency. In conclusion, Delegated Proof of Stake (DPoS) consensus is lightweight and scalable.

To sum up, these studies collectively highlight the growing interest and potential of blockchain in revolutionizing healthcare data management, security, privacy, and interoperability. According to Table 1, their designs are based mainly on off-chain storage and access control.

III. BENEFITS OF BLOCKCHAIN IN MEDICAL DATA SHARING

Tamper-resistant and immutable features can be better supported using ledger database, such as LedgerDB, VeDB or blockchain. While blockchain offers a fully decentralized and transparent database to manage data, LedgerDB provides a centralized yet immutable and auditable solution, and VeDB focuses on verifiable data integrity, potentially with varying levels of decentralization. Blockchain is more suitable for applications needing high transparency, decentralization, and trust without intermediaries.

Using a blockchain for medical data sharing offers several potential advantages, especially in terms of security, transparency, and control over personal information. First, data recorded on a blockchain is stored in a tamper-resistant and immutable ledger. Once information is added to the blockchain, it cannot be easily altered or deleted. This provides a high level of data integrity and protection against unauthorized modifications. Secondly, blockchain uses cryptographic techniques to secure data. Personal data can be encrypted, and access can be controlled through cryptographic keys, ensuring that only authorized parties can view and interact with the data. Thirdly, traditional centralized systems are vulnerable to data breaches, as a single point of failure can expose a large volume of sensitive information. Blockchain's decentralized nature distributes data across a network of nodes, reducing the risk associated with centralized databases. Moreover, blockchain's distributed architecture enhances data resilience. Even if some nodes in the network go offline or experience issues, the data remains accessible through other nodes, ensuring continuous availability. Lastly, users have greater control over their personal data. With blockchain, individuals can control access to their information, grant permissions, and revoke access as needed. This puts users in charge of who can access and use their data. Smart contracts on a blockchain can automate and enforce data usage agreements, ensuring that data is accessed and used in accordance with the user's preferences.

A smart contract serves as an automated agreement governed by code, which executes itself when specific conditions encoded within it are fulfilled. These contracts operate on blockchain networks like Ethereum, where they are stored immutably, ensuring their integrity. Ethereum provides a decentralized platform for executing smart contracts. In our framework, smart contracts govern access permissions, ensuring that only authorized individuals can access specific medical records. Ethereum's smart contracts govern access to COVID-19 medical records, providing a transparent and decentralized permission system. These contracts specify access rights, ensuring that only authorized entities can retrieve and analyze sensitive pandemic-related information. The details of the designed smart contract are given in the next sections.

IV. KEY COMPONENTS OF THE SYSTEM

Ethereum is a platform which serves as a modern blockchain. It serves as a community-driven technology underpinning the cryptocurrency known as ether (ETH), along with a myriad of applications available for immediate use. Ethereum stands out as the go-to platform for Web3 development due to its pioneering role in smart contracts, a large developer community, an established ecosystem, strong security and decentralization, interoperability standards, continuous improvement efforts, and widespread enterprise adoption. These factors make it a robust and versatile foundation for building decentralized applications and shaping the future of the internet.

By leveraging Ethereum and IPFS, we achieved a more secure, efficient, and patient-centered approach to data sharing. Ethereum's smart contracts can manage permissions and consent, while IPFS ensures that the actual data is stored

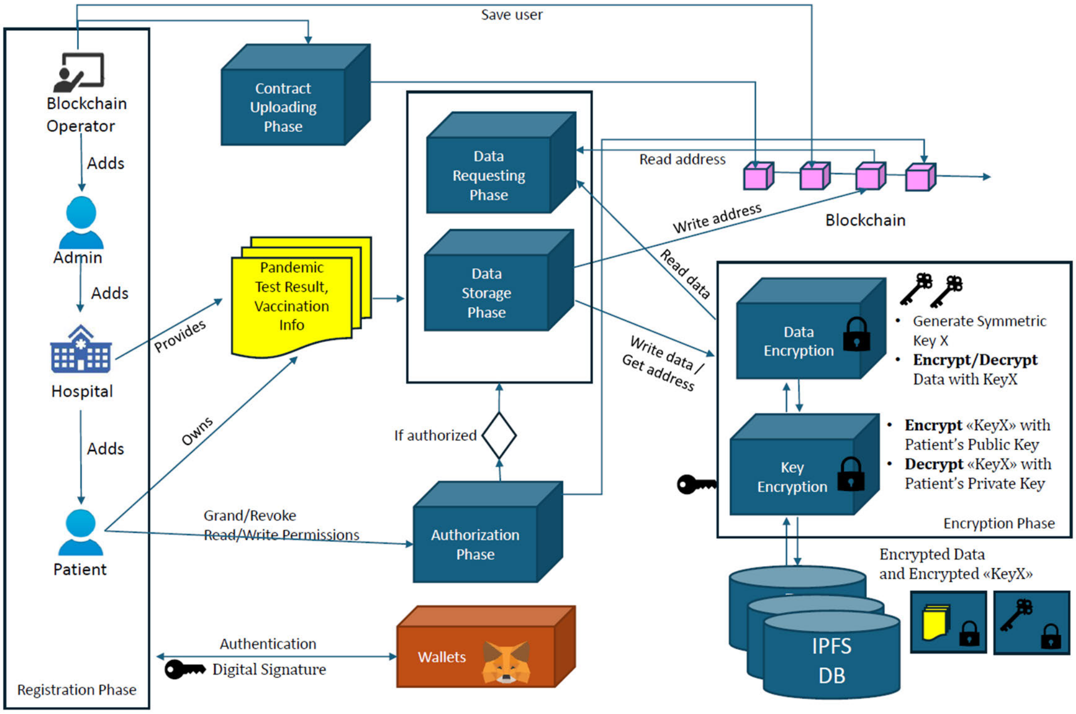


FIGURE 1. Overall system architecture.

securely and efficiently. IPFS allows for decentralized storage of medical data, distributing it across multiple nodes. This makes the system highly scalable, capable of handling large volumes of data without relying on centralized servers.

