Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

Med-block: Secure Health Record Management System Using Blockchain with Ipfs

Mrs. D. Mohanapriya, S.Suresh Kumar, P.J.Vivin Shanker, M.Mukesh, M.Sathish
Assistany Professor – Computer Science and Engineering, Nandha College of Technology, Erode, Tamil Nadu
UG – Computer Science and Engineering, Nandha College of Technology, Erode, Tamil Nadu

ABSTRACT- **In recent years, the digitization of healthcare records has transformed the way patient information is stored and accessed. Traditional centralized storage systems have proven vulnerable to various cyber threats, prompting the exploration of decentralized technologies like blockchain and Inter Planetary File System (IPFS) for securing health record management systems. This project focuses on the design and implementation of a secure health record management system leveraging the combined strengths of blockchain and IPFS. Blockchain, known for its immutable and transparent nature, provides a tamper-proof ledger for recording transactions related to patient health records. IPFS, on the other hand, offers a distributed and decentralized file storage solution, ensuring data availability and resilience against single points of failure. The proposed system architecture involves the integration of blockchain for transaction management and data integrity verification, Through smart contracts, access control mechanisms, and encryption techniques, the system ensures that only authorized parties can access and modify patient data, maintaining confidentiality, integrity, and availability throughout the data lifecycle. This project aims to contribute to the ongoing efforts in revolutionizing health record management through blockchain and IPFS technology, providing a secure and efficient solution for managing sensitive medical data in an increasingly digitized healthcare landscape.**

Keywords**: blockchain, IPFS (Interplanetary file system), health record management, confidentiality, decentralisation, smart contracts, cryptography**

1. INTRODUCTION:

Information technologies introduce a number of resources and benefits to the healthcare field. Electronic Health Records, health records, such as patient's medical history, are one of the most widely employed resources, providing a wide view of a patient's medical status. Health records are commonly originated and shared with collaborators (e.g., physicians, nurses) through cloud computing systems, which results in a more convenient approach to managing such records. Cloud-based systems, however, introduce security challenges in healthcare. A recent report shows that healthcare data breaches are highly common, wherein several of them are classed as unauthorized access, which may lead to inappropriate use of health records (e.g., unwanted advertisements or lower chances of conquering a job opportunity).

Due to security vulnerabilities, various countries (e.g., USA, Brazil, and those from European Union) have established regulations defining health records as sensitive data that should be shared only under patient consent. Such regulations define several requirements, which we call health record properties. For instance, only authorized collaborators should access health records (confidentiality and access control properties). Mechanisms must also exist to legitimately grant access to records in emergency situations (emergency access property), and to anonymized records for research purposes (anonymity property). Besides, the properties of access revocation and interoperability must also be addressed.

Those properties motivate the design of solutions to secure healthcare information systems. A number of literature proposals provide schemes based on centralized servers to store and share health records. The security of such solutions rely on the fact that the server is trusted not to disclose sensitive data, such as information related to user credentials and patient records. This results in a single point that, when compromised, can make the entire system fail. Moreover, these solutions address only a subset of health record properties, while not fulfilling fundamental ones.

In Med-Block, we provide the following novel contributions a blockchain-based protocol (Med-Block), based on our previous work which enhances the schemes employed in the previous protocol to fulfil the security properties of confidentiality and interoperability an analysis of Med-Block, explaining how it satisfies health record properties, and comparing it with related work and an experimental evaluation of a Med-Block Proof of Stake (PoS), showing that it can reduce from 27% up to 91% the time to access health records, and reduce up to 53% client-side memory overhead, compared to related work.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

2. PROPERTIES OF HEALTH RECORDS

Because health records are targeted by cybercriminals, several countries established regulations requiring any entity to employ security measures when handling health data. The Health Insurance Portability and Accountability Act (HIPAA), enacted by the United States Congress in 199, provides guidelines that must be observed by all national healthcare organizations (e.g., hospitals). In 2016, the European Union has approved the General Data Protection Regulation (GDPR), recognizing that health records need special limitations regarding access and treatment through appropriate security mechanisms. Inspired by the GDPR, Brazil's government enacted the General Law for Personal Data Protection (LGPD) that presents similar principles.

