Decentralized Electronic Health Records: Improving Security, Efficiency, and Accessibility

Shobha , Mahima M, Onkar B.K,. Aditya Vijaykumar, Nishu Priya

Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology,
Bangalore, Karnataka, India
0000-0002-3695-0898
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology,
Bangalore, Karnataka, India
0000-0001-7222-2508
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology,
Bangalore, Karnataka, India
0000-0001-9353-6522
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology,
Bangalore, Karnataka, India
0000-0002-4331-2042
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology,
Bangalore, Karnataka, India
0000-0002-9472-0089

shobha.p@nmit.ac.in ,_1nt19cs106.mahima@nmit.ac.in, 1nt19cs132.onkar@nmit.ac.in,
1nt19cs015.aditya@nmit.ac.in, 1nt19cs015.aditya@nmit.ac.in, 1nt19cs130.nishu@nmit.ac.in

Abstract— The necessity of Electronic Health Records (EHR) has become evident over the past few decades but, the issues surrounding it have made it seem like a downgrade in comparison with the previous hassle-filled maintenance of physical health records. Some of the common problems include unstructured data storage, lack of data interoperability, absence of data accessibility, privacy concerns, lack of transparency, and vulnerability to data hacks and leaks.

The current model of EHR is built around the idea of a centralized third-party vendor which collaborates with a healthcare institution to store the records. This induces a risk of vendor lock-in, lack of transparency, and absence of data interoperability. Digital security and privacy concerns in the current centralized model, in this case, remain a big obstacle to mass adoption. This can be overcome with user-owned data and blockchain-backed signature records.

Additionally, the concept of Decentralized Identifiers (DID) is at the very core of this proposed system, which helps individuals securely establish their virtual presence without being subject to arbitrary intervention by any third parties governing their data. While a few projects published have experimented with this, the paper will aim to overcome the problem of redundancy as well, i.e., in case a user loses access to their wallet.

In general, the entire experience of requiring medical attention remains complicated and worrisome for the average citizen. The goal of this work is to help overcome this.

A system that will be a Digital, Trustless, User-owned Health Records management solution implemented with Decentralized Identifiers (DID) and backed by Blockchain tech is proposed in this paper, that aims to resolve all the data **security** and privacy issues in the healthcare industry for stress-free access to medical services and overall well-being.

Keywords - *Blockchain, Decentralized Identifier, Electronic Health Records.*

INTRODUCTION

A. Background

The Problem statement identified in this paper focuses on the understanding of the Electronic Health Records System. To elaborate further, maintaining physical health records has always been a hassle. They are often easily lost, misplaced, or damaged.

These records are also at risk of being tampered with, faked, or misused. Every single health record is an important piece of an individual's medical history. Additionally, these records might be unavailable at dire times of need such as an accident or while travelling and staying in a different city.

The obvious answer to this is to digitize these physical health records, and multiple health tech companies have tried implementing different implementations of this solution. These digital versions of medical charts, diagnoses, treatment plans, and various other health documents related to the medical history of the patient are referred to as Electronic Health Records (EHR).

Several of these EHRs systems function out of just one cloud server which not only makes them a single point of failure but also makes them easy targets for hackers to hack into these systems and steal sensitive data. Hence, while EHR systems are absolutely necessary for easing the process of receiving accurate medical reports and diagnoses, none of the current digital solutions is trustworthy. Several users are concerned about privacy, data security, and lack of transparency.

B. Research Objectives

Through extensive research, deeper understanding and insight into the problems faced by the various stakeholders in the usage of electronic health records such as patients, doctors, and hospitals achieved. To identify the main grievances at hand faced by the numerous variables. With the guiding concepts identified as EHR, DID, Ethereum Blockchain, and IPFS for the implementation the objective is proposed,

Conduct extensive evaluation of the previously proposed models and frameworks for EHR management and storage to recognize relevant information and synthesize and evaluate it according to the guiding concepts. These frameworks are analyzed to see what aspects of the problem it's solving, how it's trying to solve it, and what the breakthroughs and shortcomings of it are.