The system is designed on the Ethereum platform. To test the system, Solidity smart contract is developed to interact with a client software which is a ReactJS application using web3.js. We run a local blockchain network on Ganache and debug the smart contract using Ethereum Remix IDE, and MetaMask wallet to login the system. The client software also interacts with IPFS using Infura and ipfs-http-client. As encryption methods, we used different algorithms like AES and ChaCha20 which are implemented in CryptoJs and ChaCha NPM libraries. Technologies and tools used for Pandemic Blockchain are shown in Fig. 1.

When a patient undergoes a medical test, the resulting data is encrypted and stored on IPFS. A corresponding smart contract is created on the Ethereum blockchain, linking to the IPFS hash and specifying access permissions. Authorized hospitals query the smart contract, retrieving the IPFS hash. They use this hash to fetch the encrypted data from IPFS, decrypting it in the client application for analysis. Only authorized parties with the decryption keys can access the actual medical records. As shown in Fig. 2, there are several phases in this system. Fig. 3 and Fig. 4 show use cases of the system. The details of phases are given below.

A. REGISTRATION PHASE

First, users need to register to the system. Users interact with the Ethereum network using public and private key pairs. The private key, kept secret by the user, is crucial for authorizing transactions and accessing digital assets. Public keys, derived from private keys, serve as the public address for receiving funds. Every action in blockchain needs this digital signature process. There is one key pair for each user for digital signature: KeySignaturePrivate, KeySignaturePublic.

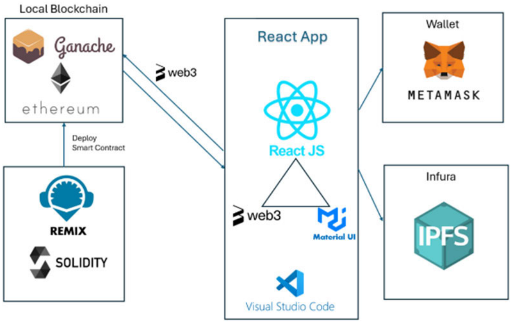


FIGURE 2. Technologies used for pandemic blockchain dApp.

We used digital wallets for storing KeySignaturePrivate of users. Storing users' private key in the wallet can be accomplished using MetaMask since it is a digital wallet and browser extension designed to empower users to engage with decentralized applications (DApps) and services built on blockchain networks directly through their web browsers.

MetaMask uses the industry-standard AES-256-GCM (Advanced Encryption Standard with a 256-bit key in Galois/Counter Mode) algorithm to encrypt private keys. AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. MetaMask

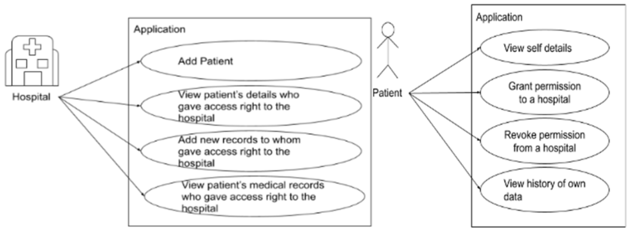

Hospital
Application
Add Patient
View patient's details who gave access right to the hospital
Add new records to whom gave access right to the hospital
View patient's medical records who gave access right to the hospital
Patient
Application
View self details
Grant permission to a hospital
Revoke permission from a hospital
View history of own data

FIGURE 3. User use cases: Hospital use cases; patient use cases.

derives an encryption key from the user's password using a key derivation function (KDF). This process ensures that the encryption key is not directly derived from the user's password but goes through a secure key derivation process. The private key is then encrypted using the derived encryption key and the AES-256-GCM algorithm. GCM mode provides authenticated encryption, ensuring the confidentiality and integrity of the encrypted data. The encrypted private key is stored locally on the user's device or browser. The encrypted private key can be decrypted later when needed, using the user's password to derive the encryption key.

In the system proposed, users need to be added to the system. Blockchain operators can add admin users. Admin users can add hospitals to the system. In this system, patients can be added by hospitals. The first record is saved by a hospital who adds the patient. Hospital information can be queried by anyone.

B. SMART CONTRACT UPLOADING PHASE

The second phase is smart contract uploading. A user who is the blockchain operator can upload the smart contract. Smart contract address is used by client software. Operator also handles the client software. It acts like a system administrator. Client software runs on a centralized server and provides user interfaces to interact with the smart contract by web3. The UML diagram of the smart contract is given in Fig. 5.

C. AUTHORIZATION PHASE

The patient should give "write" access right to the hospital before adding any record. So, the third phase is authorization. The authorization information is held in the smart contract and saved on blockchain. The access control of the medical data is managed by the owner of medical data. The owner of medical data is a patient according to GDPR. Therefore, patients can grant or revoke access rights. There are two types of access rights. One of them is "write" right. If a hospital has "write" right, they can store any record for the patient. The other right is "read" right. Anyone on the system can have "read" right. If the patient wants to grant access to read his/her history of records to someone, he/she needs to know the blockchain address of the requester.

D. DATA STORAGE PHASE

The medical data is stored on a different database rather than the blockchain itself. We stored the unique hash address of

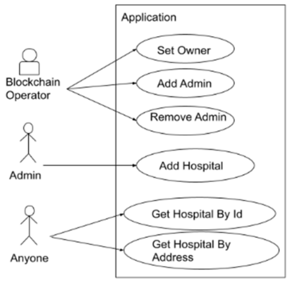


FIGURE 4. Blockchain operator use cases, admin use cases and queries for hospitals.