- Confidentiality: Technical measures must be adopted to keep health records inaccessible and/or unintelligible for parties that have no permission to gain any knowledge about them.
- Access control: Patients must own the right to control who accesses their health records, providing consent for any collaborator or type of collaborator that will have access to the records.
- Integrity: Health records must be protected against unauthorized modification and deletion.
- Revocation: Patients have the right to revoke, at any moment, the consent given for any collaborator to access their records.
- Emergency access: In case of emergency situation patient cannot give consent to access records by the doctors. so, to tackle this scenario, patient will add his emergency person to the system, then in emergency situation the emergency person can give consent to access records by the doctor in behalf of the patient.
- interoperability: Service providers like insurance company, hospitals, physician etc… can also operate with this system by register themselves with the system by reaching the particular administrator in the organizations who owns this system.
- Decentralisation: Decentralization of medical records involves distributing patient information across a network of computers, reducing reliance on a central authority. This approach enhances security, privacy, and accessibility of health data, empowering individuals to control their own information. Decentralized systems also enable seamless sharing of medical records among healthcare providers, improving the overall quality of care.

3. BUILDING BLOCKS

A. CRYPTOGRAPHIC PRIMITIVES

- PUBLIC KEY ENCRYPTION

  Public key encryption, exemplified by the RSA algorithm, uses a pair of keys: a public key, which is widely distributed and used to encrypt data, and a private key, which is kept secret and used to decrypt the data. In RSA encryption, the public and private keys are mathematically related but computationally infeasible to derive one from the other.

- ONE-WAY HASH FUNCTION

  A hash function (e.g., SHA-256) is a deterministic mathematical algorithm that receives a message m as input and outputs a fixed-size hash value $H(m)$. For a specific message m, this function always outputs the same hash value.

- SYMMETRIC KEY ENCRYPTION

  Symmetric key encryption, exemplified by the Advanced Encryption Standard (AES), uses a single key for both encryption and decryption of data. AES is a symmetric key algorithm that is widely used for securing sensitive information due to its efficiency and security. In AES encryption, the same key is used to both encrypt and decrypt the data, making it essential for both the sender and receiver to have access to the secret key.

B. BLOCKCHAIN

Blockchain is a distributed ledger technology that enables secure, transparent, and immutable record-keeping of transactions across a network of computers. The basic idea behind blockchain is that data is stored in blocks that are linked together in chronological order to form a chain. Each block contains a cryptographic hash of the previous block, along with transaction data, and is secured through consensus mechanisms like Proof of Stake (PoS). This structure ensures that once data is recorded, it cannot be altered without changing all subsequent blocks.

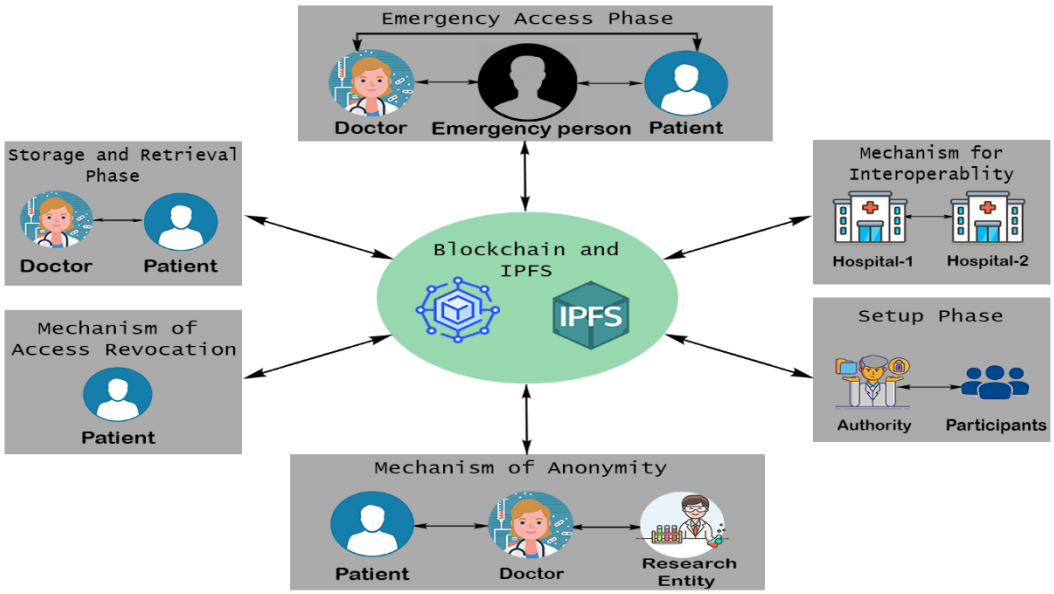
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

In the health sector, blockchain technology is revolutionizing the way medical records are managed and shared. By storing health records on a blockchain, patients can have greater control over their data, granting access to healthcare providers as needed while maintaining privacy and security. Additionally, blockchain can improve the interoperability of health systems by providing a unified platform for exchanging medical information securely.

