Blockchain based Health Care Protocol

Kaviyaraj R[*,2]
Department of Computational Intelligence,
SRM Institute of Science and Technology,
Kattankulathur, India.
https://orcid.org/0000-0002-1858-1582

Akshat Singh
Undergraduate
Department of Computational Intelligence,
SRM Institute of Science and Technology,
Kattankulathur, India.

***Abstract*— The conversion of healthcare information into digital formats has completely transformed the way electronic health records (EHRs) are handled, opening up possibilities for streamlining processes and enhancing patient care. However this progress also raises concerns regarding the security and control of data access. To tackle these issues a new system is suggested in this research paper utilizing technology. This system aims to guarantee the effective management of health records by implementing detailed access controls and storage solutions off the main blockchain network. Additionally by incorporating alternative storage methods outside the blockchain network it effectively addresses scalability challenges typically associated with technology. Furthermore the structure underscores the importance of privacy and confidentiality through access limitations. By leveraging technology this proposed system provides a secure platform, for managing electronic health records reducing the risks of data tampering and unauthorized access.**

Keywords*— *Electronic Health Systems, Data Security, Privacy Concerns, Role Based Access, Time Based Access, Two-Factor Authentication

I. Introduction

Digitized health data brings in an entirely new era of running medical records with an unbelievable level of accessibility and efficiency. Modern day health systems involve Electronic Health Records (EHRs) to provide easy communication between health service providers and effective treatment of patients per individual needs. However, even with such a digitization speed in medical records, issues of access control and data safety continue to remain. Medical data in this case will thus need to be attended to sensitively, bearing in mind threats presented through cyberspace, as desperate needs have to provide strong securities for the protection of patient's confidential and private information.

In line with this, this research work presents a novel approach to exploiting the disruptive potential that blockchain technology offers for healthcare data security and access management empowerment in the face of these challenges. With the use of cryptographic principles and the decentralized architecture of the blockchain, the framework aims to have a platform architecture handling electronic health records from tampering. Designed to assist in the healthcare market, the solution seeks confidentiality and data integrity against an intention to fix the scalable problems of classical blockchain solutions..

II. Background

Their use is indeed a very important landmark in the modernization of national healthcare systems. Electronic health records (EHRs) refer to digital records where all patients' data, including diagnosis, treatment plans, lab results, and medical history, can be stored. Their translation from paper-based to electronic records eased the smooth working in the industry, retrieval of information, and communication with the providers. This new digital move has also made health companies more open to risks in cyberspace than ever before, some of which have never been seen before.

Worries over data security and privacy persist even in the healthcare industry, with the advent of EHRs. Medical data are very sensitive and hence expose them to cyberattacks, highly common. This takes various forms, including but not limited to those that arise from ransomware attacks, identity theft, illegal access to data, or breaches.

Added to this, healthcare data management is further complicated due to the ability to fulfill a strictly necessary law, such as the Health Insurance Portability and Accountability Act (HIPAA). This has brought an enormous pressure on healthcare institutions to safeguard the information of patients, ensuring at the same time that it does not go beyond the limits that law allows them to. Access controls and encryption are two common securities proven critical in the protection of healthcare data from attacks. Lack of necessary depth of information usually describes a barrier to a guideline for access control being applied rigorously, hence preventing unauthorized access. Besides, the traditional centralized storage of data has inherent risks. Such centralized servers are a single point of failure, which may have been targeted by hackers.

This has increasingly attracted people to explore state-of-the-art technologies for an improved security posture of healthcare systems and to overcome the limitation of traditional paradigms in response to such constraints. This can be one of the potential sources of providing solutions to the privacy and security-related impediments that are presently a bane to data management within healthcare. The blockchain is a decentralized ledger that records transactions made upon a distributed node network. Its first brush with the limelight came as the technology underpinning cryptocurrencies such as Bitcoin. Being free from any central authority, its decentralized architecture intrinsically provides resistance to tampering and unauthorized modification, hence reducing the risks associated with such malpractices to single points of failure. In fact, blockchain technologies through open, transparent, and secure platforms for EHR management are able to ensure integrity, confidentiality, and authenticity by use of cryptographic techniques.

