National College of Ireland

Block chain Enhanced Personal Health Records Sharing with Integrity Verification

MSc Research Project
MSc Cyber Security

C Chandana
Student ID: X22223835

School of Computing
National College of Ireland

Supervisor: Eugene Mclaughlin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: C Chandana

Student ID: X22223835

Programme: MSc. Cyber Security **Year:** 2024

Module: MSc Research Practicum

Supervisor: Eugene Mclaughlin

Submission Due Date: 12/08/2024

Project Title: Blockchain-Enhanced Personal Health Records Sharing with Integrity Verification

Word Count: 6036 **Page Count 19**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: C Chandana

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Block chain Enhanced Personal Health Records Sharing with Integrity Verification

C Chandana
X22223835

Abstract

Mainly, the need to share the personal health records (PHRs) is highly important in the current society due to the raging use of technology. This project specifically attempts to solve the problem of efficient PHR management through the incorporation of block chain technology. The system involves three primary stakeholders: administrators, patients who are the data owners and data users that are hospital staff, insurance companies, and other medical personnel. The existential question in such research includes is the data stored on the block chain tampered in any way. Proposed system effectively authenticates the data integrity with the help of SHA hashing to prevent unauthorized modifications in data. It is a hybrid cloud where the application part of it runs on a private cloud for security reasons while data is on the public cloud for efficiency. Attribute Based encryption guarantees that the health records data is only accessible by the right personnel while making the data searchable, improving performance, and protecting the information from the alteration.

1 Introduction

The features of exchanging or maintaining Electronic Health Records have turned into vital necessities for being relevant to the principles of digitized health for better patient care and organizational competency. This analysis shows that the traditional EHR systems are not completely free from the problem of data security, data sharing, or lack of patient control even with modern technological advancements. Some data that recent researches provide include that block chain technology is capable to meet the need of data security, data privacy, and efficient access control Shamshad et al., (2020); Tanwar et al., (2020). Approximately 20% to 30%of the healthcare institutes are changing their approach from traditional to electronic health record. The integration of block chain for secure and authenticated data management is the major concern of this paper's examination of the possibility of how block chain may revolutionize the sharing of personal health records (PHR) through a hybrid cloud model. This way, using both public and private approaches to the cloud guarantees encryption of data on a private basis as well as on the public basis, though storing it in the public cloud. This method utilizes the private cloud server's ability for secure encryption and while relies on public cloud's scalability as well.

The main research question is how might block chain technology improve PHR security and integrity? & what are the real-world effects of using a hybrid system?

2 Related Works

This section discusses how the innovative technology can be applied to protect cloud computing, give the patient control and improve EHR data quality, privacy and, share ability. It also provides an overview on how the analytic tools of the machine learning and data mining enhances the value and analysis of EHR data for both clinical and research purposes. Nevertheless, these achievements do not necessarily translate into real-world applications and especially empirical research in healthcare. Evolutions in its growth and deployment are discussed with indicators to illustrate where research and advancements are needed to enhance the safety, privacy and management of electronic health records.

Block chain Technology in EHR Management

Epic technologies achieve the objectives of privacy, security, and efficiency using block chain in managing EHR. The Shamshad et al. (2020) suggested that two types of block chain, the private and the consortium one, public key encryption and searchable keywords to the medial record should be provided to enhance access control and minimize security threats, hence, diagnosed and curative efficacies. According to Tanwar et al. (2020), block chain can thereby simplify and decrease the costs of healthcare by enhancing the capability of databases to work with one another and guarantee safe patient record retrieval. Zarour et al. (2020) confirm the efficiency of private block chain methodologies for the real exchange of EHR information safely. In 2022, Lee and colleagues propose a block chain-based solution to build on these efforts still.

Patient Empowerment and Access Control

The technology of block chain enhances the patient's authority and control access that had been planned to change the EHR systems revolution. Next Block chain, according to Hajian et al. (2023), promotes self-control of the records and strengthens patient handling of illnesses, in addition to reconstructing beliefs about healthcare services. Chelladurai et al. (2021) explain how the block chain patient centric smart contracts offer safe storage of fragmented Health records and how permission can be managed. This leads to increase in efficiency and transparency of the organization. According to Chouhan et al. (2023), block chain is proposed as improved solution to problem areas of centralization and security for EHR systems, where the decentralization of EHR significantly improves patients' privacy and reliability. While real world applications of block chain technology remain very limited, Cerchione et al. (2023) see the potential that the concept can help solve for security and fragmentation. Sivan et al., (2021) examine on the aspect of integration with cloud-based systems.

Cloud Computing and Security

Cloud computing and block chain integration answers questions concerning security of cloud base EHRs and other associated matters. For data integrity and for the confidentiality of the block chain-enhanced cloud e-Health record system, Benil et al. (2020) recommend elliptic curve encryption and certificateless aggregate signatures. According to the work of Kanwal et al. (2021), which concern the evaluation of privacy preserving access control models, while analysing Attribute Based access control and anonymization for protection of the EHRs, the application of formal methods is highlighted. To reduce the unwanted access and data breaches Keshta et al. (2021) urged the government to enhance the privacy laws and to establish a strong security framework besides recommending system standardization. Jusak et al. (2021) describe methods of anonymization sensitive medical data that relies on IoT as data is being transferred and stored in public cloud platforms. Walid et al. (2021) discuss the following in the field of Attribute Based Encryption.