One advantage of public blockchains over private blockchains is their decentralized nature. Public blockchains are open to anyone and are maintained by a distributed network of nodes, making them highly resilient to censorship and tampering. This decentralization ensures that no single entity has control over the blockchain, enhancing transparency and trust in the system. Additionally, public blockchains are more secure against attacks as they rely on a large number of independent nodes to validate transactions.

The existing system employs Ciphertext-Policy Attribute-Based Encryption (CP-ABE), known for its computational complexity and memory overhead, making it slow and resource-intensive. Additionally, the current system is centralized, relying on a private blockchain for data management and security. In contrast, our proposed system introduces a more efficient approach by utilizing the Advanced Encryption Standard (AES) with RSA encryption. AES with RSA is renowned for its speed and reduced memory footprint, offering a faster and more resource-efficient alternative. Moreover, our system enhances security and decentralization by utilizing a public blockchain, ensuring that data is stored and managed across a distributed network of nodes rather than a single centralized authority. This approach not only improves the performance and scalability of the system but also enhances data security and integrity.

4. EXPERIMENTAL METHODS



A. SETUP PHASE

In this setup phase, MetaMask is utilised for authentication, ensuring that user credentials like email and password are not required. Because, MetaMask will authenticate the user by their public and private keys. Participants such as hospitals, doctors, and research entities are registered by the admin, providing their identity proof for verification and integrity purposes. This process helps establish a secure and trusted network of users within the system. Once registered, doctors can proceed to register patients, and patients can designate an emergency contact. In the event of an emergency, the assigned contact person can provide consent to doctors, allowing them to access the patient's health records. This setup ensures secure and efficient management of health records while maintaining user privacy and data integrity.

B. STORAGE AND RETRIEVAL PHASE

In the Med-Block system, doctors are required to obtain consent from patients before storing their health records on IPFS. When a doctor wants to store a patient's health records, they must first send a request to the patient. The patient then verifies the identity of the doctor and their hospital to ensure

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

integrity. This verification process helps establish trust between the patient and the doctor. After verification, the patient can either deny or accept the request from the doctor. This entire process is managed through the use of smart contracts, which ensure that the consent is recorded immutably on the blockchain, providing a secure and transparent way to manage patient data.

In the retrieval phase, the doctor also has to get consent from the patient to access their health records. This requesting process and granting process are the same as the storage phase. After the doctor gets consent from the patient by sending a request, he can access the patient records stored in the IPFS by identifying the CID stored in the blockchain. Once the doctor retrieves the CID from the blockchain, it is in encrypted format. He has to decrypt it with AES to get the original CID. Then, the doctor can use this CID to retrieve the health record from the IPFS. This record is also stored in an encrypted format. Once he retrieves the record from IPFS, he has to decrypt it with AES and RSA for viewing the original record of the patient..

