International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Secure EHR: A Blockchain-Based Approach for Decentralized and Security Management of Electronic Health Records

Shashank[1]
[1] PG scholar, Department of MCA, Dayananda Sagar College of Engineering, Bangalore,
Sp8819762@gmail.com

Alamma B.H[2]
[2] Assistant professor Department of MCA, Dayananda Sagar College of Engineering, Bangalore
Alamma-mcavtu@dayanandasagar.edu

Abstract:
The Electronic Health Record (EHR) is a digital representation of a patient's medical history, encompassing demographics, medications, past medical history, laboratory data, and reports such as X-rays. However, the current centralized storage of EHRs limits patients' control over their own medical data and poses challenges for secure sharing among different healthcare providers. To address this issue, we propose a decentralized and secure approach using InterPlanetary File Systems (IPFS) for storage and the RSA algorithm for record encryption. By leveraging the combination of block chain and cryptography, our solution aims to provide patients with full control over their health records while ensuring data integrity.
keywords: EHR, IPFS, RSA, Block chain

I. INTRODUCTION

The Electronic Health Record (EHR) is a comprehensive digital representation of a patient's medical history, encompassing vital information such as demographics, medications, past medical conditions, laboratory data, and diagnostic reports like X-rays [1]. EHRs offer numerous advantages over traditional paper records, including quick access to patient information, standardized documentation, and improved tracking, which can lead to reduced errors and improved healthcare outcomes.

However, the current centralized storage model of EHRs poses several challenges, particularly regarding patients' control over their own medical data and secure sharing among different healthcare providers [1]. Patients often lack access to their complete health records, and sharing data between institutions becomes cumbersome due to incompatible systems and concerns about data security and privacy.

To address these issues, our proposed solution aims to introduce a decentralized and secure approach to EHR management. By leveraging the powerful combination of block chain technology and cryptography, we intend to grant patients full control over their health records while ensuring data integrity and confidentiality [2]. Block-chain, a cryptographic protocol that creates a tamper-resistant chain of records, allows for decentralized data management [2]. We suggest utilizing InterPlanetary File Systems (IPFS) for the storage and sharing of digital health records [5]. IPFS, being a decentralized protocol, enables data distribution and retrieval across multiple computing devices by using content-addressing to uniquely identify each file [5]. Ensuring the confidentiality of health records is paramount to protect patient privacy. Asymmetric Key Cryptography, such as the RSA algorithm, can be employed to encrypt the data before uploading it to IPFS [3]. This encryption method provides an added layer of security, making the records accessible only to authorized parties. The combination of block chain technology and cryptography offers a robust solution to the challenges faced by the current EHR systems. Patients can have more control over their health data, granting access to specific healthcare providers when needed, while maintaining the privacy and integrity of the information.

II. LITERATURE SURVEY

This paper provides an overview of the ethical issues associated with electronic health records (EHRs). It discusses the challenges related to data privacy, security, and patient autonomy in the context of centralized storage systems. The authors highlight the need for decentralized and secure approaches to address these issues effectively [1].

This systematic review explores the integration of block chain technology with electronic health records (EHRs). The paper discusses the advantages of using block chain for EHRs, including improved data integrity, security, and interoperability. It also examines challenges such as scalability, regulatory compliance, and the need for standardization. The review highlights the potential of block chain technology to enhance the security and accessibility of healthcare data [2].

In this survey, various cryptographic encryption algorithms are explored. The paper discusses symmetric key encryption, asymmetric key encryption, and hybrid encryption techniques. It compares and evaluates different algorithms based on factors such as security, efficiency, key management, and cryptographic strength. The survey provides a comprehensive understanding of different encryption algorithms and their suitability for different use cases [3].

This survey focuses specifically on symmetric key encryption techniques. "It conducts a comparative analysis of well-known symmetric encryption algorithms, including DES, AES, Blowfish, and RC4." The paper evaluates these algorithms based on their security features, performance, and key length requirements. The study offers valuable insights into the respective strengths and weaknesses exhibited by each algorithm, aiding in the selection of an appropriate encryption technique for specific applications [4].