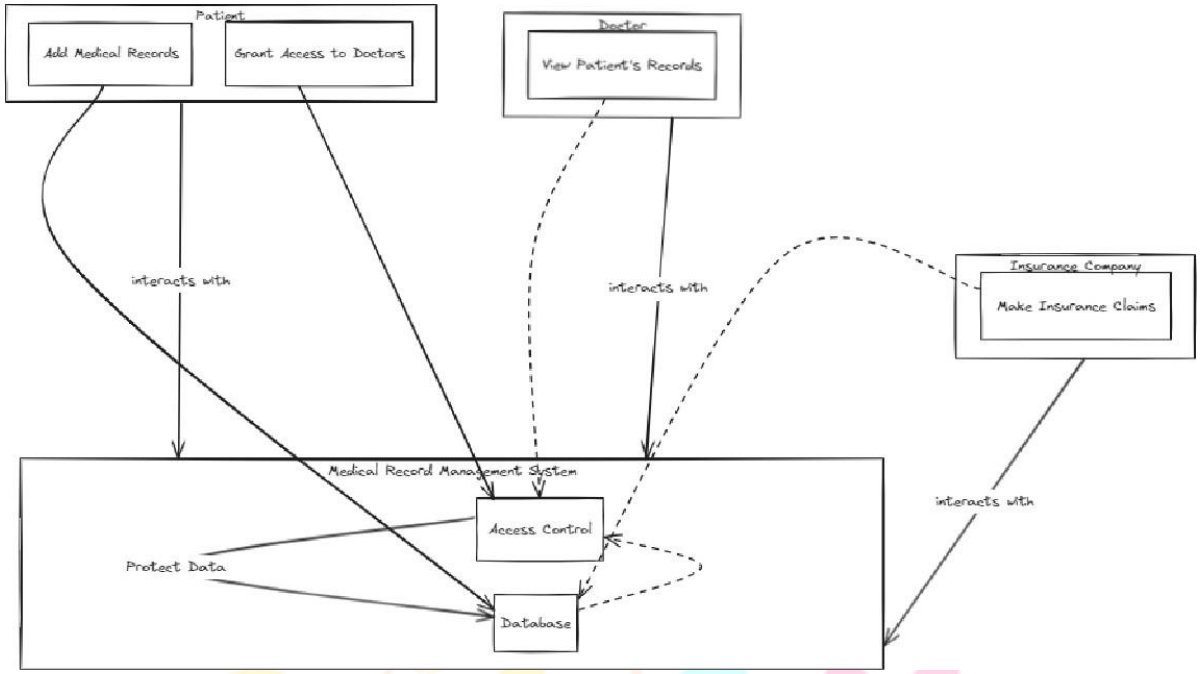


Fig 1: System Flow Diagram

III. PROPOSED SYSTEM

The new system is proposed to make use of blockchain technology in the maintenance of electronic health records (EHRs). In simple essence, the system makes use of the decentralized ledger of blockchain technology to provide a very secure and tamper-proof platform for processing and storage of data emanating from the medical quarters. The system presents reduced threat from unauthorized access and tampering by use of the distribution of data across a network of nodes, using cryptographic techniques for integrity and confidentiality of EHRs.

The important aspect of the proposed approach is that it proposes the approach with off-chain storage technologies to overcome the problem of scalability in the mainstream of the traditional blockchain system. The approach to storing large amounts of data, such as medical records and diagnostic pictures, off the blockchain while maintaining cryptographic proof, assures the integrity of the data. So this approach maximizes storage.

It realizes efficiency and increases the speed of data retrieval for a high-performance system. This is in line with the granular access restrictions in this system, together with off-chain storage, controlling access that users do have towards EHRs to ensure that patient privacy is protected. The system implemented the model of role-based access control to provide different roles with different permissions according to organizational functions and responsibilities. It reduces the risk of data breach and, in so doing, unauthorized disclosures, ensuring that only those persons who have been granted permission have the ability to access information required of them in executing their duties.