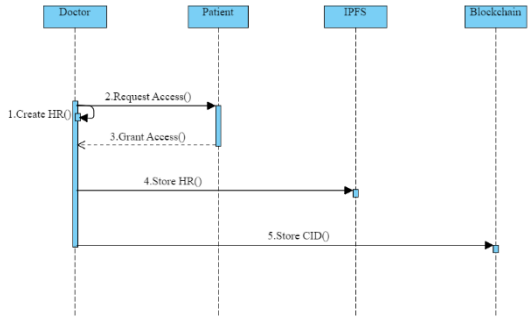


Figure B.1: STORAGE PHASE

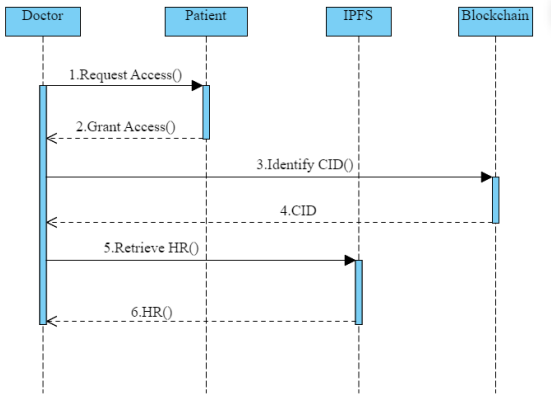


Figure B.2: RETRIEVAL PHASE

C. EMERGENCY ACCESS PHASE

In the emergency access phase, patients have the ability to add multiple emergency contacts who can provide consent on their behalf in case of an emergency. This feature is crucial as it ensures that doctors can access the patient's health records promptly, even when the patient is unable to give consent directly. This streamlined access to information can significantly improve the effectiveness of treatment during emergency situations, as it eliminates the need to gather information from other providers such as health insurance or physicians, saving valuable time. Patients retain control over their health information, as they can revoke emergency access granted to their designated contacts once they have fully recovered. This approach ensures that patient privacy is maintained while enabling timely and informed medical interventions during critical situations.

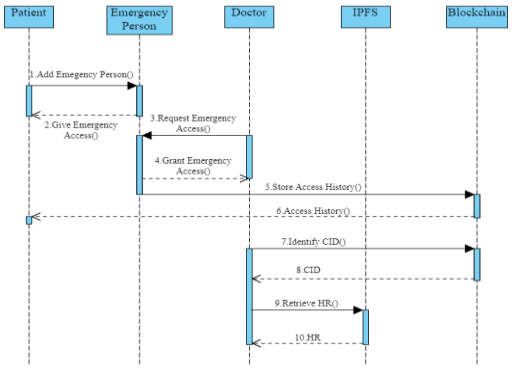


Figure C.1: EMERGENCY PHASE

D. ANONYMITY

In Med-Block, In case of anonymity, research entities can request anonymized health records of patients for studies and research purposes. However, they do not have direct access to the patient health records stored in IPFS. Instead, they must obtain consent from the doctor who registered the patient. Before granting access, the doctor must also obtain consent from the patient. Research entities request anonymized patient records from the doctor, who can then provide consent for access. Once consent is given, the research entity can retrieve the records by accessing the CID from the blockchain and using it to retrieve the records from IPFS. This ensures that research entities do not know the identity of the patient, and vice versa, ensuring the anonymity of the health records.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

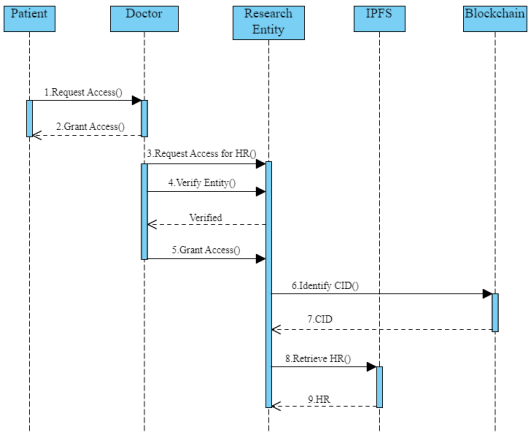


Figure D.1: ANONYMITY PHASE

E. ACCESS REVOKATION AND INTEROPERABILITY

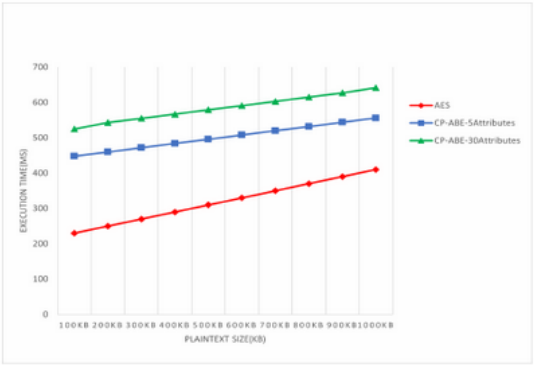
In Med-Block, to achieve Anonymity, patients have the ability to revoke access to their health records granted to doctors or emergency contacts at any time. This can be done using smart contracts in the blockchain, which ensures that the revocation is recorded and enforced. If a doctor needs to access the patient's records after access has been revoked, they would need to contact the patient to reconsent to the request. The same applies to emergency contacts, who can also have their emergency consent revoked by the patient. Additionally, patients can revoke emergency access granted to emergency contacts if they feel that the person is misusing their authority. Similarly, doctors can revoke access granted to research entities if they believe that the entity is inactive or misusing the health records. This ensures that patients have full control over who can access their health information and helps prevent unauthorized access and misuse of data.