This research paper introduces a novel approach for a secure data sharing platform by leveraging the integration of block chain technology and IPFS. It explores the benefits and challenges of utilizing these technologies for data security and decentralization. The paper discusses the potential advantages of using block chain and IPFS, such as data immutability, transparency, and distributed storage. It also addresses the challenges of scalability, performance, and interoperability. The proposed solution aims to establish a robust and tamper-proof system for secure data sharing [5].

This review paper provides an in-depth analysis of the Secure Hash Algorithm (SHA) and its variants. It explores the properties, applications, and security aspects of different SHA algorithms, including SHA-1, SHA-2, and SHA-3. The authors discuss the strengths and weaknesses of each variant, highlighting their cryptographic properties, collision resistance, and computational efficiency. The paper offers insights into the use cases and comparative analysis of SHA algorithms, aiding in the selection of suitable hashing algorithms for various applications [6].

III.METHODOLOGY

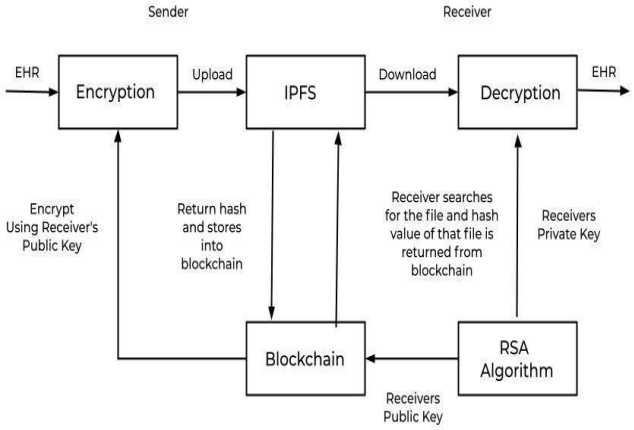

Figure (1) Flow diagram of EHR sharing system

To enhance the security and sharing of Electronic Health Records (EHRs),multi-step process is proposed. To enhance data security, the initial step involves encrypting the Electronic Health Records (EHRs) using the recipient's public key. The encryption process is facilitated by employing the RSA algorithm [3]. This algorithm generates both private and public keys, with the public key being stored securely within the block chain [3].

Following the encryption process, the encrypted EHR file is uploaded to the InterPlanetary File System (IPFS), which serves as a decentralized protocol for file storage and sharing. Once successfully uploaded, IPFS generates a unique hash value for the file, which is then recorded in the block chain for future referencing and retrieval purposes. [5].

When the intended receiver needs to access the encrypted EHR file, they can search for the corresponding hash value within the block chain [5]. Upon finding the matching hash value, the receiver can utilize it to download the encrypted file from IPFS. To decrypt the file and access its contents, the receiver employs their private key, which is kept confidential and known only to them [3].

A. Generating Public Private key pairs:

The RSA algorithm serves as an illustration of an asymmetric cryptography algorithm, functioning with two

separate keys: the public key and the private key [3]. When data is encrypted with the public key, it can only be decrypted using the corresponding private key. To maintain transparency and facilitate accessibility, the public key is openly stored on the block chain, rendering it visible to the public [3]

B. Encrypting EHR:

To secure Electronic Health Records (EHRs), they are encrypted using the public key associated with the individual to whom the health record belongs[3].

C. Uploading Encrypted file to IPFS:

The InterPlanetary File System (IPFS) is a distributed protocol and peer-to-peer network designed to facilitate the storage and sharing of data among various computing devices [5]. By uploading the encrypted file onto IPFS, a hash value is generated and recorded on the block chain, making it publicly accessible [5].

D. Retrieving files from IPFS:

To retrieve the content from IPFS, one can utilize the hash value stored in the block chain. However, since the content is encrypted, decryption requires the use of the corresponding private key[5].