The system highly focuses on data security through implementing very strong methods of encryption, which assure that privately kept data is secure in the blockchain. This ensures that the patients' information is kept private and safe, even in a case where a security breach or unwanted access trial takes place. It is because it ensures EHRs are encrypted both during transit and when at rest. This increases the confidence and trust of patients in the security of their medical records. All taken together, the proposed system indeed is a holistic solution for managing health care data, with the proposed system lying in the integration of access control methods with the blockchain technology, offering security and transparency.

The object of the system would be to resolve the dynamic challenges faced by the healthcare industry and, at the same time, try to encourage safe digital healthcare solutions by providing a scalable, secure, and privacy-based management system for electronic health records.

IV. RELATED WORK

A.

The solution suggests revolutionizing access control by proposing data accessibility of the attributes of the user rather than the pre-assigned identity. This granular approach

to data access increases security, simplifies management for permissions, and allows for safe exchange of data in scenarios with specific access requirements. But in ABE, high key management complexity is obtained, and potential performance overhead due to additional cryptographic operations. However, despite all the difficulties and drawbacks, ABE provides fine control granularity over sensitive data and, therefore, represents an appealing solution for many types of security-aware applications.

B.

aims to facilitate simplification in key management by allowing the elimination of the need for the pre-distribution of public keys; instead, users' public keys will be computed from users' unique identity, like their email addresses. This simplification is a convenient way and potentially reduces administrative burden. However, BIE raises concern over its vulnerability to blocking attacks, where a rogue identity can be used to gain illegal access. The security to the whole system is inverse, equated to one's faith in the authority issuing keys. It is therefore extremely important to ensure the integrity and robustness of this central authority.

C.

leverages JSON content access records provided by the power of the blockchain. This immutability increases trust and auditability because it renders an unalterable history of all efforts to connect. At the same time, the very inherent characteristics of blockchain technology, such as being distributed, and consensus mechanisms, have aspects related to scalability problems and potential performance throttles.

D.

emphasizes the relation between sharing data and privacy in health care is that it presents the way to access by personnel from an authorized health care facility to the essential data for the patients, and on the other hand, maintaining security from the source facility. This lends room for better collaboration and effective care. Federated access control, on the other hand, requires the complex definition of interoperability standards and supports the realization of close collaboration between the health care organizations involved. For these reasons, this setup is often difficult to be put into practice

E.

emphasizes This means a lot of flexibility, since it allows an individual or a company to build access control policies through the use of many attributes and conditions. This would allow you to exercise fine control and, in this case, customization to your business needs. However, it can be complex to manage such complex policies. As such, clear, consistent, and complete policies often involve expertise; and in cases where they are inconsistent, many security gaps are likely to be created, or it is likely for there to be interference with effective access management.

F.

aims to dynamically adjust access permissions based on a real-time assessment of potential threats. This approach can increase security in environments where threats are constantly evolving. By considering factors such as user behavior, device location and access times, RBAC can limit access in high-risk situations and enable broader access in low-risk times. However, implementing an effective RBAC system requires the development of accurate risk assessment models and continuous monitoring of these factors, which can require intensive resource deployment and constant maintenance.

G.

values the patient's autonomy to handle his own health data. In this way, the patient controls his access permissions and decides who will access his information; therefore, transparency and trust of the clientele to the system is assured. This focus on putting the user in control has a possible downside: patients without enough expertise about the complexities and implications of access control would put themselves at risk of inappropriately granting access or taking decisions that would be to the detriment of their proper handling. Therefore, successful implementation can only be achieved through educational endeavors that would leave the patients well-prepared for making informed decisions concerning the sharing of data.