I. RELATED WORK

A thorough and detailed literature survey was carried out that involved studying and referring to all recent IEEE papers that were found to be highly relevant to the idea, problem statement, and proposal being considered.

The framework published in the paper titled "Using Blockchain for Electronic Health Records" by A. Shahnaz served as a relevant starting point once the objectives are identified and elaborated. The need for granular access by the end-user and combining off-chain solutions with on-chain Blockchain features were valuable insights to direct us in this research [2].

The issue surrounding Data Accessibility, Data Interoperability, and Data Privacy in the context of Electronic Health Records (EHR) and a solution to resolve the same using Smart Contracts and Blockchain proposed in the research paper by Dr. R Chinnaiyan and the team was a highly relevant framework that has been analysed before delving into this proposed system [1].

Another common issue is that health institutions don't share the same portal for patients' health records and even within the same health institution when a patient is required to visit another doctor for consultation, the process of having the necessary health records accessible is cumbersome. Patients are forced to carry hard copies to ensure the records are available. This problem is amplified in the cases of an emergency when health records must be accessible within a short time frame. Most attempts at facilitating the necessary data accessibility of electronic health records have led to security attacks and data breaches that have led to the sensitive health information of millions of users being exposed and worse, reports of them being sold on the dark web [1].

Y. Wang proposed a cross-blockchain based privacy-preserving data sharing (CPDS) solution for EHRs data chains among various private blockchains in the hospital and has Wanchain as a service (WaaS) to store the unique index of EHRs and solve the problems of privacy leakage and deleting EHRs data [5].

G. Carter, H. Shahriar, and S. Sneha proposed an EHR sharing framework that uses Amazon Web Services to tackle problems of data scalability and storage requirements along with Ethereum blockchain for its use of smart contracts for the transparency provided while being cost friendly [3].

A hybrid distributed system architecture that is secure and private is proposed using blockchain for better security, patients' privacy by using a consent form, and with time maintaining data consistency while noting all of the health records that were shared with respective healthcare and insurance providers [4].

In addition to the above mentioned papers, referenced several others related to Decentralized Identifiers (DID) [6][7][8][9][10], Verifiable Credentials[6][7], Blockchain[8][11][12][13], User Data Privacy[7][12], Decentralized Storage[12] and IPFS[9][11][13], which helped us understand the previously implemented methodologies, gain valuable insights and validate not only the problem statement but also the approach for the proof of concept.

II. PROPOSED METHOD

A. Architectural Design

The main components of the model which are the 3ID Connect, Ceramic & DataStore, IPFS and the frontend [Fig 1]. 3ID connect helps recover the DID associated with the user wallet while Ceramic & DataStore works on encrypting and decrypting the health records and fetching the encrypted EHRs stored under the associated DID and also maintains access records for security footprints.

PFS helps create the distributed storage network for the encrypted health records. All these processes are carried out with the help of a clean and modern UI/UX.

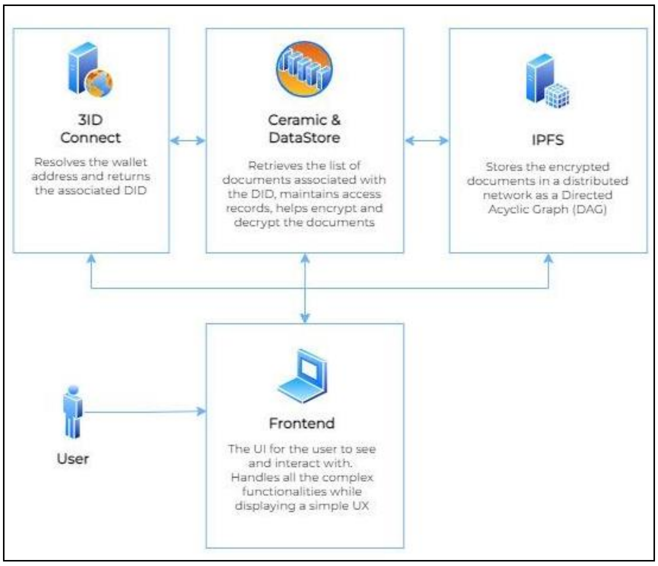
3ID Connect
Resolves the wallet address and returns the associated DID
Ceramic & DataStore
Retrieves the list of documents associated with the DID, maintains access records, helps encrypt and decrypt the documents
IPFS
Stores the encrypted documents in a distributed network as a Directed Acyclic Graph (DAG)
User
Frontend
The UI for the user to see and interact with. Handles all the complex functionalities while displaying a simple UX