E. Key Generation Algorithm:

Step 1**:** Generate the RSA modulu

Choose any two large prime numbers 'q' and 'r'. And Compute the multiplication of 'q' and 'r' and assign it as 'z': z = q * r

Step 2**:** Compute Euler's Totient Function.

Compute ϕ(z) = (q - 1) * (r - 1), which represents the count of "positive integers" less than 'z' that are relatively prime to 'z'.

Step 3**:** Choose the Public Key

Choose a number 'a' should greater than one and less than ϕ(z) such that 'e' has no common factor with ϕ(z) except one. This can be verified by checking that gcd(a, ϕ(z)) = 1.

Step 4: Calculate the Private Key

To determine the modular multiplicative inverse of 'a' modulo ϕ(z), let's denote the inverse as 'd'. It must satisfy the equation: (a * d) mod ϕ(z) = 1.

The resulting public key is the pair of numbers (a, z), which is made public.
The resulting private key is the pair of numbers (d, z), which should be kept confidential.

F. Encryption Algorithm:

Encryption-Algorithm(q,a,z)

Suppose there is a sender who intends to encrypt a plaintext message 'P' using the recipient's public key (z, a). The encryption algorithm can be described as follows:

Step1: To encrypt the plaintext message.

To compute the ciphertext 'C' using the formula: C = (P^e) mod z.

'P' represents the plaintext,

'a' is the public exponent,

'z' is the modulus, and '^' denotes exponential

The resulting 'C' is the ciphertext.

G. Decryption Algorithm:

Decrypt-Algorithm(EHR, {d, z})

Assuming the receiver possesses the private key 'd', the decryption algorithm is as follows:

Step1: To decrypt the ciphertext 'C' using the private key.

compute the plaintext 'P' using the formula: P = (C^d) mod z.

'C' represents the cipher-text,

'd' is the private exponent,

'z' is the modulus, and '^' denote exponential

'P' is the plaintext.

H. Hashing Algorithm:

This algorithm describes the process of generating a hash value for a given message. It ensures that the length of the hash remains the same regardless of the input size, maintaining data integrity and making it difficult to reverse-engineer the original message [6].

Step 1: Padding the Message

To satisfy the requirement of having a message length precisely 64 bits less than a multiple of 512, it is necessary to append additional bits to the original message. The appended bits should begin with a '1' bit and be followed by '0' bits until the desired length is achieved. This ensures that the message conforms to the specified length criteria.

Step 2**:** Modulo Calculation.

Calculating the modulo of the original message (without padding) using a specific value, such as 2^64.
Append the resulting value to the padded bits, creating a message block that is a multiple of 512 bits.

Step 3: Initialization

Set the hash buffers to their initial or default values as part of the initialization process.

Step 4: Processing the Message

The message is divided into 512-bit chunks, and each chunk undergoes 64 rounds of operations. At each round, calculate a value called W(i) using specific functions and previous values:
$W(i) = W^{(i-16)} + \sigma^0 + W^{(i-7)} + \sigma^1$.

Step 5: Finalizing the Hash

The output generated from each round serves as the input for the subsequent round, creating a chain of processing. This process continues iteratively until all bits of the message have been processed.

The result of the last round for each message block gives the hash for the entire message.

The length of the hash is typically 256 bits.

I. Linear Search Algorithm:

By utilizing the Linear Search Algorithm, you can effectively search for a specific EHR using its corresponding hash code. However, it's important that the efficiency of the search depending on the size of the array and the distribution of hash codes.

LinearSearchAlgorithm(A, N, VAL):

Step 1: Initialize POS to -1.

Step 2: Initialize I to 1.

Step 3: Continue executing the following steps as long as the condition "I is less than or equal to N" is satisfied.

Step 4: Check if A[I] is equal to VAL. - If true, set POS to I and print POS. - Go to Step 6.

Step 5: Increase the value of I by 1.

Step 6: Check if POS is still -1. - If true, print "VALUE IS NOT PRESENT IN THE ARRAY".

