JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Sec-Health: A Blockchain-Based Protocol for Securing Health Records

V. Tharun Kumar Reddy[1], V. Kalyan Srinivas[2], K. Shiva Sai Krishna[3], Mr. Shankar Raj Soni[4]

[1,2,3]UG Students , [4]Assistant Professor.

[1,2,3]Department of Computer Science and Engineering (Internet of Things)

[4]Department of Information Technology

[1,2,3,4]Guru Nanak Institutions Technical Campus, Hyderabad, Telangana.

1.Abstract:

"In light of the security risks associated with electronic storage and exchange of medical records, several nations have enacted regulations mandating that healthcare information systems adhere to comprehensive security standards, encompassing emergency access, interoperability, confidentiality, access control, integrity, revocation, and anonymity. While existing solutions often prioritize specific attributes or impose security restrictions, addressing all requisite security and supplementary criteria remains a challenge. To tackle this issue, we propose Sec-Health, a blockchain-based protocol designed to safeguard health records. Through a thorough analysis of Sec-Health across various attack scenarios and its ability to mitigate existing solution limitations, we illustrate its efficacy. Furthermore, our evaluation of a Sec-Health Proof of Concept demonstrates substantial improvements, reducing access times by 26% to 90%."

2.INDEX TERMS:

- blockchain-based protocol
- health records
- security requirements
- complementary security requirements
- access control
- confidentiality
- integrity
- revocation
- anonymity
- emergency access
- interoperability

3. Introduction:

Information technologies offer numerous benefits to the healthcare sector, with electronic health records (EHRs) being a key resource frequently utilized. EHRs provide comprehensive insights into a patient's medical history and current condition. Cloud computing platforms are commonly employed for the creation and distribution of EHRs, facilitating collaboration among healthcare professionals. Many countries, including the United States, Brazil, and the European Union, have enacted legislation designating health records as sensitive information, necessitating patient consent for disclosure due to inherent security vulnerabilities. These regulations outline various requirements, termed "health record properties," such as access control, confidentiality, and data integrity. To provide context for our proposed solution, Sec-Health, we present an overview of cryptographic primitives and foundational concepts, including blockchain and the Inter Planetary File System (IPFS). Cryptographic primitives such as public key encryption, hash functions, threshold cryptosystems, and Ciphertext-Policy Attribute-based Encryption (CP-ABE) are fundamental to ensuring data security and access control. IPFS is introduced as a decentralized file system that enhances data resilience and retrieval efficiency by distributing data across multiple nodes. Blockchain technology, characterized by its decentralized network and transactional transparency, is described as the basis for Sec-Health. Transactions within a blockchain involve resource registration or transfer, authenticated through digital signatures associated with public-private key pairs. In summary, this paper presents an exploration of essential cryptographic principles and technological frameworks underpinning Sec-Health, a blockchain-based protocol aimed at enhancing the security and accessibility of healthcare records.

4.Literature Survey:

1.**TITLE:** Security framework for cloud based electronic health record (EHR**) system.**
AUTHOR : R. Ganiga, R. Pai, M. Pai, and R. Sinha

YEAR :2022

DESCRIPTION :

Any hospital management system must include health records. The method of recording health information has changed as a result of more recent technological advancements. The efficiency of medical staff has increased due to the ease of organizing and maintaining medical records, which were formerly managed through different paper charts. An example of a high-tech medical management technology designed for developing nations like India is the Electronic Health Records (EHR) System. The Electronic Health Record (EHR) links the Electronic Medical Records (EMR) across all participating hospitals via various networks in a national health system. EHR provides a rapid and efficient means for healthcare providers to exchange and manage patient data.

2.TITLE: A robust and lightweight secure access scheme for cloud based E-healthcare services

AUTHOR : M. Masud, K. Choudhary, and M. S. Hossain

YEAR : 2021

DESCRIPTION :

Modern healthcare services have replaced traditional healthcare services by having doctors diagnose people remotely. This shift is largely due to cloud computing, which makes patient medical records easily accessible to all parties involved—including physicians, nurses, patients, and life insurance agents. Cloud services provide a wide range of mobile access to patients' electronic health records (EHR) and are scalable and affordable. Patients' electronic health record security and privacy remain important issues despite the cloud's many advantages, such as real-time data access. Given the sensitivity and importance of the patient health information, transferring it over an unsecured wireless media presents a number of security risks, including eavesdropping and modification. This work presents a strong and lightweight secure access strategy for remote healthcare, taking into account the security requirements.