Advances in Data Mining and Machine Learning for EHRs

Electronic health records (EHRs) are becoming more useful for clinical and research applications because to developments in data mining and machine learning. According to Groenhof et al. (2020), data mining algorithms may reliably extract patient smoking status information from electronic health records (EHRs), hence enhancing the quality of clinical data. In order to extract insights beyond predetermined classifications from electronic health records (EHRs), Wang et al. (2020) employ unsupervised machine learning algorithms to identify patient subgroups and disease clusters. When Wu et al. (2020) compare text mining and diagnostic codes to identify depressed symptoms; they discover that text mining more effectively overcomes the constraints associated with functional impairment evaluation. Introducing a framework for modeling scenarios of missing data in EHRs, Getzen et al. (2023) emphasize the effect on illness prediction models. Clinical advances in natural language processing (NLP) are examined by Kormilitzin et al. (2021).

Theoretical and Empirical Advancements

Recent advancements in the theoretical and practical analysis of the problem set an emphasis on such significant concepts as secured cloud computing and its connection with data security. To make new concept safe and free from external attack and to avoid unwanted tempering in the data, Awadallah et al. (2021) explored the need of safe data integrity solution in cloud environments and the use of block chain technology with cloud computing. In the topic of shift towards cloud computing for big data processing, Awysheh et al. (2021) document the application of security by design approaches. Specifically, Zhu et al. (2021) recommend the

configurations of Semantic Web and Attribute Based Encryption (ABE) technologies to improve data access control as well as the safety of cloud based EHR systems. In the case of the multi cloud computing environment, Walid et al. (2020) propose different mechanisms of work scheduling that would allow for properly utilising resources and improving services' quality. Chinnasamy et al.,(2022), have also pointed out safer ways for cloud storage.

Gap Analysis

Most of the studies conducted in the past may amass theoretical advantages of block chain technology in the healthcare sector or may highlight its technical prospects and accomplishment without concrete research findings. The areas of the application of block chain with the hybrid cloud solutions and their scalability and performance improvement are discussed here but are still unclear. Also, while attribute-based access control (ABAC) is more proactive, there is still limited information on its suitability in multiple actors and scene-changing contexts, such as those that accompany privacy-sensitive data exchange, like PHP. These chasms could be filled to enhance instantaneous, secure PHR sharing in its reliability, efficiency and security with effective data confidentiality and efficient user experience.

3 Research Methodology

To ensure that they follow appropriate science, this section justifies the methods of assessing and conducting research in this study. The technique has been partially defined by the previously cited work and is based on the related work identified in pervious section.

3.1 Research Procedure

In the process of study there are several procedures that aim at data collection, management and analysis which were applied. The actions comprised:

Review of the Literature: To ensure that this was done, a critical literature review of block chain technology, RSA, ECC and ABAC was conducted to lay a theoretical foundation.

System Design: A user defined block chain to safeguard the storage of data in the proposed system architecture and the access control was made fine grained using ABAC. Hence, data integrity together with secure communication was ensured by the RSA and ECC algorithms on board.

User-Defined Block chain: A user-defined block chain system is a structure that prevents data from being altered and stolen by third parties; moreover, SHA hashing and attribute-based encryption are applied to protect personal health records.

Implementation: The specific block chain solution and Python language were used to enable the system in question.

3.2 System Requirements

- **Hardware Requirements**: High performance computing systems with multi-core processors and substantial storage capacity to handle block chain operations and EHR management.
- **Software Requirements**: Custom block chain framework, ABAC policy management tools, and cryptographic libraries for RSA and ECC implementations.
- **Cloud Storage Space**: Block chain Blocks are generated in this system will be stored in Cloud Storage space, for this prototype model Drive HQ is used.

3.3 Techniques Applied

User Defined Block chain Implementation: A customized block chain was created, which meant that the organization could establish the consensus type and block format based on the systems need.

SHA Hashing: SHA hashing which is used in the user-defined block chain helps to authenticate data since personal health records are protected from any forms of unauthorized modifications during storage and transmission.

ABAC Integration: For this purpose ABAC policies were set and integrated in the system to control the access based on the user attributes and available context information.

Cryptographic Algorithms: It achieved the method of RSA and ECC algorithms for data encryption and secured key exchange.

4 Design Specification

This section outlines the methods, architecture, as well as the frames that make up the suggested system. It also explains to the user(s) the meaning of any new models or algorithms that may form part of the Proposed System.

Proposed System

A number of critical components and activities are involved in the driving EHRs, as shown in the system architecture given in Figure 1 that consists of the System Manager (Admin) a divided and secured back like emblem. BC Storage, a block chain based storage solution named,

employs distributed ledger technology for its delivery of scalable and easily accessible data storage. The segments of this block chain that address the building block of storage are known as BC Blocks. An icon of the hospital emphasizes the healthcare orientation of the EHR System. The main program for the processing of patient health information is through the EHR System. The Verification System is responsible for the requests for accessing the data that it holds in its custody aiming at maintaining the security and the integrity of the data. This includes the uploading of EHRs by the data owners to BC Storage.