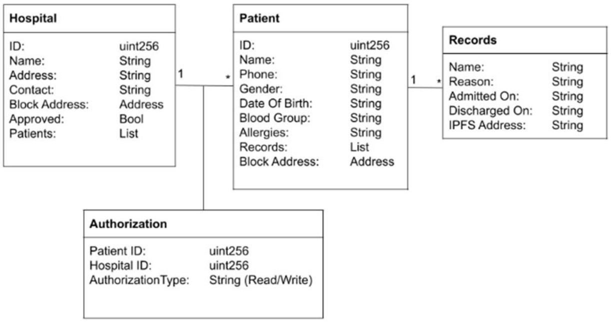


FIGURE 5. UML diagram of smart contract objects.

original data on the blockchain. The InterPlanetary File System (IPFS) is used for storing COVID-19 medical data in a decentralized manner. IPFS serves as a protocol and network architecture crafted to establish a decentralized approach for storing and exchanging hypermedia. This system operates as a distributed file system, allowing peers to share files directly with one another. It aims to address some of the limitations and challenges associated with centralized file storage and retrieval systems. IPFS provides a distributed file system that ensures data availability and fault tolerance. Each medical record is stored with a unique hash address on the IPFS network. Before storing the original data to the IPFS, it is encrypted. After encryption, its hash is calculated. The hash is signed with the digital signature of the patient. The encrypted original data and signed hash are concatenated and stored on IPFS. This method ensures data availability and resilience as well as security. To minimize the database storage size, we can use json format for medical data with metadata as follows:

```
{{
"nodeID":"1001",
"dataType":"covid19TestResult",
"affectedUserKey":"1132423",
"timestamp":"1475679929",
"location":"39.858425, 116.287148",
"result":"positive"
},
{
"nodeID":"1002",
"dataType":"covid19Vaccination",
“affectedUserKey”:”1132423”,
“timestamp”:”1706638069”,
“location”:”39.858425, 116.287148”,
“result”:”Biontech”
}}
```

In this metadata, dataType is diversifiable. We used two data types which are “covid19TestResult” and “covid19Vaccination”. The result is either “positive” or “negative” for “covid19TestResult” while result is vaccine type such as “Biontech” for “covid19Vaccination”. This important information can be held on IPFS with this simple json script. With this method, hospitals can record more than one result in a block by saving this information respectively in a json.

E. DATA ENCRYPTION PHASE

Hospitals that want to write the records must send requests to the patient. Patient grants access with “write” right. COVID-19 medical data is encrypted before being stored on IPFS and decrypted only when accessed by authorized parties. This ensures end-to-end security and privacy for patients. In other words, it ensures that patient privacy is maintained while allowing efficient data sharing among healthcare providers. The encryption is done by using one of the symmetric key ciphers that can be AES or ChaCha. The symmetric keys are generated by the system on local Hospitals. The generated symmetric key, called Key X, is encrypted by using the patient’s public key with an asymmetric cipher such as RSA or ELGamal. After encryption, both encrypted medical data and encrypted Key X are stored on IPFS. The encryption process can be seen in Fig. 6.

Hospitals that want to read the records must send requests to the patient too. Patient grants access with “read” right. If a hospital has “read” right, it can send a request to the patient to read the record. Patient decrypts its symmetric key “Key X” of the encrypted data after the system gets from IPFS. Then the patient sends Key X to the hospital. The original data can be read by hospitals by decrypting the data with Key X. The decryption process can be seen in Fig. 7.

As a symmetric key stream cipher, we chose **ChaCha20** in ChaCha NPM library. It was designed to provide a secure and efficient alternative to existing encryption algorithms. It is a good choice for encryption and decryption of medical data. One private key to encrypt/decrypt the data is needed since it is symmetrical: Key X. Patients use their private key to decrypt the symmetrical Key X. The system asks the patient for their private key. After entering their private key, the system decrypts the Key X and sends it to the requestor.

ChaCha is a type of stream cipher, which means it encrypts data one bit or byte at a time, in contrast to block ciphers that operate on fixed-size blocks of data [36]. It generates a keystream. The algorithm uses this keystream to XOR with plaintext to produce the ciphertext. The original ChaCha cipher is known as ChaCha20, which uses a 20-round version of the ChaCha algorithm. Additionally, there is a 12-round variant called ChaCha12. ChaCha is often used in conjunction with the Poly1305 message authentication code (ChaCha20-Poly1305), providing a secure and efficient authenticated encryption scheme. It is known for its speed and efficiency, making it suitable for use in situations where quick encryption and decryption are crucial, such as in real-time communication protocols. Overall, ChaCha is a well-regarded stream cipher that provides a good balance of security, simplicity, and speed, making it a suitable choice in medical data management.

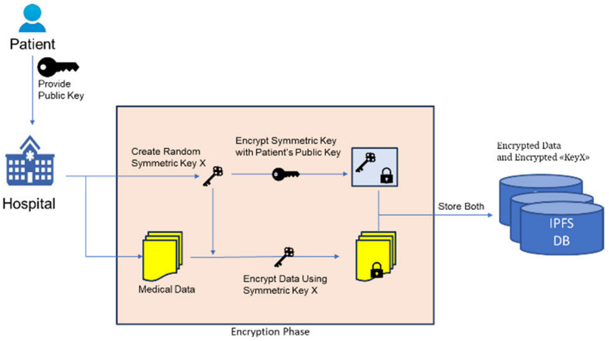


FIGURE 6. Encryption process.

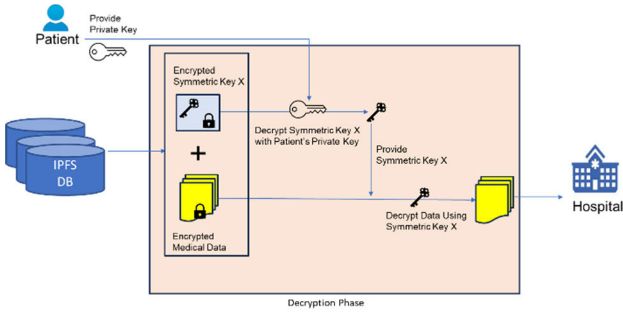


FIGURE 7. Decryption process.

As an asymmetric encryption, we chose **RSA** which is the most popular one among public key ciphers. Factoring the product of two large prime numbers ($n = p * q$) into its prime factors is difficult. The security of RSA relies on this principle. If factoring remains computationally infeasible for sufficiently large key sizes, RSA encryption provides a secure means of communication. RSA is commonly used for securing sensitive data, digital signatures, and key exchange protocols in various applications such as secure email communication, online banking, and the implementation of secure web connections (HTTPS).