Interoperability is a key aspect of Med-Block, as it enables seamless communication and data exchange between different components of the healthcare system. Med-Block is designed to be interoperable with existing healthcare infrastructure, allowing it to integrate smoothly with electronic health record (EHR) systems, hospital information systems (HIS), and other healthcare data sources. This interoperability ensures that patient health records can be accessed and shared securely across different platforms and systems, improving the efficiency and quality of healthcare delivery. By adhering to interoperability standards and protocols, our system can enhance collaboration among healthcare providers, researchers, and patients, leading to better healthcare outcomes and patient experiences.

5. RESULTS AND EVALUATION

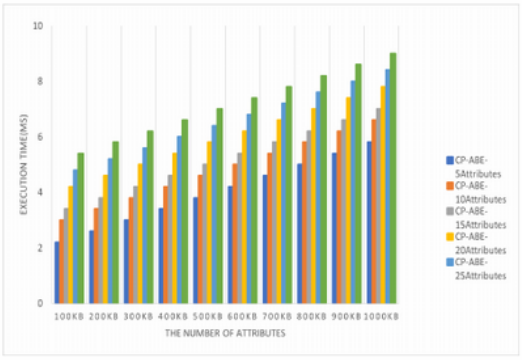
Proposed system represents a significant improvement over existing ones using CP-ABE cryptography algorithm. While the existing systems using CP-ABE cryptography algorithm provide a level of security for health records, they can be complex and resource-intensive to implement and maintain. CP-ABE requires significant computational resources for key management and access control, which can lead to performance bottlenecks and increased costs. Additionally, CP-ABE may introduce scalability challenges as the number of users and access policies grows, potentially limiting the system's ability to handle a large volume of health records efficiently. By utilizing AES-256 with RSA cryptography, Proposed system enhances security and efficiency in managing health records. AES-256 is a symmetric key encryption standard that provides robust protection against brute-force attacks, ensuring that health records remain confidential. Additionally, RSA cryptography offers secure key exchange and digital signatures, further bolstering the system's security. The integration of blockchain and IPFS enhances data integrity and availability, ensuring that health records are immutable and accessible when needed. Overall, Proposed system provides a more secure and efficient solution for managing health records compared to existing systems.

5.1 Execution Time Comparison Between Existing System and Proposed System By Cryptographic Security

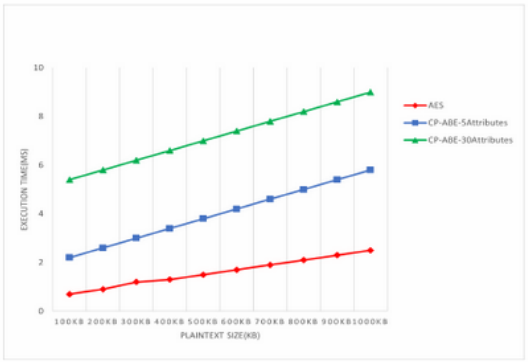


(b) Comparison of Encryption Time for CP-ABE Vs. AES

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

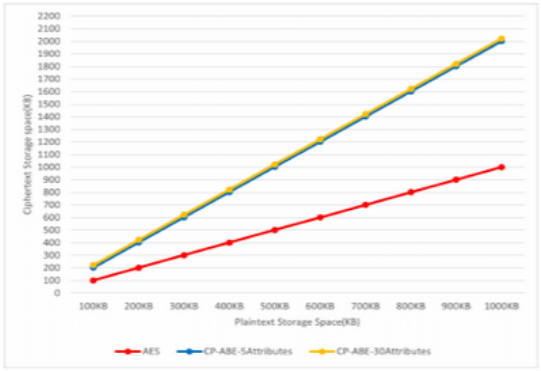


(a) Comparison of execution Time for CP-ABE Vs. AES



(b) Execution Time of CP-ABE and AES with growing data size

5.2 Memory Usage Comparison Between Existing System and Proposed System by Cryptographic Security



(c) Comparison of ciphertext size for CP-ABE vs. AES

5.3 Summary of the solutions and their fulfilled properties, wherein PR1 is confidentiality, PR2 is access control, PR3 is integrity, PR4 is emergency access, PR5 is access revocation, PR6 is interoperability, PR7 is anonymity and PR8 is decentralization.