3.TITLE : 'Secure health data sharing for medical cyber-physical systems for the healthcare 4.0

AUTHOR : H. Qiu, M. Qiu, M. Liu, and G. Memmi

YEAR : 2022

DESCRIPTION :

In the era of Health 4.0, end users' data security and privacy in Medical Cyber-Physical Systems (MCPS) have been jeopardized by the recent spate of cyberattacks. Instead of considering end users' needs, traditional standard encryption algorithms for data protection are created with the system architecture in mind. Data safety and privacy will be jeopardized once the key is exposed since encryption techniques are shifting the security of the data to the protection of the keys. In order to safeguard data safety and privacy even in the event that both the transmission medium (such as cloud servers) and the keys are stolen, we present in this work a secure data storage and sharing technique that combines a selective encryption algorithm with fragmentation and dispersion. The foundation of this approach is user-centric design.

4.TITLE: 'E-health cloud security using timing enabled proxy re-encryption

AUTHOR : V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare,

YEAR : 2022

DESCRIPTION :

The healthcare industry is drawn to the advances in cloud applications. The study of electronic health records, or EHRs, is becoming more and more significant in the scientific journals. The need for security and privacy must be carefully considered because EHRs include sensitive data.

Digital technologies are being used more often thanks to services like outsourcing and increasing processing. Three key areas of study are reliability, scalability, and security: digital data interconnects with various network devices. In databases that are outsourced, security plays a crucial role. Previous works that have been introduced by research communities include searchable encryption and proxy re-encryption. The healthcare application still hasn't met all of its security standards. However, before searching encryption deteriorates in terms of computational capability for storing. Our proposal for timing is presented in this publication.

5.proposed System:

The objective of Sec-Health is to address the malicious behaviors stated above by identifying, stopping, and/or mitigating them. We suggest Sec-Health, a block chain-based health record security protocol that satisfies all of the primary security requirements as well as supplementary ones specified by existing laws. We demonstrate Sec-Health's suitability by examining it in a number of attack scenarios and outlining how it addresses issues with other solutions.

6. SOFTWARE REQUIREMENTS:

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the team's and tracking the team's progress throughout the development activity.

Front End: J2EE (JSP, SERVLETS)

Back End: MY SQL 5.5

Operating System : Windows 07

IDE: Eclipse

7.HARDWARE REQUIREMENTS:

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design.