F. DATA REQUESTING PHASE

Authorized hospitals query the smart contract for patients’ history, retrieving the IPFS hash address. The authorization list is stored on smart contracts. If a user or hospital is authorized to reach someone’s medical data, they can reach the hash address of it. They use this hash to fetch the encrypted data from IPFS, decrypting it locally for analysis with data encryption phase. Only authorized parties with the decryption keys can access the actual medical records. Patients use their private key to decrypt the generated symmetric key that is used for encryption of medical data. Decrypted generated symmetric key is stored on IPFS alongside encrypted medical data. The decryption process can be seen in Fig. 7.

V. CHALLENGES AND CONSIDERATIONS

Blockchain and usage of cryptography provide many benefits for sharing medical data. While the potential benefits are significant, it's crucial to note that implementing blockchain for medical data sharing requires careful consideration of legal, regulatory, and privacy concerns. Additionally, usability, scalability, and interoperability challenges must be addressed for widespread adoption.

A. SECURITY

The decentralized nature of the blockchain and encryption of medical data enhance security of COVID-19 medical data, reducing the risk of unauthorized access and ensuring data integrity. First, the system relies on blockchain's digital signature for authentication and hashing design. Secondly, we store the authorized hospital address list for each patient on the smart contract. Also, we encrypt medical data with a generated symmetric key. Then we encrypt the generated symmetric key with the public key of the user. This is also proof of who owns the data. Only patients can decrypt the key. If they want to give access to the hospital, they give the symmetric key to the hospital. Hospitals can decrypt medical data by using symmetric keys. This design ensures the security of personal data. Unauthorized users cannot read the data.

There are two encryption processes for storing each medical record, as well as two decryption processes for retrieval of each medical record. These are bottlenecks of personal data sharing. For encryption, AES or ChaCha20 can be used for symmetric key encryption. Both are good options. AES can be faster with hardware support, but pure-software implementations of ChaCha20 are almost always fast and constant-time. **ChaCha20** is consistently faster than AES as shown in Fig. 8 and we used ChaCha20 in the final design. As an asymmetric encryption, we chose RSA which is the most popular one among public key ciphers. They are industry standards which NIST approved for their strong security.

Ethereum primarily uses the Elliptic Curve Digital Signature Algorithm (ECDSA) for ensuring the security and integrity of transactions. ECDSA is a widely adopted public-key cryptography algorithm that is used to create digital signatures. The public key is derived from the private key using elliptic curve cryptography. In the context of Ethereum, ECDSA is employed to generate and verify digital signatures associated with transactions.

Cryptographic hashes are functions that produce always in fixed-length value for any arbitrary input. Keccak-256 hash function contributes to the overall security and reliability of Ethereum's blockchain. SHA-256 is approximately 50% faster than Keccak-256. However, the SHA-256 is weaker than Keccak-256. The Keccak-256 was chosen by Ethereum since it is much stronger compared to SHA-256. IPFS primarily uses the SHA-256 hash algorithm by default. This algorithm is utilized to generate unique identifiers for content stored on the IPFS network. IPFS supports many other hashing algorithms.

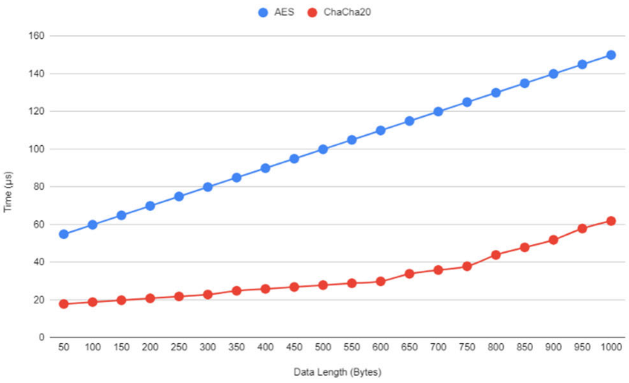


FIGURE 8. **Performance comparison of AES and ChaCha20.**

B. PRIVACY

Patients retain control over their COVID-19 data, granting permission selectively. The use of encryption ensures that sensitive information remains confidential. Robust encryption techniques safeguard sensitive pandemic-related information. The smart contract holds the hospitals' addresses that are allowed to read or write. Users can revoke these access rights. Users can also delete the original data from IPFS. If a user deletes their record, the record on blockchain shows only an empty storage address. It becomes a dummy record. None of the records on blockchain can be deleted. They are permanent in history. However, the off-chain design allows us to delete original data. This is a necessity for regulations like GDPR, HIPAA and HL7. Adherence to regulatory standards, including those specific to COVID-19 data, is crucial to ensure legal compliance and ethical handling of pandemic-related information. Ethereum provides transparent and auditable trails of who accessed or modified the data, which is crucial for compliance with regulations.

It is essential for medical data to prevent data from being shared without the consent of the real owner, to ensure data ownership and to take precautions against possible abuse. This includes the risk of data breaches, unauthorized access, or even malicious use of the data for purposes such as discrimination or blackmail. Implementing robust security measures and encryption protocols is essential for safeguarding patient data and preventing misuse. By using smart contracts in the blockchain, we give data ownership to the real owner. By encrypting the data while it is stored outside the blockchain, we prevent the data from being shared without the consent of the real owner. Because only the real owner needs to approve the data stored outside to be decrypted.

In the context of medical data storage systems, robust cryptographic systems within the blockchain are imperative to protect user rights, though an optimal solution is yet to be identified.