H.

data is encrypted with certain access policies in a way that only users whose characteristics coincide with the policies would be able to decrypt the information. This allows very fine-grained control based on very complex criteria—an important advantage. However, this brings about greater key management and encryption/decryption processes complexity, unlike standard ABE, and thus probably impacts the performance and scalability of the system

I.

this will allow those authorized to operate directly on the encrypted data without actually having to do decryption, hence a very strong advantage in data protection, as the information will remain encrypted during phase analysis or processing. Nevertheless, current homomorphic encryption schemes face hurdles. One really important consideration with such schemes is the computational overhead, in that it may impair the processing speeds. Thus, it hardly brings them to application in resource-challenged environments. The suitability of a concrete task with them must also be gauged very carefully to the already mentioned scope limitation of supported operations compared to traditional encryption methods

J.

A way the users can have proof that they have some qualities or knowledge to show to a verifier without showing details about what it refers to is disclosed. It can be useful in access control situations where a user has to prove

his granted permissions but sensitive information cannot be given out. However, the ZKP also faces challenges. Such complex evidence can take much time in computation and, at the same time, reviewing it. This can impact the performance drastically. Besides, the security of FPC systems highly depends on some basic cryptographic assumptions. Any breach in this case can compromise the effectiveness of the system.

V. METHODOLOGY

The developed system was designed using a very systematic approach to ensure that the health management solution is secure, dependable, and effective. After that, for the proper implementation of all the features which are critical at the same time, to prove the functionality of the system, the method involves some critical phases, and they include assessing and implementing and finally testing the system.

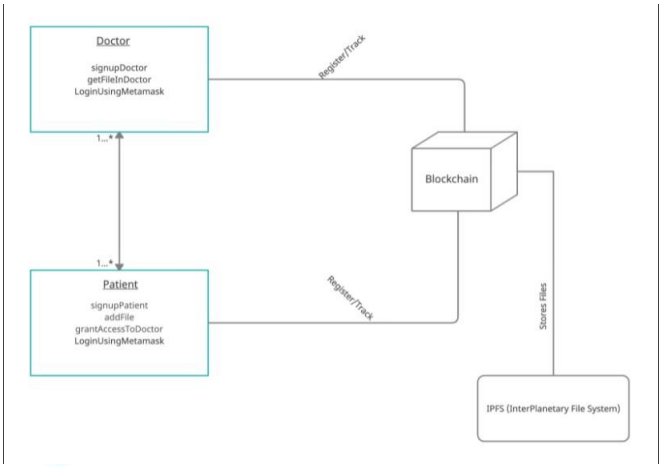
The following is the manner through which the first step will be approached: assessment of the potential system vulnerabilities, current deficiencies in the system, and the analysis of the present scenario of healthcare data management practices. In fact, assessment will set the base of improvements developed further to have a complete understanding of the limitations and requirements in healthcare data security and access control.

The stage of implementation activity, which comes after the analysis phase, will focus on the addition of crucial elements into the system architecture to add the ability toward security and access control. All these present the need to design and develop important components, like off-chain storage solutions, methods of encryption, and role-based access control (RBAC) systems that shall mitigate identified security risks and ensure regulatory compliance.

After incorporating these main components in the system, it's important to test the functionality, performance, and safety of the system in accordance with the proposed solution. This testing phase will involve the scenario and use case concerning a wide variety of tests in understanding, assessing, and determining how much the system enforces patient data access control guidelines while reducing possible security threats. Before deployment, the testing phase will be carried out in detail so that issues or any other type of vulnerabilities present, which may make the system feeble and unreliable, are located and repaired.

Accordingly, compliance with the industry standards and best practices at each of the various levels in the development process will have to be implemented in order to assure that the proposed solution is sustainable and effective. Corrective action on time should be taken through continuous monitoring and evaluation of the performance and the security posture of the system in order to identify the new potential threats and vulnerabilities.

Fig 2. Class Diagram



In other words, the emphasis was laid on the proposed system in a methodical approach concerning security, dependability, and the need for adhering to regulatory compliance in health care data management. The solution will tend to discuss the emerging challenges that the health business is prone to and advocate the support of safe and effective digital health solution use through implementation of requisite features and testing to adherence.