The primary user whose privacy this EHR system must protect is the data owner. When the data owner uploads the Electronic Health Records (EHRs) that need to be kept on block chain storage, Algorithm 1 is utilized for the block construction below, as seen in figure 2. The block generation procedure depicted in figure 3 is clearly shown in the sequence diagram below.

The attribute to be created by the data users is assigned by the data owner, who also provides the decryption key to the data users. Upon uploading the electronic health records, the data owner needs to designate who can access them.

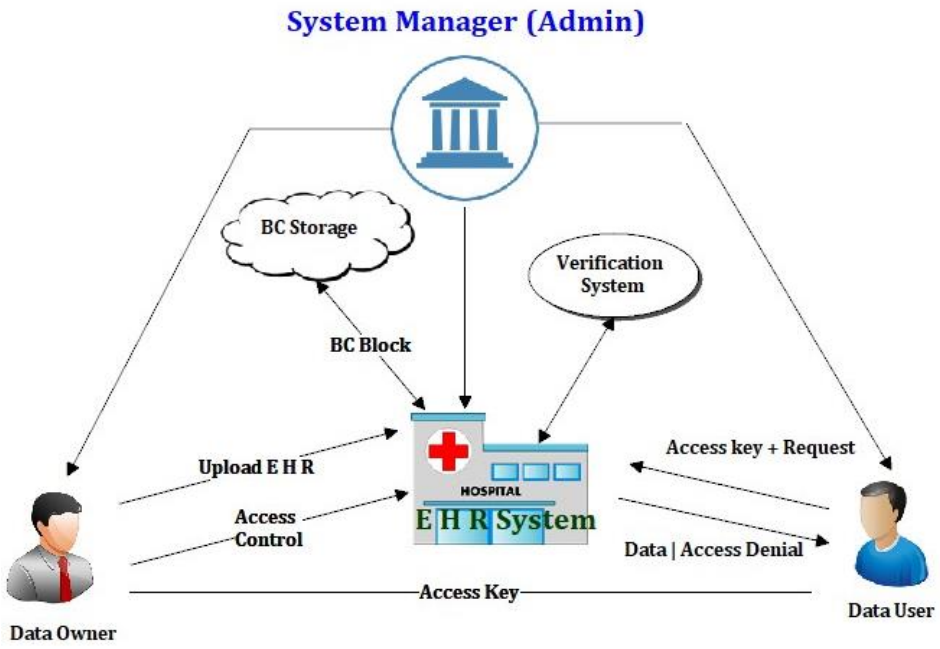

Figure 1: Proposed EHR System Architecture

Algorithm 1: Block Creation Process

Input : Electronic Health Record
Output : Block chain Block
User : Data Owner

```
if N transactions are added in upload queue
    Generate the Root-Hash-code from data
    Fetch Pervious Block Hash code (PBV)
    Form Header PBV-RH-TimeStamp-Nonce
    Encrypt data and create Block Body
    Merge Header and Body to create block
else
    wait and check
```

Figure 2: Block Creation using Algorithm 1

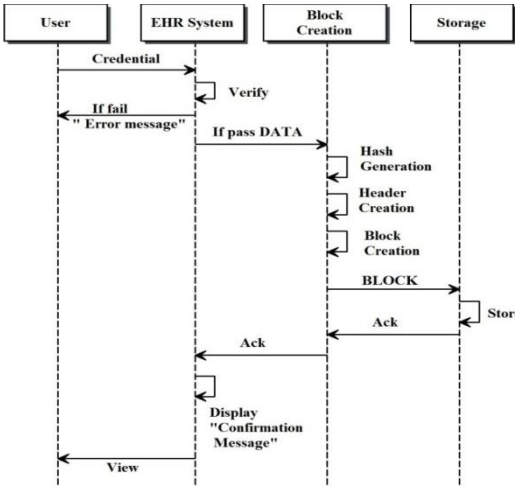

Figure 3: Block Creation Process

Verifying that each block in the block chain is intact is the auditor's responsibility. The use of Algorithm 2 for verification is shown in Figure 3. The sequence diagram that follows clarifies the block verification process that is shown in Figure 4.

Algorithm 2: Block Verification Process

Input : Block ID
Output : Status of the Block
User : Admin

```
if number of Block (N) > 0 then
    List the Block details
    Fetch block to be tested & Extract data
    From the transaction generate Hash Code(1)
    Fetch Previous Block Hash Code
    Compare both Hash Code and show result
else
    Display no block the verify
```

Figure 3: Block Verification Process Using Algorithm2

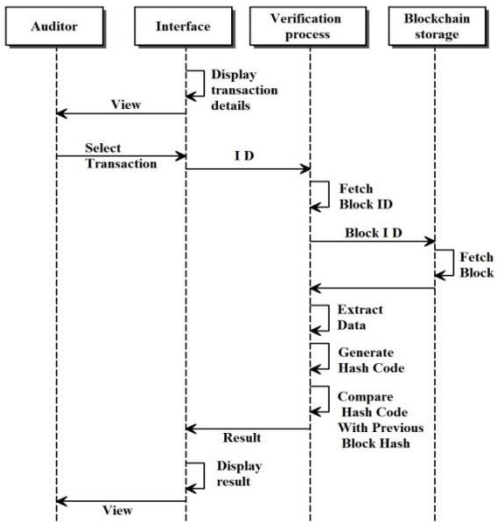

Figure 4: Block Verification Process

The admin user, who is also in responsible of managing the block chain storage settings, will create data owners. There will be unique encryption and decryption keys for every data owner.