C. INTEROPERABILITY

The framework supports interoperability among healthcare providers, fostering a more cohesive and efficient healthcare ecosystem, and facilitating collaborative efforts to combat the spread of COVID-19. We used Ethereum with Web3.0. However, we can change the blockchain easily thanks to Web3.0. The data on IPFS can be transferred to another database easily. Also, more different databases and blockchains can work together with the proposed framework. Concerning data privacy and compliance with international healthcare standards. There will be no problems with data privacy and compliance with international health standards. Because we do not keep people's medical data on the blockchain. We no longer need to keep people's national identification numbers because, thanks to our encryption method, they will have their own private passwords in their wallets where they keep their cryptocurrency passwords, and they will be able to prove that they have the password without ever showing this information to the other party.

D. SCALABILITY

As the number of medical records grows, scalability becomes a concern. Design considerations should address potential bottlenecks and ensure efficient data retrieval during the ongoing pandemic. We chose Ethereum over Hyperledger Fabric for implementation. Transaction Per Second (TPS) metric is used to compute the number of transactions processed and recorded on the Blockchain per second. Ethereum provides 20 transactions per second while Hyperledger Fabric provides 2000 transactions per second. Hyperledger Fabric is designed with scalability in mind and is a permissioned blockchain framework developed by the Linux Foundation and is specifically aimed at enterprise-level applications. On the other hand, Ethereum has faced scalability challenges, but several initiatives and upgrades have been planned or implemented to address these issues. The biggest motivation of Ethereum is that it is public and has a great community behind it. It's important to note that achieving scalability in a blockchain network depends on various factors such as the big community behind it, network design, hardware infrastructure, and the specific use case. While blockchain systems provide the tools and features to build scalable solutions, the implementation details and configurations play a crucial role in achieving optimal scalability for a particular deployment.

On the other hand, Ethereum presently relies on a Proof of Work consensus mechanism, which consumes a substantial amount of energy. Expanding to accommodate millions of users would greatly increase energy usage, leading to significant environmental and sustainability issues. With Ethereum 2.0, transitioning to PoS will reduce energy consumption and potentially increase the network's scalability. Under PoS, validators need far fewer resources than miners in PoW. This significantly cuts down on electricity usage and diminishes the necessity for specialized, resource-heavy hardware.

Ethereum 2.0 seeks to improve scalability through sharding, which breaks the network into smaller, more manageable sections. This boosts transaction throughput and lowers the energy cost per transaction, enhancing overall resource efficiency. Continuous enhancements and optimizations in Ethereum's protocols ensure efficient network operation, focusing on reducing computational demands and increasing transaction processing efficiency. Currently, Ethereum's inherent scalability limitations threaten the system's ability to efficiently handle a large volume of transactions. Reliance on Ethereum's public network could result in congestion and delays, impacting the system's performance.

There are potential solutions for Ethereum's scalability issues like layer-2 scaling solutions, sharding or transitioning to more scalable blockchain platforms. First, layer-2 scaling solutions can be applied. Examples of layer-2 scaling solutions are rollups that process transactions off-chain and then post the transaction data on-chain, state channels that allow users to conduct multiple transactions off-chain, with only the initial and final states being recorded on-chain and plasma framework that allows the creation of child blockchains that run alongside the main Ethereum chain. Secondly, splitting the Ethereum blockchain into smaller, more manageable pieces can be applied. This process is called Sharding. This method effectively increases the network's capability by allowing simultaneous processing, thereby greatly improving scalability. Thirdly, we can transition to more scalable blockchain platforms:

- Polkadot enables the simultaneous operation of multiple blockchains (parachains) and seamless communication between them. Its collaborative security approach and cross-chain capabilities position it as a potential substitute for Ethereum.
- Binance Smart Chain (BSC) is recognized for its elevated throughput and minimal transaction costs. It employs a consensus mechanism termed Proof of Staked Authority (PoSA), combining features from Proof of Stake (PoS) and Proof of Authority (PoA) to facilitate rapid and cost-effective transactions.
- Cardano has scalability via its Ouroboros Proof of Stake (PoS) protocol, crafted for superior throughput and energy conservation. Its stratified structure distinguishes the settlement and computation layers, refining overall performance.

We can use hybrid solutions to handle scalability issues of Ethereum. Sidechains are independent blockchains that run parallel to the Ethereum mainnet. They can have their own consensus mechanisms and provide a way to offload transactions from the main chain. Users can transfer assets between the main chain and sidechains as needed. Lastly, Protocols like Cosmos and Polkadot enable interoperability between different blockchains, allowing Ethereum to offload some of its traffic to other chains without sacrificing functionality or security. By utilizing these solutions, Ethereum can address its present scalability challenges.

E. PERFORMANCE OF SMART CONTRACT

Computation costs of decentralized applications (dApps), particularly on platforms like Ethereum, refer to the expenses associated with executing operations on the blockchain. These costs are typically measured in terms of gas fees. A smart contract consumes gas when it runs on Ethereum. "Gwei" is a denomination of the cryptocurrency Ether (ETH), which is used on the Ethereum blockchain. It is the smallest unit of Ether, like how "wei" is the smallest unit of Ethereum. One Ether (ETH) is equal to 1,000,000,000 (one billion) Gwei. Gwei is commonly used to measure the cost of gas, which is the fee required for executing transactions or smart contracts on the Ethereum network. Transactions on Ethereum are typically priced in Gwei per unit of gas, with higher gas prices indicating faster transaction processing times. The gas costs of the smart contract are given in Table 2. Gas price is accepted 60 Gwei which is the average of the last six months of 2023. In January 2024, 1 Ether was 2500 USD in crypto market. It is one of expensive cryptocurrencies which causes a bottleneck for global usage of dApps.

According to Table 2, "contract create" phase costs 671.79 USD. This is a one-time expense. Adding a patient costs 47.74 USD. Granting access rights costs 6.73 USD, while revoking access rights costs 4.17 USD. Each user needs to grant access rights to each hospital when the hospital needs to write or read the patient's history. Adding a new record for a patient costs 24.91 USD.

The costs depend on the market prices of Ether. The costs are not bound to the user record sizes. This allows lower costs. Implementing the framework on a public blockchain like Ethereum incurs substantial costs, especially for creating contracts and managing transactions. There are high costs associated with gas fees, which could hinder widespread adoption.