Fig 1 - Architectural Diagram

B. Data Flow Diagram

The movement and interaction of data in the proposed model are depicted in Fig 2. It includes the functionalities such as login and authentication and viewing and storing a health record through this.

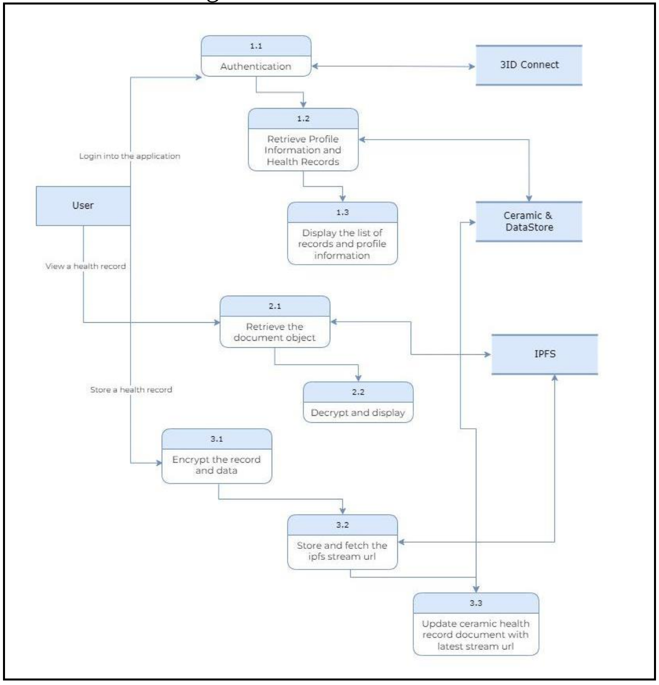
1.1
Authentication
3ID Connect
1.2
Retrieve Profile Information and Health Records
Login into the application
User
1.3
Display the list of records and profile information
Ceramic & DataStore
View a health record
2.1
Retrieve the document object
IPFS
2.2
Decrypt and display
Store a health record
3.1
Encrypt the record and data
3.2
Store and fetch the ipfs stream url
3.3
Update ceramic health record document with latest stream url

Fig 2 - Data Flow Diagram

When a user logs into the application, the authentication is done by fetching the DID with the help of 3ID Connect with which user information is retrieved and the associated health records from Ceramic & DataStore. This is displayed on the dashboard with a successful login. The DID being fetched here could be linked to multiple user wallets, providing the necessary redundancy against wallet loss.

To view a document, the encrypted health record is fetched from the distributed storage network and displayed after decryption. The same is updated in the access records. To store a health record, it is first encrypted and stored in the distributed storage network, the corresponding IPFS stream URL is then fetched and updated into the ceramic health records document.

III. METHODOLOGY

A. Brief Insight

In this work VueJS is chosen for the front end of this work owing to its simplicity and easy integration in large-scale projects and frameworks are used for designing the User Interface assets, and VueX store for State Management. The backend is not a dedicated infrastructure but is rather a shared one which allows for data interoperability at all levels, and utilises Ceramic Datastore with IPFS working in tandem.

B. Pseudo-Code

The implementation uses JavaScript and DID Authentication implemented using Ceramic, 3ID Connect, and the User's Blockchain wallet.

The following piece of code completes the authentication process and then fetches the user profile and the list of health records using the definition of each of their schemas. The list of health records fetched includes only a title, date and the base32 serialized CID string of the encrypted JWE object which is stored on IPFS.