Proposal	PR1	PR2	PR3	PR4	PR5	PR6	PR7	PR8
Ganiga et al. [6]	✓	✓	✓	×	×	✓	×	×
Masud et al. [24]	✓	✓	✓	×	×	×	✓	✓
Liu et al. [25]	✓	✓	×	×	×	×	×	×
Kumar and Chand [26]	✓	✓	✓	×	✓	×	✓	×
Qiu et al. [27]	✓	✓	✓	×	×	×	✓	×
Varadharajan et al.[28]	✓	✓	×	×	✓	×	×	✓
Mhatre and Nimkar [5]	✓	✓	×	×	✓	✓	×	×
Abunadi and Ramasamy [29]	✓	✓	✓	×	×	✓	×	×
Patel [7]	×	✓	✓	×	×	✓	✓	×
Shen et al. [8]	✓	✓	✓	×	✓	✓	×	×
Zhuang et al. [30]	✓	✓	✓	×	×	✓	×	×
Rahuiamathavan et al. [31]	✓	✓	✓	×	×	×	✓	×
Zghaibeh et al. [32]	×	✓	✓	×	×	✓	×	×
Da Costa et al. [12]	✓	✓	✓	×	✓	×	×	×
Sec-Health[1]	✓	✓	✓	✓	✓	✓	✓	×
Med-Block	✓	✓	✓	✓	✓	✓	✓	✓

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

5.4 Execution time comparison between med-block and existing approaches using health records with sizes smaller than 1 MB

Existing approach	1-10sec
Proposed approach	0.8-9sec

6. CONCLUSION AND FUTURE ENHANCEMENT

In our work, we introduce Med-Block, a blockchain-based protocol that not only secures health records but also addresses all their main properties. These properties include confidentiality, access control, integrity, access revocation, emergency access, interoperability, anonymity, and decentralization. Unlike related proposals that rely on highly centralized mechanisms, Med-Block offers several decentralized features, ensuring that no single entity can compromise the healthcare system. While some proposals are based on a trusted or semi-trusted server, our protocol provides a more secure and decentralized approach. Additionally, compared to decentralized solutions that often focus on specific properties, Med-Block addresses the challenging problem of fulfilling all main properties of health records. This comprehensive approach sets Med-Block apart, making it a robust and secure solution for managing health records in a decentralized and secure manner.

In the Med-Block system, one slight disadvantage is its implementation using the public blockchain, Ethereum, which employs the Proof of Stake (PoS) consensus algorithm. During periods of high network traffic, this can lead to increased costs for storing record meta-data in the blockchain. To address this issue, a future plan is to migrate Med-Block to the Enterprise Ethereum Alliance (EEA) consortium blockchain. This transition will enable multiple organizations to contribute to the blockchain, thereby ensuring that the cost of storing record meta-data remains low compared to a public blockchain. By leveraging the EEA consortium blockchain, Med-Block aims to improve scalability and cost-effectiveness, making it more efficient for securely managing health records.

7. REFERENCES

[1] Leonardo da Costa, Billy Pinheiro, Weverton Cordeiro, Roberto Araujo and Antonio Abelem "Sec-Health: A Blockchain-Based Protocol for Securing Health Records," in Proc. IEEE Int. Conf. E-Health Netw., Appl. Services (HealthCom), Belem, Brazil,Feb. 2023, pp. 16605–16618

[2] C. S. Kruse, A. Stein, H. Thomas, and H. Kaur, "The use of electronic health records to support population health: A systematic review of the literature," J. Med. Syst., vol. 42, no. 11, p. 214, Nov. 2018.

[3] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "EHealth cloud security challenges: A survey," J. Healthcare Eng., vol. 2019, pp. 1–15, Sep. 2019.

[4] HIPAA Journal. December 2021 Healthcare Data Breach Report. Accessed: Sep. 2, 2022. [Online]. Available: https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/

[5] I. M. Lopes, T. Guarda, and P. Oliveira, "General data protection regulation in health clinics," J. Med. Syst., vol. 44, no. 2, p. 53, Feb. 2020.