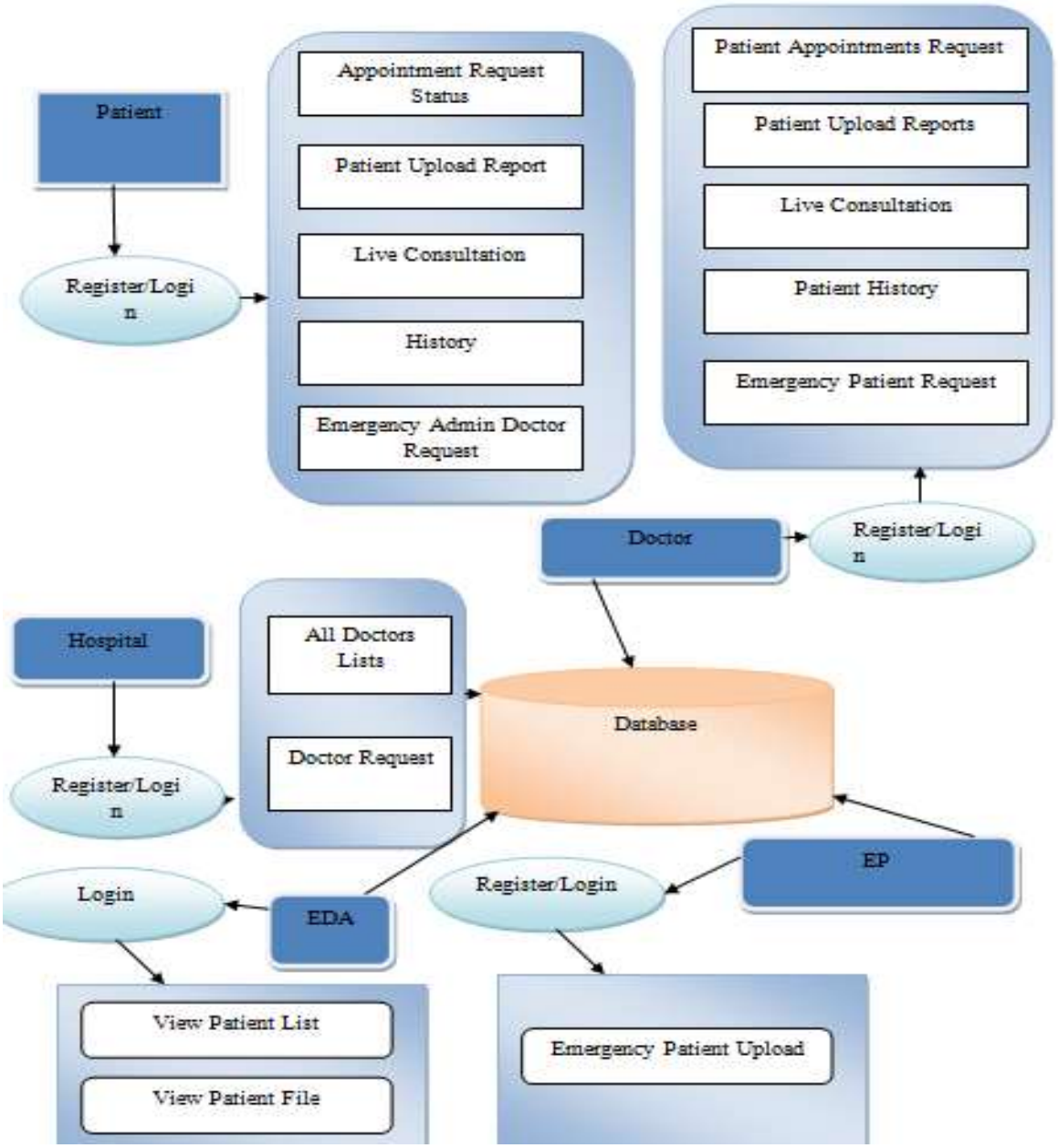
PROCESSOR: PENTIUM IV 2.6 GHz, Intel Core 2 Duo.