4.2 Block chain Design

A block chain is a technique of recording data that minimizes the risks of hacking since it is difficult to tamper with the system. It also works differently in that it serves as a distributed

electronic record in the form of a database. Each block is made up of several transactions; every transaction that occurs generates a new block for all the parties involved in the process. Recalling that block chain is a type of distributed ledger technology (DLT), it records transactions using an unalterable digital signature referred to as a hash. Some nodes are involved in validation and verification in order to enable the completeness of transactions between the parties involved without any intermediaries. Some important values of the block in block chain are Header, which is hashed periodically by miners by changing the nonce value. Previous Block Hash, which links each block to its predecessor. Timestamp, which records the creation time of each document or event. Nonce, a onetime number used in the proof of work process to find a valid solution the Root Hash that helps in tracking blocks. The architecture diagram of block chain is shown in figure 5.

4.3 Attribute Based Access Control (ABAC)

ABAC stands for Attribute Based access control; here the decisions depend on user, resource, and environmental parameters and not on roles to allow or forbid access. When reviewing the limits of access capabilities, it takes into account the categories of resources, users, and other aspects such as the position and time of the process. What is more, ABAC can provide sufficiently precise control because of its flexibility in comparison to conventional constraints of role-based access control in complicated situations when constant restrictions can be insufficient.

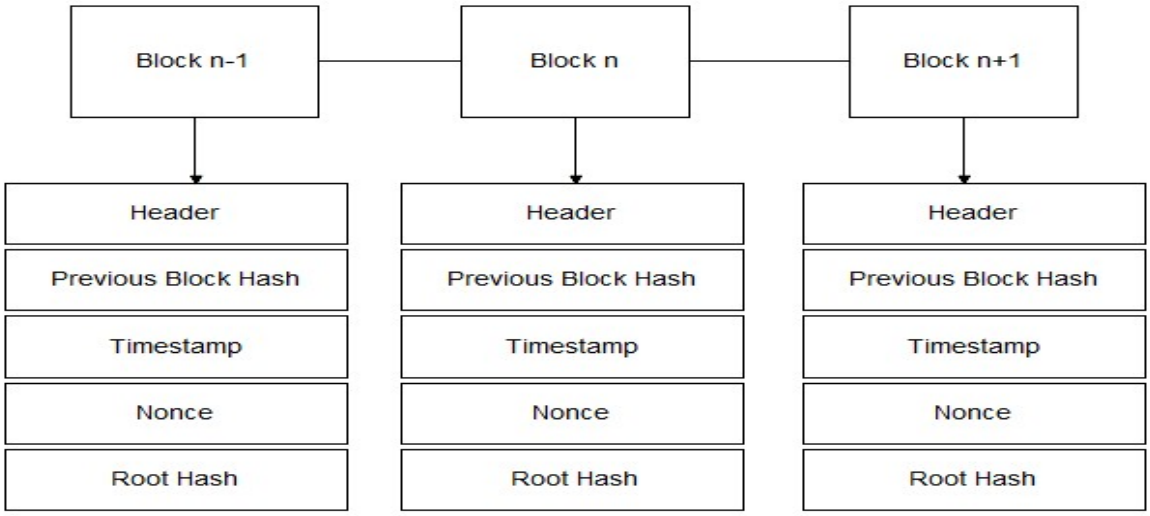

Figure 5: Block chain Architecture

Thus, ABAC makes a great effort to follow the data protection legislation and ensure the IT services and the data are protected from improper access. Launched in 2011 by the Federal Chief

Information Officers Council, ABAC improves authoring structures and enables secure exchange of information.

4.4 Cryptographic Algorithms

RSA Algorithm: an authentication procedure of data, based on player's public key and encryption for secure data transmission. RSA employs a 128 byte key size to enhance the level of security.

ECC Algorithm: a modern-day cryptographic technique that is in some ways more secure than RSA but for smaller key sizes. For encryption and digital signatures, ECC utilizes 32byte keys for these two operations so that the rates of processing and storage can be made efficient.

In this design specification, a detailed account of the system's design, technologies used, and included algorithms is presented. They ensure that the system is capable of utilizing the block-chain and cryptology techniques to securely store and protect the EHRs.

5 Implementation

The last activity in the implementation for the project was to open a general framework for the admin and data owners, as well as creating secure procedures to organize data employing the multiple web pages and features of the project. The system was designed to produce several key outputs: transformation of the data information, the written algorithm code and the secure user communication. Some of key functionalities are stated below,

5.1 Admin Management

Admin Login and Management: An admin operational form (Figure 6) was also used to enable admin authentication into the system after validating the credentials. If an admin is not already logged, then, the system validates the user credential (ID and password) with the data base. Hence, if a card is valid, then it allows entry and welcomes the admin; otherwise, if input is invalid, it instructs the admin to try again. If already logged in, then it goes to the admin home page if not it goes to admin login. Some of the objects that can be managed by admin are data owners, users, and files among others.