Here each authenticated DID instance returns the relevant user data while using the same schema and data models [Fig 3]. This allows any application to import the same data models and consume the response to produce any desired results. It is this part of the application which enables data interoperability between applications while the user completely remains in control of the data.

```
Initialise with required variables
        Model <- Data models being used
        Ceramic <- Ceramic node with RPC url
        Web3modal <- Different wallet provider options

Execute procedure for auth and data fetch

authenticateAndFetch()
        CALL Web3modal() and store provider
        CALL threeIDAuth(provider, ceramic) and store threeID
        Did <- new DID (threeID, ceramic)
        CALL authenticate() on Did and store authenticated
        IF authenticated is FALSE Return NULL
        DataStore <- new DIDDataStore( ceramic, model)
        CALL DataStore.get(UserProfile) and store UserProfile
        CALL DataStore.get(HealthRecordsList) and store
```

```
HealthRecordsList
        return UserProfile, HealthRecordsList
```

Fig 3 - Pseudo Code of 3ID Connect authentication and data retrieval using DID DataStore

For the proof-of-concept implementation, researched and consulted with a few doctors to identify an appropriate generic schema for storing health records. The objective here was to have a highly flexible schema which can be made use of for most given scenarios. This can of course be improvised, and additional templates or schemas can be added in the future.

The following[Fig 4] schema includes straightforward fields such as the title of the health records, the date of diagnosis, the name of the doctor, the diagnosis done, and finally, the medicines prescribed.

Property Name	**Property Type**
Title	String
Diagnosis Date	Date
Doctor Name	String
Diagnosis	String
Medicines Prescribed	String

Fig 4 - The schema used for creating and storing all the health records

The encryption of the record object takes place using the authenticated user's private keys. The implementation includes the dag-jose packages which allows the publishing of the data to IPFS and implements the ECDH-1PU+XC20PKW with XChaCha20Poly1305 algorithms for encryption[6], as described by the International Engineering Task Force.

The same approach is used during decryption as well. In the case of decryption, the id of the record is first fetched from the DID Store through the interoperable model, the encrypted health record object is then fetched from IPFS, and finally decrypted using the authenticated did instance which has the user's keys.

IV. Results

While implementing this, various technical challenges were encountered throughout the process of building the different parts of the front end, particularly so while integrating with the various Ceramic and other related packages. All of these were resolved in time to complete the working alpha prototype.

The current implementation and built status of the project allows users to log in to the application by using their blockchain wallets. To allow for a user-friendly experience, Portis wallet integration has also been completed which allows for a simple email and password form of authentication. The more advanced users can simply connect using a hardware wallet like the Ledger through WalletConnect or simply through a hot wallet such as Metamask.

The user has to then sign a message to authenticate their login through 3ID Connect and share the response with the DID details. Upon successful authentication, Ceramic and DID Store are set up to retrieve the basic profile details and the list of health records, which includes the title and the pointer to the IPFS encrypted record object.

Presently, health records can be created, encrypted and stored only by the user themselves through their own dashboards. The encryption makes use of the ChaCha20 stream cipher with the Poly1305 authentication, the usage of which in IETF protocols is standardised by RFC 8439[7]. The encryption takes place in the client browser window, and the resulting object is published on IPFS, finally storing the IPFS stream id in the DID DataStore.

Finally, the user can click on any given health record, the id of which is used to fetch from IPFS and is then decrypted within the client's window where the client DID private keys are available.

V. Conclusion and Future Work

In hospitals and medical offices, electronic health records are the clear and unavoidable future of patient care. This work has sought to validate the presence of the problem through research throughout this paper.

It was discovered that a decentralized electronic health record system was a viable solution based on preliminary as well as extensive research. When compared to existing medical record systems, the proposed decentralized electronic health record system offers increased security and data exchange efficiency.

With the right implementation using technologies such as Blockchain and DIDs, the entire medical ecosystem can interact with each other seamlessly whenever necessary, all while maintaining the necessary amount of security and privacy.