VI. RESULT AND ANALYSIS

Fig 3. The main landing page.

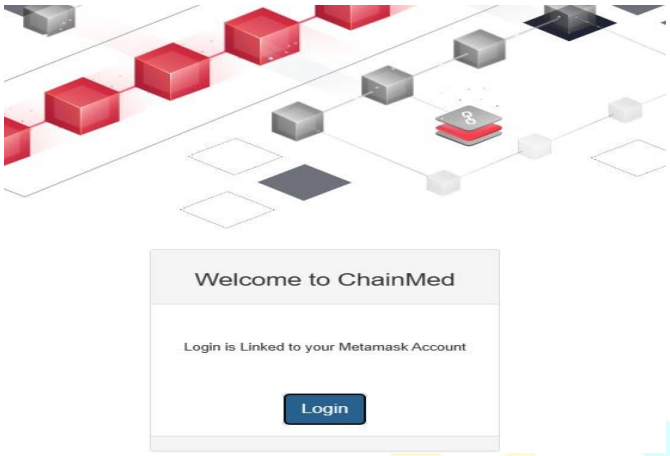


Fig 4. Screenshot of the Compiled Contracts

```
Compiling your contracts...
===========================
> Compiling .\contracts\Agent.sol
> Compiling .\contracts\Migrations.sol
```

```
> Compiled successfully using:
   - solc: 0.5.1+commit.c8a2cb62.Emscripten.clang
```

Fig 5. Screenshot of Contract Migrations

```
Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0x9bc337f3eef4a9cb3f65ef2832f9beacc51beff8ea9d911e6ee022d3cdb1b03e
   > Blocks: 0            Seconds: 0
   > contract address:    0xE51fc339776E78791097ca99E76f7e4D9f0C035C
   > block number:        1
   > block timestamp:     1711087802
   > account:             0x57940888cB2Fa4B219e651b9A03F56C40E88309F
   > balance:             99.99917434
   > gas used:            244640 (0x3bba0)
   > gas price:           3.375 gwei
   > value sent:          0 ETH
   > total cost:          0.00082566 ETH

   > Saving migration to chain.

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.00082566 ETH
```