Data Owners Management: Creating data owners and listing them became possible due to the web pages (Figures 7). The page for the data owners list checks if the user is an admin. If they are, it selects all records of data owners existing in the database and presents them on the web page. The create data owners page deals with the process of account creation for data owners. This one gather data from a form, verifies if the input email and code have been taken already,

and creates encryption keys. It preserves the details, directs a new email with the login information, and displays a message of success of the submission.

File Management by Admin: List of files of different data owners that can be viewed by everyone along with the details namely the date the file was uploaded, the name of the owner along with the name of the file, and any remarks about the file and its size. This extends a guarantee that only the admin users shall have access to this info. Users Management by Admin: The users list page retrieves a list of users along with their attributes and data owners from the database and then displays this data on an admin page.

5.2 Data Owner Management

Data Owner Login and Management: Data owner login page describes all the activities related to the login process of the data owners. In case the user is not logged in, he or she can log in through his/her email address and Password. If the details are correct they are welcomed and led to the homepage of the site. This page also exhibits a list of users connected to a data owner. If the name of data owner exists in the session, then it pulls out user data from the Database and shows it.

User Creation by Data Owners: The create user page should enable a data owner to create a new user. They can input the required data of the user. First, the system verifies, if the certain email is registered in the system. Otherwise, it preserves the data, delivers the login information to the user, and goes to the list of users.

File Management by Data Owners: Files list in data owner page (Figure 8) is the information of files that have been uploaded by a certain data owner and file access and delete buttons are also provided. This list contains information: what file name it is, what data it contains, when it was created, etc. The data owner file upload page is responsible for uploading and processing files for a specific data owner. It saves the uploading file and reads the file content in order to relieve words' frequency of usage. According to the analysis, it either assigns the file as sensitive or non-sensitive depending on the analysis. For all but the sensitive ones, it stores the files in a cloud service and informs the data owner through email. For sensitive files, it pops up a dialog box for the data owner with message containing an alert message and an option to allow the uploading. In case the data owner chooses 'No' the file is not uploaded and the program does not store any information pertaining to the file. If 'Yes', the file is encrypted through RSA & ECC then stored in the database and an encrypted block is generated for the block chain. It is also responsible for file deletion as well as updating records in the database as contained in the files.

Attribute Addition: To create a domain for data owners, a domain management page was included. It establishes if the parsed domain code is unique, and if the domain name has not been

taken by another person. In case, both are unique, it appends the domain with the calendar ID; in another case, it displays an error message and takes to the domain list page. This functionality also facilitated adding of attributes to domains, which helped in increasing the manoeuvrability in domain management.

5.3 User Management

User Authentication and File Access: The user login interfaces were incorporated for the purpose of identification of the users and grant them authorization to access their documents. Files could be downloaded from the remote server and depending on the current context of the running application then decryption and extraction of files could be done. Files' authenticity was maintained through hash code juxtaposition as part of verification processes.

Below images depict the Admin Management

In figure 6 shows the login page for the Admin. The admin can login through the below shown login page.

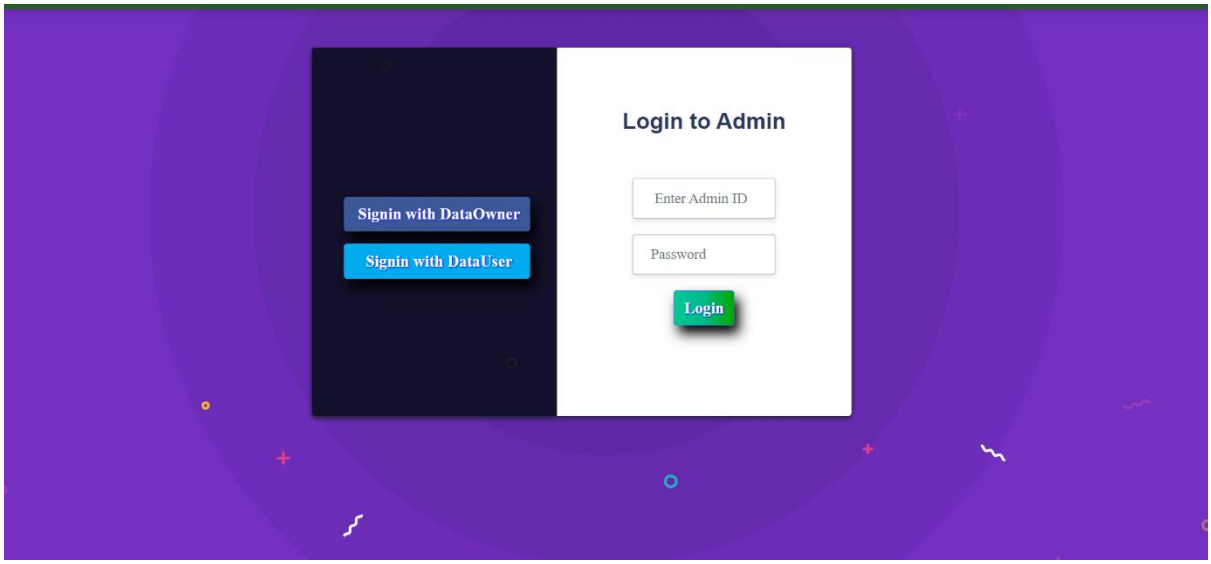

Figure 6: Admin Login

In Figure 7 shows that the admin can list the data owners. It is clearly observed that it enables the entry of the data owner such as data owner's email I'd, username, user I'd, and the password.