TABLE 2. Smart contract cost test (Gas Price = 60 GWEI, 1 ETHER = 2500 USD).

Function	Gas Used	Actual Cost (Ether)	USD
Contract Create	4478617	0.268717020	671.7926
addAdmin	47943	0.002876580	7.1915
addHospital	230843	0.013850580	34.6265
addPatient	318317	0.019099020	47.7476
addAuth	44896	0.002693760	6.7344
revokeAuth	27814	0.001668840	4.1721
addRecord	166129	0.009967740	24.9194
getHospitalByAddress	0	0	0
getPatientDetails	0	0	0

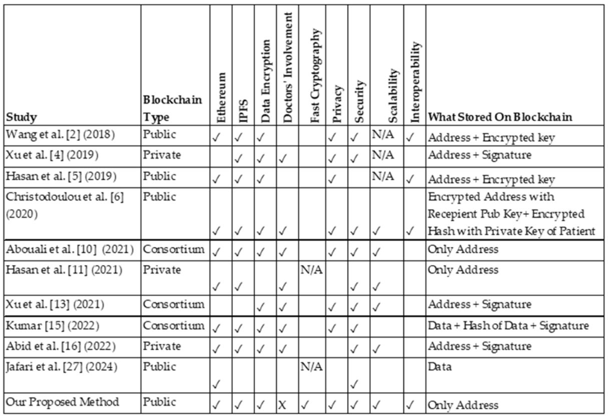
F. SOCIAL IMPACT

Beyond these technical considerations, the broader social impact of implementing blockchain for medical data sharing is subject to discussion. Blockchain can facilitate secure and efficient sharing of medical records between healthcare providers, leading to better coordination of care and faster diagnosis and treatment. Moreover, blockchain can empower patients by granting them greater control over their health data, enabling them to securely share it with their chosen providers. Implementation of such a system makes the lives of people easier, especially in areas with inadequate resources or high risk. Handling large volumes of data in central systems can lead to performance bottlenecks and high costs. Instead of setting up a central system to store medical data and allocating resources for it, they can connect directly to this ready-made decentralized system and start sharing data. In areas with high pandemic risk, this system helps prevent the spread of the pandemic as it reduces face-to-face contact. The existence of such a system has a positive social impact on society.

VI. RESULTS

The integration of Ethereum and IPFS for medical data sharing offers a compelling alternative to existing solutions, addressing critical issues of security, scalability, interoperability, and cost-efficiency. By leveraging these advanced technologies, healthcare providers can achieve a more secure, efficient, and patient-centric approach to managing medical data, ultimately leading to better healthcare outcomes. Our proposed framework has significant advantages over existing centralized and traditional solutions. Our framework uses ChaCha20 encryption which is faster than AES. Decentralized solutions proposed in literature uses IPFS too. The comparison of the proposed solution with existing methods in terms of privacy, security, scalability, interoperability, and cost-efficiency is given in Table 3.

TABLE 3. Comparison of the proposed solution with existing methods.



Study	Blockchain Type	Ethereum	IPFS	Data Encryption	Doctors' Involvement	Fast Cryptography	Privacy	Security	Scalability	Interoperability	What Stored On Blockchain
Wang et al. [2] (2018)	Public	✓	✓	✓			✓	✓	N/A	✓	Address + Encrypted key
Xu et al. [4] (2019)	Private		✓	✓	✓		✓	✓	N/A		Address + Signature
Hasan et al. [5] (2019)	Public	✓	✓	✓			✓		N/A	✓	Address + Encrypted key
Christodoulou et al. [6] (2020)	Public	✓	✓	✓	✓		✓	✓	✓	✓	Encrypted Address with Recepient Pub Key+ Encrypted Hash with Private Key of Patient
Abouali et al. [10] (2021)	Consortium	✓	✓	✓	✓		✓	✓	✓		Only Address
Hasan et al. [11] (2021)	Private	✓	✓		✓	N/A		✓	✓		Only Address
Xu et al. [13] (2021)	Consortium			✓	✓		✓	✓	✓		Address + Signature
Kumar [15] (2022)	Consortium	✓	✓	✓	✓		✓	✓			Data + Hash of Data + Signature
Abid et al. [16] (2022)	Private	✓	✓	✓	✓			✓	✓		Address + Signature
Jafari et al. [27] (2024)	Public	✓				N/A		✓			Data
Our Proposed Method	Public	✓	✓	✓	X	✓	✓	✓	✓	✓	Only Address

In a pandemic, real-time access to medical data and sharing of data are crucial for timely decision-making. Quick response times allow healthcare providers, researchers, and public health officials to rapidly obtain current information on infection rates, patient records, and resource availability. Latency time starts from encryption, continues with storing to IPFS or cloud and ends before block creation. Block creation also takes time since block creation always took

15 sec on Ethereum because of proof of work. As the number of requests and the amount of data increases, the time cost increases. We need a system which rapidly responds to a pandemic situation. The advantages of our proposed framework are its speed, its faster and stronger cryptography which ensures privacy and usage of public blockchain.

Our proposed framework provides overall better performance than existing solutions. We compared the framework with other studies which use Ethereum blockchain and off-storage like IPFS. We ensure privacy and security with cryptographic methods. We claim our proposed algorithm is scalable for a few reasons. First, our data is minimized, so computation costs will be lower. Reading and writing operations in IPFS exhibit excellent performance regarding latency and response time, as 1 MB of data can be processed within 100 milliseconds. Time consuming activities are cryptographic key generation and encryption. So, we did not use heavy cryptographic methods. Secondly, we use Ethereum which is transitioning to scalable Ethereum 2.0. We can also apply scalable solutions which we discussed in previous section V-D. Scalability. We claim our proposed method is interoperable because off-chain data addresses can be transferred to any other blockchain easily from a public blockchain. In our proposed framework, cost efficiency is provided by eliminating cloud servers, doctors' signature procedure and using fast cryptography.