Fig 6. Local Ganache Server

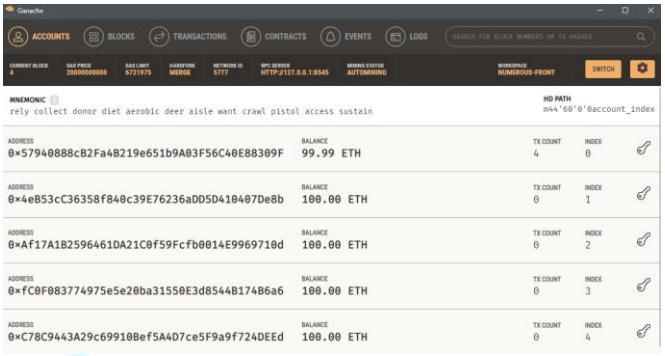


Fig 7. User Registration Page

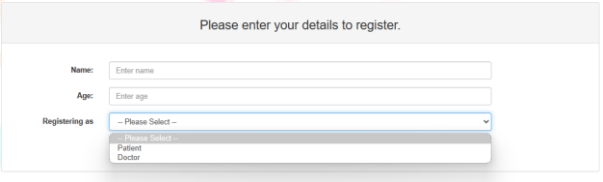


Fig 8. Patient Landing Page

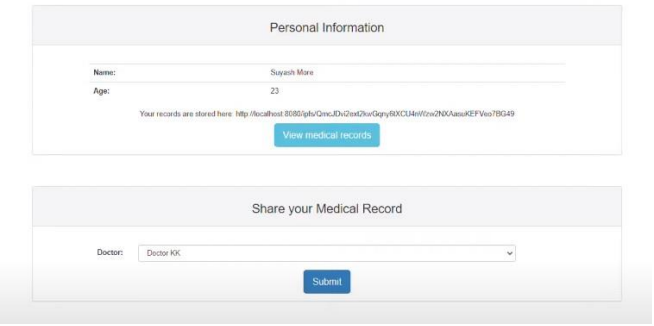
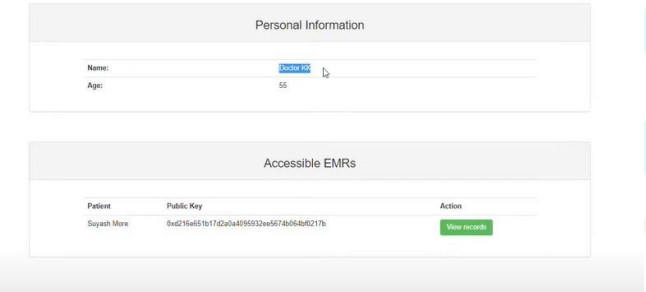


Fig 9. Doctor Landing Page



VII. FUTURE WORK

The future is very bright in further developing and enhancing the health data management system, with great prospects. Research in the future could ascertain how the use of artificial intelligence could predict health trends and offer individual treatment routines. This has the potential to transform the way we deliver patient care to one that is more proactive and individualistic. In addition, we shall improve interfacing features of the system with other medical technologies that wearables will provide, in this case, real-time health data for improved monitoring and decision-making. Lastly, we would take into consideration recent advances in blockchain technology to improve system security and efficiency while protecting patient information. The efficacy and accessibility of healthcare services could be significantly impacted by these next initiatives.

Future research will also look into how to improve accessibility and the user experience of the system. With the development of technology, there is an increasingly growing demand for improving access and the user experience of the healthcare system and healthcare services in general.
Perhaps interesting in future development would be the involvement of user studies; hence, understanding requirements and preferences in the product from different types of user groups, such as patients, healthcare professionals, and administrators. The results of the user study could be useful to improve data visualization, simplify navigation, and improve usability in general of user interface designs. We will also ensure that the system is accessible to people with disabilities through compatibility with screen readers and through alternative input ways. Thus, future releases of the healthcare data management system may emphasize accessibility and user experience in such a way that will enable their users to be the most productive possible.

REFERENCES

[A] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In EUROCRYPT 2005, pp. 412-428. Springer, Berlin, Heidelberg, 2005.

[B] Beguelin, Jean-Luc, Jean-Marc Robert, and Michel Yung. "Filtered-IBE: Efficient revocation in identity-based encryption." In International Conference on Cryptology and Information Security in Latin America, pp. 107-120. Springer, Berlin, Heidelberg, 2007.

[C] Azab, Mohamed, et al. "Blockchain-based access control for secure e-health records." Journal of Medical Systems 43.2 (2019): 29.

[D] Yu, Yu, et al. "Federated access control for healthcare data in cloud computing." IEEE Transactions on Information Technology in Biomedicine 17.8 (2013): 1714-1723.

[E] Sandhu, Ravi S., Edward J. Coyne, and Haleh Nissenbaum. "Federated access control using role-based access control (RBAC)." In Proceedings of the National Computer Security Conference, vol. 95, pp. 169-180. 1995.

[F] Sandhu, Ravi S., and Qi Li. "Role-based access control models." IEEE Computer 39.9 (2006): 34-40.

[G] Ienca, Maria Alexandra, et al. "Patient-centric access control in healthcare information systems: A systematic review." Journal of biomedical informatics 49 (2014): 124-133.

[H] Amit, and Brent Waters. "Fuzzy identity-based encryption." In EUROCRYPT 2005, pp. 412-428. Springer, Berlin, Heidelberg, 2005.

[I] Gentry, Craig. "Computing arbitrary functions of encrypted data." In Communications of the ACM, vol. 51, no. 12, pp. 39-47. ACM, 2008.

[J] Goldreich, Oded, Silvio Micali, and Ronald L. Rivest. "A digital signature scheme secure against adaptive chosen-message attacks." SIAM Journal on Computing 17.2 (1988): 285-308.