RAM: 4GB DD RAM

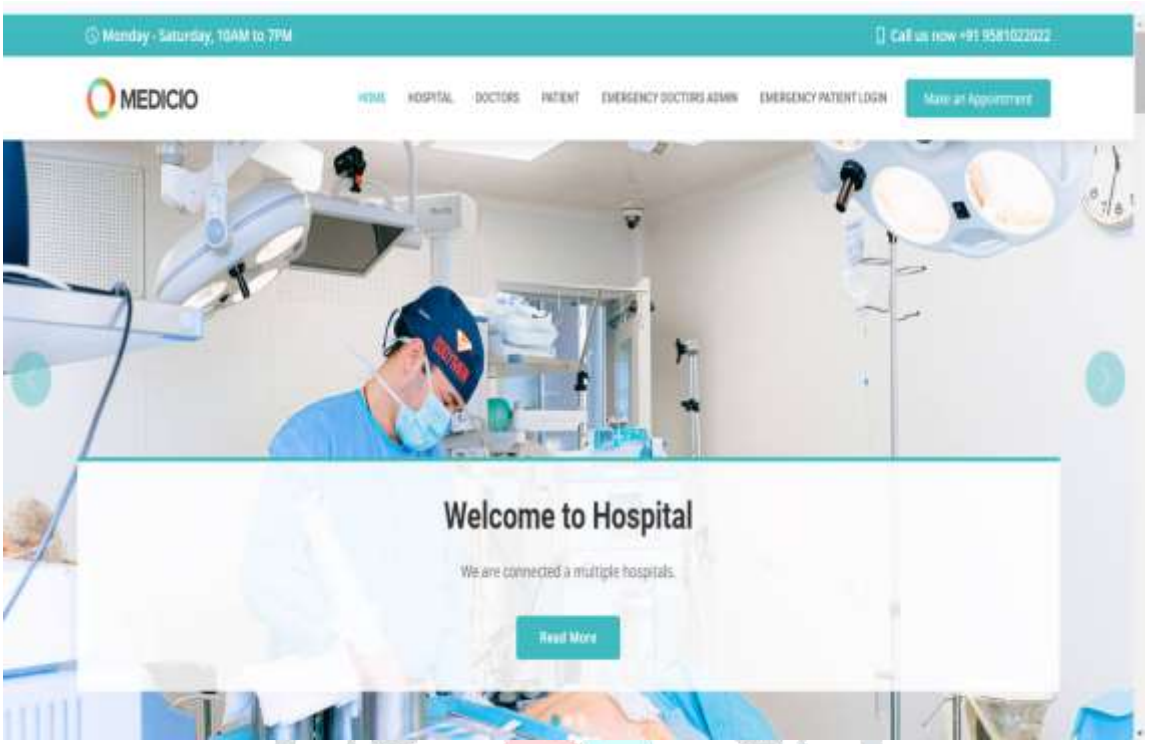
MONITOR: 15" COLOR

HARD DISK: 250 GB

8. SYSTEM ARCHITECTURE:



9. SNAP SHOTS:


Monday - Saturday, 10AM to 7PM
Call us now +91 9581022022
MEDICIO
HOME
HOSPITAL
DOCTORS
PATIENT
EMERGENCY DOCTORS ADMIN
EMERGENCY PATIENT LOGIN
Make an Appointment
Welcome to Hospital
We are connected a multiple hospitals.
Read More


Hospital Login

10.CONCLUSION:

In this work, we proposed Sec-Health, a blockchain-based protocol that secures health records while addressing all of their main properties, namely confidentiality, access control, integrity, access revocation, emergency access, interoperability, and anonymity. Sec-Health shows security advantages compared to related proposals that present highly centralized mechanisms. While those proposals are generally based on a trusted or semi trusted server, Sec-Health affords several decentralized features, preventing one single entity from compromising the healthcare system. Furthermore, compared to decentralized solutions, our protocol addresses the challenging problem of fulfilling all the main properties of health records, whereas other solutions focus on offering mechanisms for specific properties only. Experimental evaluations of a Sec-Health PoC demonstrated the practical feasibility of our protocol.

11.FUTURE ENHANCENENT:

As future work, we plan to implement the other Sec-Health mechanisms (e.g., those related to emergency access, anonymity) and evaluate them in different scenarios. Furthermore, we intend to test Sec-Health with block chain platforms of using each of them and select the best one to implement our protocol. We will also investigate types of modification we can apply to Sec-Health such that it can execute more efficiently along with the selected block chain platform. Another future work is to design a collaborative scheme to from the block chain. Finally, we plan to investigate a new version of Sec-Health in the context of quantum networks/internet..

12. REFERENCES:

[1] 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.

[2] Y. Al-Issa, M. A. Ottom, and
A.Tamrawi, ‘‘E-Health cloud security challenges: A survey,’’ J. Healthcare Eng., vol. 2019, pp. 1–15, Sep. 2019.

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

[4] 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.

[5] 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

[6] R. Ganiga, R. Pai, M. Pai, and R. Sinha, ‘‘Security framework for cloud based electronic health record (EHR) system,’’ Int. J. Electric. Compute. Eng., vol. 10, pp. 455–466, Feb. 2020.