Our framework is better because it combines advanced scalability, enhanced security, and cost-efficiency. It uses Ethereum for secure transactions and IPFS for decentralized storage. This ensures real-time data access and integrity while keeping costs low. Unlike centralized systems, it protects against data breaches and single points of failure. It is a resilient solution for critical applications. Our framework also integrates easily with existing systems, making it adaptable and future-proof. This comprehensive approach overcomes the limitations of other frameworks and places us at the forefront of innovation in medical data sharing applications for pandemic data like COVID-19.

VII. CONCLUSION

The global fight against a deadly pandemic is a collective effort that requires leveraging all available technologies to halt or slow its spread. COVID-19 has exposed a critical issue – the lack of fluidity in health data. Blockchain, an impactful and revolutionary technology with proven applications like Bitcoin and Ethereum as alternative financial systems, can play a pivotal role. It offers distinct advantages such as bypassing third-party verifications, ensuring secure and private data sharing, and outperforming traditional databases in terms of security and efficiency. We used recent technologies and implemented a new framework for medical data sharing, specifically Covid-19 data. We used Ethereum public blockchain for running our smart contract and IPFS for storing medical data. In the literature, they usually use private or consortium blockchains. Using a public blockchain, not only do we ensure transparency and security, but also any user can participate easily. We used an existing encryption method and proposed a new decryption method for the data. Our decryption method is simpler, faster, and more efficient way than proposed methods in literature since they use mostly data cloud and doctors' signature. So, eliminating cloud server usage, complex cryptographic algorithms and the process of doctors' signature speeds up the overall system. In addition to this, usage of ChaCha20 algorithm accelerated the process because it is faster than AES algorithm. We are the first in literature to use ChaCha20 and compare it with AES for medical data sharing purposes. On the other hand, there are disadvantages of this framework based on technology and non-technical users. Ethereum can be a problem for scalability, so we can use another specialized blockchain platform which is open for everyone to join for storing and sharing pandemic data. The other problem can be non-technical users who have problems interacting with digital wallets and decentralized application websites. Due to these problems, it may be difficult to use worldwide for now. However, if we see this framework as a starting point, as technology advances, this idea will mature and be used in the next pandemic. In future, we can use scalable solutions for Ethereum like sharding and we can improve security by adding more security layers. To sum up, we found a new way to store and share medical data which is fast and secure. As blockchain technology continues to mature, its applications in healthcare are poised to revolutionize the industry, placing control over sensitive medical information back into the hands of patients while ensuring the highest standards of security and privacy.

REFERENCES

[1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jun. 3, 2024. [Online]. Available: http://www.bitcoin.org

[2] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[3] Y. Luo, H. Jin, and P. Li, "A blockchain future for secure clinical data sharing: A position paper," in *Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Netw. Function Virtualization*, Mar. 2019, pp. 23–27, doi: 10.1145/3309194.3309198.

[4] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019, doi: 10.1109/JIOT.2019.2923525.

[5] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020, doi: 10.1109/ACCESS.2020.3043350. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9286584

[6] K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, "Health information exchange with blockchain amid COVID-19-like pandemics," in *Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2020, pp. 412–417, doi: 10.1109/DCOSS49796.2020.00071.

[7] B. Vardhini, S. N. Dass, R. Sahana, and R. Chinnaiyan, "A blockchain based electronic medical health records framework using smart contracts," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2021, pp. 1–4, doi: 10.1109/ICCCI50826.2021.9402689.

[8] A. Panwar and V. Bhatnagar, "A cognitive approach for blockchain-based cryptographic curve hash signature (BC-CCHS) technique to secure healthcare data in data lake," *Soft Comput.*, pp. 1–15, Nov. 2021, doi: 10.1007/s00500-021-06513-7. [Online]. Available: https://link.springer.com/article/10.1007/s00500-021-06513-7

[9] Q. Qin, B. Jin, and Y. Liu, "A secure storage and sharing scheme of stroke electronic medical records based on consortium blockchain," *BioMed Res. Int.*, vol. 2021, pp. 1–14, Feb. 2021, doi: 10.1155/2021/6676171.

[10] M. Abouali, K. Sharma, O. Ajayi, and T. Saadawi, "Blockchain framework for secured on-demand patient health records sharing," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf.*, Dec. 2021, pp. 35–40.

[11] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-enabled telehealth services using smart contracts," *IEEE Access*, vol. 9, pp. 151944–151959, 2021, doi: 10.1109/ACCESS.2021.3126025.

[12] L. Ricci, D. D. F. Maesa, A. Favenza, and E. Ferro, "Blockchains for COVID-19 contact tracing and vaccine support: A systematic review," *IEEE Access*, vol. 9, pp. 37936–37950, 2021, doi: 10.1109/ACCESS.2021.3063152.

[13] L. Xu, M. Lin, Y. Feng, and Y. Sun, "BPDST: Blockchain-based privacy-preserving data sharing on thin client for electronic medical records," *J. Comput. Inf. Technol.*, vol. 29, no. 4, pp. 235–250, Dec. 2022, doi: 10.20532/cit.2021.1005412.

[14] M. Jain, D. Pandey, and K. K. Sharma, "A granular approach to secure the privacy of electronic health records through blockchain technology," *Int. J. Distrib. Syst. Technol.*, vol. 13, no. 8, pp. 1–20, Aug. 2022, doi: 10.4018/ijdst.307899.

[15] R. Kumar, "Scalable inter-operable and secure healthcare framework for sharing patient medical report using blockchain and IPFS technology," Oct. 2022, doi: 10.21203/rs.3.rs-2115239/v1. [Online]. Available: https://www.researchsquare.com/article/rs-2115239/v1

[16] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," in *Software—Practice and Experience*. Hoboken, NJ, USA: Wiley, Apr. 2022, pp. 841–867, doi: 10.1002/spe.2983.

[17] M. M. Sheeraz, M. A. I. Mozumder, M. O. Khan, M. U. Abid, M.-I. Joo, and H.-C. Kim, "Blockchain system for trustless healthcare data sharing with hyperledger fabric in action," in *Proc. 25th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2023, pp. 437–440, doi: 10.23919/ICACT56868.2023.10079423.