Figure 7: Create Data Owner

Below images depict the Data Owner Management

In figure 8 given below shows that the data user can upload and access the file.

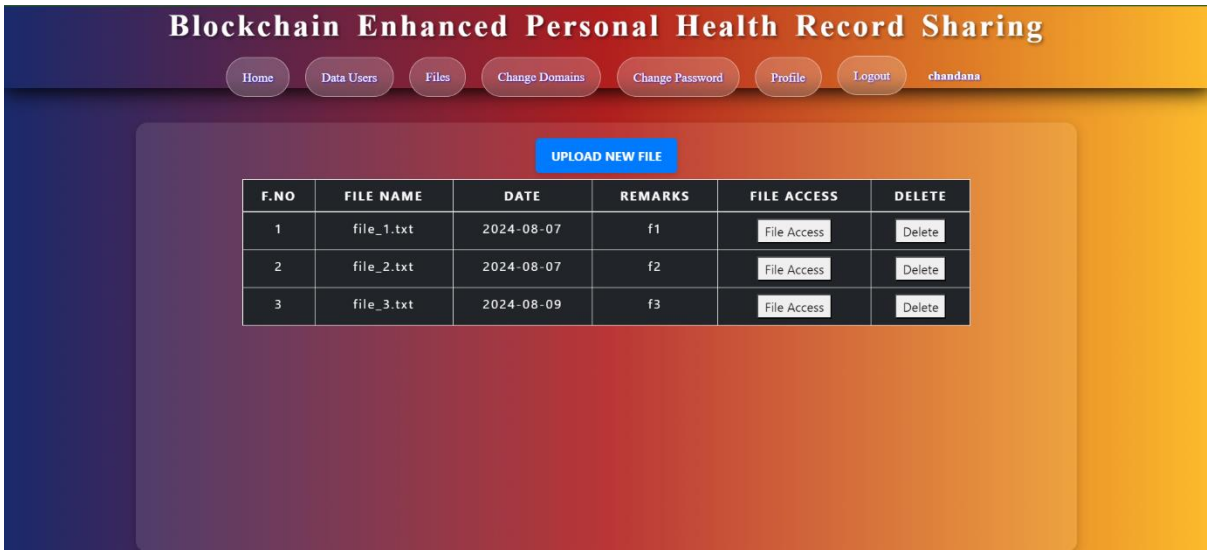

Figure 8: Files List

Below images depict the User Management

In the figure the data user can verify all the files.

Figure 9: User Files with verify option

Technology Stack

Implemented tools and languages included the backend scripting tool Python, web application framework Flask, and database engine MySQL. The front end was coded using HTML, CSS and JavaScript skills that include both the front end and back end. To use increase security, the block chain system was implemented for archive storage and the verification of transactions. RSA and ECC encryption algorithms were used to ensure security to the sensitive data where RSA is strong in its security while ECC is fast in its operation. When designing the system, all the possible available features to allow only authorized admins, data owners as well as users of the data and provide maximum security to the data were incorporated.

6 Evaluation and Discussion

As cited in Guo, S et al. (2022), Block chain prevents data tampering, for instance, avoids data manipulation through aspects such as impermeability, distribution of authority, and hashing. Since data is stored in blocks, once the record is made, the block cannot be altered again in any way. The only way to change a piece of data is to change that block in all the computers and this is not computationally possible. Cryptographic hash enable data integrity where any alteration of the data is picked and consensus mechanisms enable validation of new blocks preventing the block chain from malicious data.

(EJable, 2023) When it comes to block chain security, their level of security differs based on the implementation, consensus algorithm, network and security features. Some of the block chains in public domain such as bit coin and Etherum among others have been invaded but begin to stand. Overall, private block chains are comparatively safe. The general security essentially relies on the lowest denominator. The probability of a 51% double-spending attack on Bit coin is approximately 0.1% per year. Security is still an open research subject and methods are in constant development. Albeit, block chain systems are not impregnable; the risk significantly rises as the value stored in the block chain system rises.

Health records contain some of the most private information a person can have: medical history, diagnosing, treatment, etc. It is crucial to store, manage and share these records in a secure method to safeguard the patient's privacy and the contents of the records in health care Wu et al. (2022). Conventional approaches of holding EHRs in voluminous centralized data bases have been observed to be easily susceptible to hacking, unauthorized interface, and manipulation Yeo, L. H. and Banfield, J., (2022). Consequently, new block chain technology has been developed to solve some security challenges Hoang et al., (2020). In this section of the paper, a prototype model was created hence using a User Defined block chain to examine the potentials of block chain in EHR management. The use of User Defined block chain led to the ability to define the consensus mechanism and the structure of the blocks with all the conditions required by the healthcare domain in mind. This approach allowed us to integrate the block chain system with the requirement attributed to EHRs like high data privacy, high data integrity, and high data accessibility.