[6] S. Mhatre and A. V. Nimkar, "Secure cloud-based federation for EHR using multi-authority ABE," Progress in Advanced Computing and Intelligent Engineering (Advances in Intelligent Systems and Computing), vol. 714. Singapore: Springer, 2019. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-13-0224-4_1

[7] R. Ganiga, R. Pai, M. Pai, and R. Sinha, "Security framework for cloud based electronic health record (EHR) system," Int. J. Electr. Comput. Eng., vol. 10, pp. 455–466, Feb. 2020.

[8] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," Health Informat. J., vol. 25, no. 4, pp. 1398–1411, Dec. 2019.

[9] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," Appl. Sci., vol. 9, no. 6, p. 1207, Mar. 2019.

[10] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Sep. 7, 2022.[Online].Available:https://bitcoin.org/bitcoin.pdf

[11] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014, arXiv:1407.3561.

[12] J.Bethencourt,A.Sahai,andB.Waters,"Ciphertext-policyattribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, Dec. 2007, pp. 321–334.

[13] L. da Costa, B. Pinheiro, R. Araujo, and A. Abelem, "A decentralized protocol for securely storing and sharing health records," in Proc. IEEE Int. Conf. E-Health Netw., Appl. Services (HealthCom), Bogotá, Colombia, Oct. 2019, pp. 1–6.

[14] W. B. Lee and C. D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008.

[15] LGPD. (2018). Lei no 13.709, de 14 de Agosto de 2018 (in Portuguese). Accessed: Sep. 7, 2022. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

[16] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in Proc. 8th ACM Symp. Inf., Comput. Commun. Secur. (ASIA CCS), K. Chen, Q. Xie, W. Qiu, N. Li, W.-G. Tzeng, Eds. Hangzhou, China, May 2013, pp. 523–528.

[17] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," Inf. Sci., vol. 479, pp. 567–592, Apr. 2019.

[18] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digitalsignaturesandpublic-keycryptosystems(reprint),"Commun.ACM, vol. 26, no. 1, pp. 96–99, 1983.

[19] FIPS.(2002).SecureHashStandard.[Online].Available:https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf

[20] M. Jakobsson and A. Juels, "Mix and match: Secure function evaluation via ciphertexts," in Advances in Cryptology—ASIACRYPT (Lecture Notes in Computer Science), vol. 1976, T. Okamoto, Ed. Kyoto, Japan: Springer, Dec. 2000, pp. 162–177.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

[21] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, Aug. 2001.

[22] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.

[23] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of Money," 2015, arXiv:1511.05740.

[24] Hyperledger. Hyperledger Fabric. Accessed: Sep. 7, 2022. [Online]. Available: https://www.hyperledger.org/use/fabric

[25] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain, "A robust and lightweight secure access scheme for cloud based Ehealthcare services," Peer-Peer Netw. Appl., vol. 14, no. 5, pp. 3043–3057, Sep. 2021.

[26] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, "Secure and fine-grained access controlonE-healthcarerecordsinmobilecloudcomputing,"FutureGener. Comput. Syst., vol. 78, pp. 1020–1026, Jan. 2018.

[27] M. Kumar and S. Chand, "A secure and efficient cloud-centric Internet-ofMedical-things-enabled smart healthcare system with public verifiability," IEEE Internet Things J., vol. 7, no. 10, pp. 10650–10659, Oct. 2020.

[28] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," IEEE J. Biomed.Health Informat., vol. 24, no. 9, pp. 2499–2505, Sep. 2020.

[29] V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare, "E-health cloud security using timing enabled proxy re-encryption," Mobile Netw. Appl., vol. 24, no. 3, pp. 1034–1045, Nov. 2022.

[30] I. Abunadi and R. Kumar, "BSF-EHR: Blockchain security framework for electronic health records of patients," Sensors, vol. 21, no. 8, p. 2865, Apr. 2021.

[31] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," IEEE J. Biomed. Health Informat., vol. 24, no. 8, pp. 2169–2176, Aug. 2020.

[32] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS),Bhubaneswar, India, Dec. 2017,pp.1–6.

[33] M. Zghaibeh, U. Farooq, N. U. Hasan, and I. Baig, "SHealth: A blockchain-based health system with smart contracts capabilities," IEEE Access, vol. 8, pp. 70030–70043, 2020.

[34] M. T. de Oliveira, A. Bakas, E. Frimpong, A. E. D. Groot, H. A. Marquering, A. Michalas, and S. D. Olabarriaga, "A breakglass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud," Ann. Telecommun., vol. 75, nos. 3–4, pp. 103–119, Apr. 2020