[18] L. Abdelgalil and M. Mejri, "HealthBlock: A framework for a collaborative sharing of electronic health records based on blockchain," *Future Internet*, vol. 15, no. 3, p. 87, Feb. 2023, doi: 10.3390/fi15030087.

[19] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, "DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system," *Sci. Rep.*, vol. 13, no. 1, p. 4124, Mar. 2023, doi: 10.1038/s41598-023-29170-2.

[20] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "Blockchain and COVID-19 pandemic: Applications and challenges," *Cluster Comput.*, vol. 26, no. 4, pp. 2383–2408, Aug. 01, 2023, doi: 10.1007/s10586-023-04009-7.

[21] F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, R. G. Sonkamble, and R. A. Dziyauddin, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," *Sustainability*, vol. 15, no. 8, p. 6337, Apr. 2023, doi: 10.3390/su15086337.

[22] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain application in healthcare systems: A review," *Systems*, vol. 11, no. 1, p. 38, Jan. 2023, doi: 10.3390/systems11010038.

[23] Z. Wenhua, F. Qamar, T.-A.-N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain technology: Security issues, healthcare applications, challenges and future trends," *Electronics*, vol. 12, no. 3, p. 546, Jan. 2023, doi: 10.3390/electronics12030546.

[24] F. Behnaminia and S. Samet. *Blockchain Technology Applications in Patient Tracking Systems Regarding Privacy-Preserving Concerns and COVID-19 Pandemic*. [Online]. Available: https://www.researchgate.net/publication/362053375

[25] J. Andrew, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, Jun. 2023, Art. no. 103633, doi: 10.1016/j.jnca.2023.103633.

[26] M. W. Akram, N. Akram, F. Shahzad, K. U. Rehman, and S. Andleeb, "Blockchain technology in a crisis: Advantages, challenges, and lessons learned for enhancing food supply chains during the COVID-19 pandemic," *J. Cleaner Prod.*, vol. 434, Jan. 2024, Art. no. 140034, doi: 10.1016/j.jclepro.2023.140034.

[27] A. M. H. Jafari, R. K. Patchmuthu, and S. T. H. Tajuddin, "Immutable COVID-19 vaccination certificate using blockchain," *Proc. Comput. Sci.*, vol. 233, pp. 194–203, Jan. 2024, doi: 10.1016/j.procs.2024.03.209.

[28] J. Niranjana, E. Daniel, S. Durga, and V. Kathiresan, "Enhancing storage efficiency for health data records through block chain-based storj mechanism," in *Proc. 3rd Int. Conf. Intell. Techn. Control, Optim. Signal Process.*, May 2024, pp. 1–7, doi: 10.1109/incos59338.2024.10527538.

[29] I. Wahyudi, P. Sukarno, and A. A. Wardana, "Mobile-based vaccine tracking system using Ethereum blockchain and QR code," in *Proc. Int. Conf. Artif. Intell., Comput., Data Sci. Appl. (ACDSA)*, Feb. 2024, pp. 1–6, doi: 10.1109/acdsa59508.2024.10467308.

[30] F. Ishengoma, "The potential of blockchain technology in addressing the challenges posed by the COVID-19 pandemic in African developing countries," *Israa Univ. J. Appl. Sci.*, vol. 8, no. 1, pp. 84–108, 2024, doi: 10.5281/zenodo.10646522.

[31] F. Masood and A. R. Faridi, "Developing a novel blockchain-based vaccine tracking and certificate system: An end-to-end approach," *Peer-Peer Netw. Appl.*, vol. 17, no. 3, pp. 1358–1376, May 2024, doi: 10.1007/s12083-024-01662-6.

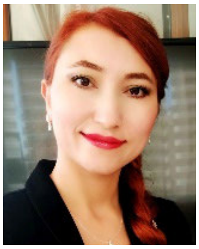
[32] A. Bisht, A. K. Das, and D. Giri, "Personal health record storage and sharing using searchable encryption and blockchain: A comprehensive survey," *Secur. Privacy*, vol. 7, no. 2, p. e351, Mar. 2024, doi: 10.1002/spy2.351.

[33] L. Wang, X. Liu, W. Shao, C. Guan, Q. Huang, S. Xu, and S. Zhang, "A blockchain-based privacy-preserving healthcare data sharing scheme for incremental updates," *Symmetry*, vol. 16, no. 1, p. 89, Jan. 2024, doi: 10.3390/sym16010089.

[34] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Sci. Rep.*, vol. 14, no. 1, p. 7841, Apr. 2024, doi: 10.1038/s41598-024-58578-7.

[35] E. U. Haque, M. S. Baig, A. Ahmed, A. Ahmad, M. Alajmi, Y. Y. Ghadi, H. K. Alkahtani, and A. Akhmediyarova, "Scalable EdgeIoT blockchain framework using EOSIO," *IEEE Access*, vol. 12, pp. 41763–41772, 2024, doi: 10.1109/ACCESS.2024.3377119.

[36] D. J. Bernstein. (Jan. 2008). *ChaCha, a Variant of Salsa20*. Accessed: Jun. 3, 2024. [Online]. Available: http://cr.yp.to/chacha/chacha-20080128.pdf



SEVAL CAPRAZ (Member, IEEE) received the degree from TOBB University of Economics and Technology, in 2012, and the M.Sc. degree in computer science from Middle East Technical University, in 2016. She is a Ph.D. student at Hacettepe University. She is currently a Senior Software Engineer in private sector. She has experience more than ten years in software development and cryptocurrencies. Her research interests include Ethereum, blockchain, distributed and parallel computing, high performance computing with GPUs, and big data.

ADNAN OZSOY received the Ph.D. degree from the School of Informatics and Computing, Indiana University Bloomington, in 2014. He is currently an Associate Professor of computer engineering with Hacettepe University. His research interests include parallel programming, high performance computing with GPUs, string matching algorithms, big data problems, distributed systems, application parallelism, blockchain applications, and cryptocurrencies.