To increase the level of protection of the system, we introduced several cryptographic algorithms into it. SHA was used for checking the integrity of storing data in the block chain; any change in the records of the block chain would be easily noticeable. Furthermore, for encryption and decryption the RSA and ECC algorithms has been used as well and the key size for RSA was 1024 bits. RSA was proven to have sufficient public-key encryption capability; therefore, ECC was the better choice for the identical security standards with lower computational costs and higher system throughput. Another development of the security model was the Attribute Based access control (ABAC) where finer control over the access to EHRs could be provided on the basis of the attributes such as role, department and consent from the patient. This dynamic access control mechanism made sure that only particular users, those who were supposed to work with certain patients, could work with the records and not just anyone could view or alter a patient's records, thus, adhering to the concepts of need to know and patients' privacy rights.

Application of this block chain prototype model showed that block chain was viable and could improve EHR nature and use in various ways. In this way, with help of block chain the system guaranteed reliability for storing, sharing, and organizing the health records while strengthening

the patient privileges of confidentially and data security. Cryptographic algorithms and ABAC maintained the confidentiality of data and kept it secure at each stage of the data lifecycle. With the help of the proposed prototype model, it was possible to demonstrate the advantages of block chain utilization in the field of EHRs; however, more studies and advancements are required to enhance the approach in terms of its capability to meet the requirements connected with scalability, interoperability, and compliance with legal regulations. If block chain technology is integrated into the different settings of healthcare, its advancement can open up improvements in the management of health records thus enhancing the welfare of patients.

The next test cases affirm the block chain data's integrity and the accurate ability of the algorithm to identify tampering as well as prove the existence of untampered information.

Test Case 1: Verification of Untampered Data

Objective: *Ensure you can confirm that data on the existing block chain has not been altered in any way.*

1. Setup:

- Ensure that the current operation of the systems is correct and the block chain as well as the hashing is also properly set.
- Load a number of PHR data, which had been prepared in advance and not altered in any way, into the system.

2. Action:

- Retrieve data from the block chain of the PHR.
- Obtain the value of the hash that is stored in the block chain.
- Calculate the hash value of the data that was obtained using the same SHA hashing algorithm as in the previous step.
- Check if the computed hash matches the hash value of the current block that exists on the block chain.

3. Expected Result:

- The hash value that is generated should be equal to hash value stored on the block chain meaning that data has not been altered.

4. Outcome:

- If the hash values match, the data is confirmed to be untampered.

Test Case 2: Verification of Tampered Data

Objective: *Ensure that manipulation of data is alert by the system.*

1. Setup:

- Make sure that the system is running as it should with the right set up of the block chain and the hashing.
- Introduce a set of PHR data into the system and check that it is properly recorded.

2. Action:

- Manually update the archived information (for instance, change a health record or modify something in the structure of the PHR data).
- Get the modified data from the block chain.
- Get the associated hash value which is stored on the block chain.
- Use the SHA hashing algorithm to determine the hash value of the modified data.
- Compare the calculated hash value with the hash value that is already stored on the block chain.

3. Expected Result:

- The computed hash value should be different from the hash value stored on the block chain, which confirms that the data has been manipulated.

4. Outcome:

- In the event that the hash values are not matching, then the system should be able to detect the tampering of the data and therefore flag the data as corrupt.

The system was able to identify the alteration of the tampered data as well as verify the unaltered data truly remained unaltered, further proving its effectiveness in both scenarios.

7 Conclusion and Future Work

From this study, it have been able to establish that block chain technology has the credentials to revolutionize the EHR management through increased security and efficiency. Thus, a prototype system was created with the help of User Defined block chain, SHA, RSA, and ECC cryptographic algorithms, as well as ABAC that allowed meeting the identified major limitations of data privacy, integrity, and accessibility in the healthcare domain. In addition, the prototype model anchored the confidence of the stakeholders through the integration of a secure platform and storage system of EHRs that also offered a systematic audit trail of transaction. Due to the implementation of the necessity of ABAC, access to the patient record was restricted and could be granted only to people with certain roles and permissions.

The next research should therefore aim at improving the scalability, integration, and the legal issues of block chain based EHR systems. This includes defining data transfer protocol from one block chain network to another and to the conventional healthcare system, global data protection compliance and network efficiency by methods such as sharding and off chain operations. However, to promote the wider acceptance of such innovations in the groups of Healthcare professionals as well as patients, the aspects of the UI/UX design will be essential. If such challenges are addressed to, block chain technology will be able to deliver it's full potential of transforming the EHR management, thereby bringing in a more secure and patient centered health system.

Acknowledgement

I would like to thank my supervisor Eugene Mclaughlin for guiding me through the research with his valuable knowledge and time. I would like to thank my colleagues for keeping me motivated and guiding me thorough the steps in my research. Thank you to my college for giving me an opportunity to do this research.

References

Awadallah, Ruba, et al. "An integrated architecture for maintaining security in cloud computing based on block chain." *IEEE Access* 9 (2021): 6951369526.