Step 7: Exit the algorithm.

J. Encrypting the Electronic Health Record:

Encrypting the “Electronic Health Record” involves converting sensitive patient health data into a secure and unreadable format. This process uses the receivers public key to encrypt the data, ensuring confidentiality during transmission or storage.

Input: Patient's Electronic Health Record (EHR), Public key of the Receiver {e, n}

BEGIN

Encrypt the EHR using the public key of the receiver.
Encrypted-EHR = encryptionAlgorithms
(EHR, {e, n})

Return encryptedEHRs

END

K. Searching and Decrypting the electronic Health Record:

Searching and Decrypting the “Electronic Health Record” involves two steps. Firstly, it searches for the encrypted Electronic Health Record using a hash value present on the block chain. Secondly, it decrypts the encrypted record using the private key of the receiver to regain access to the original, readable “Electronic Health Record”.

Input: Encrypted “Electronic Health Record”, Private key of the Receiver {d, n}

BEGIN
Search for the Electronic Health Record using the hash value present on the block chain.

EHR = LinearSearchAlgorithm(hash-Value)

Decrypt the Electronic Health Record using the private key of the receiver.decryptedEHRs = decryptAlgorithms(EHR, {d, n})
END

IV. BENEFITS

The proposed blockchain-based approach for secure and decentralized management of electronic health records (EHRs) offers several benefits. It empowers patients by giving them control over their health records, ensuring privacy and autonomy. The use of blockchain technology ensures data integrity and immutability, making it difficult to tamper with the records. Secure sharing is enabled through InterPlanetary File Systems (IPFS) and RSA encryption, allowing authorized recipients to access encrypted EHRs. The approach enhances privacy, security, and interoperability while reducing costs and complexity. It enables efficient data access, supports medical research, and ensures compliance with data regulations. Overall, the proposed approach has the potential to revolutionize EHR management by prioritizing patient control, data security, and seamless data sharing among healthcare providers.

V. CONCLUSION

This paper examines the potential advantages associated with the integration of block chain technology and IPFS in the healthcare sector for the efficient storage and management of electronic health records (EHRs). Additionally, we have developed a user-friendly interface that simplifies the process of uploading and retrieving EHRs to and from IPFS. To ensure data security and privacy, we have employed asymmetric encryption techniques to encrypt the EHRs before uploading them to IPFS. As a result, the uploaded files are stored in an encrypted format, and a unique hash value is generated for each file on IPFS, facilitating easy retrieval. By adopting this approach, we aim to improve the storage and accessibility of EHRs while maintaining their confidentiality

REFERENCES

[1] Fouzia F Ozair, Nayer Jamshed, Amit Sharma, Praveen Aggarwal. "Ethical issues in electronic health record: A general overview". Perspectives in clinical research, April 2015. DOI: 10.4103/2229-3485.153997

[2] André Henrique Mayer, Cristiano André da Costa, Rodrigo da Rosa Righi. "Electronic health records in a Blockchain: A systematic review". Research Article, Volume 26, Issue 2, September 30, 2019. DOI:10.1177/1460458219866350

[3] Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris. "A Survey on the Cryptographic Encryption Algorithms". International Journal of Advanced Computer Science and Applications, November 2017. DOI:10.14569/IJACSA.2017.081141

[4] Monika Agrawal, Pradeep Mishra. "A Comparative Survey on Symmetric Key Encryption Techniques". International Journal on Computer Science and Engineering, May 2012. DOI: 10.12691/iscf-3-1-1

[5] Muqaddas Naz, Fahad A. Alzahrani, Rabiya Khalid, Nadeem Javaid. "A Secure Data Sharing Platform using Blockchain and IPFS". Sustainability 11(24), December 2019. DOI:10.3390/su11247054

[6] Sahu, Aradhana & Ghosh, Samarendra, “Review Paper on Secure Hash Algorithm With Its Variants”,2017. DOI:10.13140/RG.2.2.13855.05289