[7]V. Patel, ‘‘A framework for secure and decentralized sharing of medicalimaging data via blockchain consensus,’’ *Health Information. J.*, vol. 25, no. 4,pp. 1398–1411, Dec. 2019.
[8] B. Shen, J. Guo, and Y. Yang, ‘‘Med-Chain: Efficient healthcare datasharing via blockchain,’’ *Appl. Sci.*, vol. 9, no. 6, p. 1207, Mar. 2019.
[9] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.Accessed: Sep. 7, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[10] J. Benet, ‘‘IPFS—Content addressed, versioned, P2P file system,’’ 2014,*arXiv:1407.3561*.
[11] J. Bethencourt, A. Sahai, and B.Waters, ‘‘Ciphertext-policy attribute-basedencryption,’’ in *Proc. IEEE Symp. Secure. Privacy*, Oakland, CA, USA,Dec. 2007, pp. 321–334.
[12] L. da Costa, B. Pinheiro, R. Araujo, and A. Abelem, ‘‘A decentralizedprotocol for securely storing and sharing health records,’’ in *Proc. IEEE Int. Conf. E-Health Network., Appl. Services (Health-Com),* Bogotá, Colombia,Oct. 2019, pp. 1–6.
[13] 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.
[14] 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
[15] K. Yang, X. Jia, and K. Ren, ‘‘Attribute-based fine-grained access controlwith efficient revocation in cloud storage systems,’’ in *Proc. 8th ACM Symp. Inf., Compute. Commune. Secure. (ASIA CCS)*, K. Chen, Q. Xie,W. Qiu,N. Li, W.-G. Tzeng, Eds. Hangzhou, China, May 2013, pp. 523–528.
[16] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, ‘‘Privacy-preservingsmart IoT-based healthcare big data storage and self-adaptive accesscontrol system,’’ *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019.
[17] R. L. Rivest, A. Shamir, and L. M. Adleman, ‘‘A method for obtainingdigital signatures and public-key cryptosystems (reprint),’’ *Commune. ACM*,vol. 26, no. 1, pp. 96–99, 1983.
[18] FIPS. (2002). *Secure Hash Standard*. [Online]. Available:https://csrc.nist.gov/csrc/media/publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf
[19] M. Jakobsson and A. Juels, ‘‘Mix and match: Secure function evaluationvia ciphertexts,’’ in *Advances in Cryptology—ASIACRYPT* (Lecture Notesin Computer Science), vol. 1976, T. Okamoto, Ed. Kyoto, Japan: Springer,Dec. 2000, pp. 162–177.
[20] D. Johnson, A. Menezes, and S. Vanstone, ‘‘The elliptic curve digitalsignature algorithm (ECDSA),’’ *Int. J. Inf. Secure.*, vol. 1, no. 1, pp. 36–63,Aug. 2001.
[21] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng,‘‘Survey on blockchain for Internet of Things,’’ *Compute. Commune.*,vol. 136, pp. 10–29, Feb. 2019.
[22] G. W. Peters and E. Panayi, ‘‘Understanding modern banking ledgersthrough blockchain technologies: Future of transaction processing andsmart contracts on the Internet of Money,’’ 2015, *arXiv:1511.05740*.
[23] Hyperledger. *Hyperledger Fabric*. Accessed: Sep. 7, 2022. [Online].Available: https://www.hyperledger.org/use/fabric

[24] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea, and M. S. Hossain,‘‘A robust and lightweight secure access scheme for cloud based E-healthcare services,’’ *Peer-Peer Network. Appl.*, vol. 14, no. 5, pp. 3043–3057, Sep. 2021.
[25] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, ‘‘Secure and fine-grained accesscontrol on E-healthcare records in mobile cloud computing,’’ *Future Gener.Compute. Syst.*, vol. 78, pp. 1020–1026, Jan. 2018.
[26] M. Kumar and S. Chand, ‘‘A secure and efficient cloud-centric Internet-of-Medical-things-enabled smart healthcare system with public verifiability,’’*IEEE Internet Things J.*, vol. 7, no. 10, pp. 10650–10659, Oct. 2020.
[27] H. Qiu, M. Qiu, M. Liu, and G. Memmi, ‘‘Secure health data sharing formedical cyber-physical systems for the healthcare 4.0,’’ *IEEE J. Biomed.Health Information.*, vol. 24, no. 9, pp. 2499–2505, Sep. 2020.