Major merits of this work include complete ownership of sovereign data by the users without third-party involvement, elimination of centralized authentication using DIDs, blockchain-based signature records to verify the authenticity, and universal accessibility.

To conclude, this ambitious work aims to improve the effectiveness, efficiency, and accessibility of medical services while establishing an example of universal guidelines for storing medical data in an organized and structured manner.

There are several improvisations that can be done to the working proof of concept. The most important of which would be creating a Doctor's Dashboard, which will allow doctors to create a health record, sign it using an NFT which represents their medical licence, and then issue it to the patient. This record can then be verified by the patient as well as any pharmacist if necessary. It unlocks a whole new realm of possibilities.

The current schema of health records has been kept generic for the proof concept, and an array of various health record schemas and templates, including specialised formats for any medical test reports or x-ray scans, may be done. This will expand the scope of records which can be digitised while still maintaining the structured nature which was one of the objectives of this undertaking.

Lastly, building a platform-independent version or a Software Development Kit (SDK) of this proof of concept, which does not include any bundled frontend framework and will allow the service provider to simply consume the SDK and build their own decentralised health records system, would be the final improvisation and part of the future work.

References

[1]. Vardhini, S. N. Dass, Sahana, and R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," in 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1–4.

[2]. A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782–147795, 2019.

[3]. G. Carter, H. Shahriar, and S. Sneha, "Blockchain-based interoperable electronic health record sharing framework," in 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019, vol. 2, pp. 452–457.

[4]. M. M. Mahdy, "Semi-Centralized Blockchain Based Distributed System for Secure and Private Sharing of Electronic Health Records," 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2021, pp. 1-4, doi: 10.1109/ICCCEEE49695.2021.9429554.

[5]. Y. Wang and M. He, "CPDS: A cross-blockchain based privacy-preserving data sharing for electronic health records," in 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), 2021, pp. 90–99.

[6]. Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," in 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020, pp. 71–78.

[7]. D. Yoon, S. Moon, K. Park, and S. Noh, "Blockchain-based personal data trading system using decentralized identifiers and verifiable credentials," in 2021 International Conference on Information and Communication Technology Convergence (ICTC), 2021, pp. 150–154.

[8]. B. Kim, W. Shin, D.-Y. Hwang, and K.-H. Kim, "Attribute-based access control(ABAC) with decentralized identifier in the blockchain-based energy transaction platform," in 2021 International Conference on Information Networking (ICOIN), 2021, pp. 845–848.

[9]. N. Fotiou, V. A. Siris, and G. C. Polyzos, "Enabling self-verifiable mutable content items in IPFS using Decentralized Identifiers," in 2021 IFIP Networking Conference (IFIP Networking), 2021, pp. 1–6.

[10]. M.-H. Rhie, K.-H. Kim, D. Hwang, and K.-H. Kim, "Vulnerability analysis of DID document's updating process in the decentralized identifier systems," in 2021 International Conference on Information Networking (ICOIN), 2021, pp. 517–520.

[11]. R. Kumar and R. Tripathi, "Implementation of distributed file storage and access framework using IPFS and blockchain," in 2019 Fifth International Conference on Image Information Processing (ICIIP), 2019, pp. 246–251.

[12]. S. Chenthara, H. Wang, K. Ahmed, F. Whittaker, and K. Ji, "A Blockchain based model for Curbing Doctors Shopping and Ensuring Provenance Management," in 2020 International Conference on Networking and Network Applications (NaNA), 2020, pp. 186–192.

[13]. D. Malhotra, S. Srivastava, P. Saini, and A. K. Singh, "Blockchain based audit trailing of XAI decisions: Storing on IPFS and Ethereum Blockchain," in 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2021, pp. 1–5.

[14]. G. Amringer, "Chacha derived AEAD algorithms in JSON Object Signing and Encryption (JOSE)," IETF Datatracker. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-amringer-jose-chacha-02. [Accessed: 09-Dec-2022].

[15]. Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," 2018.