Awaysheh, Feras M., et al. "Security by design for big data frameworks over cloud computing." *IEEE Transactions on Engineering Management* 69.6 (2021): 36763693.

Benil, T., and J. J. C. N. Jasper. "Cloud based security on outsourcing using block chain in Ehealth systems." *Computer Networks* 178 (2020): 107344.

Cerchione, Roberto, et al. "Block chain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem." *Technovation* 120 (2023): 102480.

Chelladurai, MrsUsharani, Seethalakshmi Pandian, and KrishnamoorthyRamasamy. "A block chain based patient centric electronic health record storage and integrity management for eHealth systems." *Health Policy and Technology* 10.4 (2021): 100513.

Chinnasamy, P., and P. Deepalakshmi. "HCACEHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud." *Journal of Ambient Intelligence and Humanized Computing* 13.2 (2022): 10011019.

Chouhan, Arun Singh, et al. "Block chain based EHR system architecture and the need of block chain inhealthcare." *Materials Today: Proceedings* 80 (2023): 20642070.

EJable, 2023. Data Immutability and Integrity in Block chain Network. EJable. Available at: https://www.ejable.com/block chaindataimmutabilityintegrity.

Getzen, Emily, et al. "Mining for equitable health: Assessing the impact of missing data in electronic health records." *Journal of biomedical informatics* 139 (2023): 104269.

Groenhof, T. Katrien J., et al. "Data mining information from electronic health records produced high yield and accuracy for current smoking status." *Journal of clinical epidemiology* 118 (2020): 100106.

Guo, S., 2022. How Block chain Prevents Data Tampering: Mechanisms and Examples. Block chain Simplified. Available at: https://www.block chainsimplified.com/block chainpreventsdatatampering.

Hajian, Ava, Victor R. Prybutok, and HsiaChing Chang. "An empirical study for block chain based information sharing systems in electronic health records: A mediation perspective." *Computers in Human Behavior* 138 (2023): 107471.

Hoang, V.H., Lehtihet, E. and GhamriDoudane, Y., 2020, June. Privacypreserving block chain based data sharing platform for decentralized storage systems. In *2020 IFIP Networking conference (networking)* (pp. 280288). IEEE.

Jusak, Jusak, et al. "A new approach for secure cloud based electronic health record and its experimental testbed." *IEEE Access* 10 (2021): 10821095.

Kanwal, Tehsin, et al. "Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud." *Computer Standards & Interfaces* 78 (2021): 103522.

Keshta, Ismail, and Ammar Odeh. "Security and privacy of electronic health records: Concerns and challenges." *Egyptian Informatics Journal* 22.2 (2021): 177183.

Kormilitzin, Andrey, et al. "Med7: A transferable clinical natural language processing model for electronic health records." *Artificial Intelligence in Medicine* 118 (2021): 102086.

Lee, JungSan, et al. "Medical block chain: Data sharing and privacy preserving of EHR based on smart contract." *Journal of Information Security and Applications* 65 (2022): 103117.

Shamshad, Salman, et al. "A secure block chain based ehealth records storage and sharing scheme." *Journal of Information Security and Applications* 55 (2020): 102590.

Sharma, Yogesh, and BalamuruganBalamurugan. "Preserving the privacy of electronic health records using block chain." *Procedia Computer Science* 173 (2020): 171180.

Sivan, Remya, and Zuriati Ahmad Zukarnain. "Security and privacy in cloud based ehealth system." *Symmetry* 13.5 (2021): 742.

Tanwar, Sudeep, Karan Parekh, and Richard Evans. "Block chain based electronic healthcare record system for healthcare 4.0 applications." *Journal of Information Security and Applications* 50 (2020): 102407.

Walid, Redwan, et al. "Cloud based encrypted ehr system with semantically rich access control and searchable encryption." *2020 IEEE international conference on big data (Big Data)*. IEEE, 2020.

Walid, Redwan, Karuna P. Joshi, and SeungGeol Choi. "Secure cloud ehr with semantic access control, searchable encryption and attribute revocation." *2021 IEEE international conference on digital health (ICDH)*. IEEE, 2021.

Wang, Yanshan, et al. "Unsupervised machine learning for the discovery of latent disease clusters and patient subgroups using electronic health records." *Journal of biomedical informatics* 102 (2020): 103364.

Wu, ChiShin, et al. "Using text mining to extract depressive symptoms and to validate the diagnosis of major depressive disorder from electronic health records." *Journal of affective disorders* 260 (2020): 617623.

Wu, G., Wang, S., Ning, Z., Zhu, B. (2022). Privacypreserved electronic medical record exchanging and sharing: a block chain based smart healthcare system. *IEEE Journal of Biomedical and Health Informatics*, 26(5), 19171927.

Yeo, L.H. and Banfield, J., 2022. Human factors in electronic health records cybersecurity breach: an exploratory analysis. *Perspectives in health information management*, *19*(Spring).

Zarour, Mohammad, et al. "Evaluating the impact of block chain models for secure and trustworthy electronic healthcare records." *IEEE Access* 8 (2020): 157959157973.

Zhu, QingHua, et al. "Task scheduling for multicloud computing subject to security and reliability constraints." *IEEE/CAA Journal of AutomaticaSinica* 8.4 (2021): 848865.