

**SEC-HEALTH A BLOCKCHAIN BASED PROTOCOL FOR SECURING HEALTH RECORDS****1 MANDAPATI. MANI SAI DURGASRI**<sup>2</sup> Mr. Naga Srinivasa Rao<sup>1</sup>PG STUDENT ,DEPT OF MCA<sup>2</sup> Asst. Prof, Dept of MCA**SREE KONASEEMA BHANOJI RAMARS P.G. COLLEGE (AMALAPURAM)**1. Abstract:

Storing and sharing health records through electronic systems pose security risks. To address them, several countries' regulations have established that healthcare information systems must fulfill security properties (confidentiality, access control, integrity, revocation and anonymity) and complementary ones (emergency access and interoperability). Upon tackling these issues, several proposals present security limitations and/or address specific properties only. We propose Sec-Health, a blockchain-based protocol that secures health records, addressing all of the main security and complementary properties defined in current regulations. We show that Sec-Health is a suitable solution by analyzing it under several attack scenarios and describing how it overcomes the problems of existing solutions. Furthermore, we evaluate a Sec-Health Proof of Concept, showing that it can reduce from 26% up to 90% the time to access health records, and reduce up to 50% client-side memory overhead, compared to related work

**keywords:blockchain-based protocol,health records, security requirements complementary security requirements**2. 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.

3. 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 :**

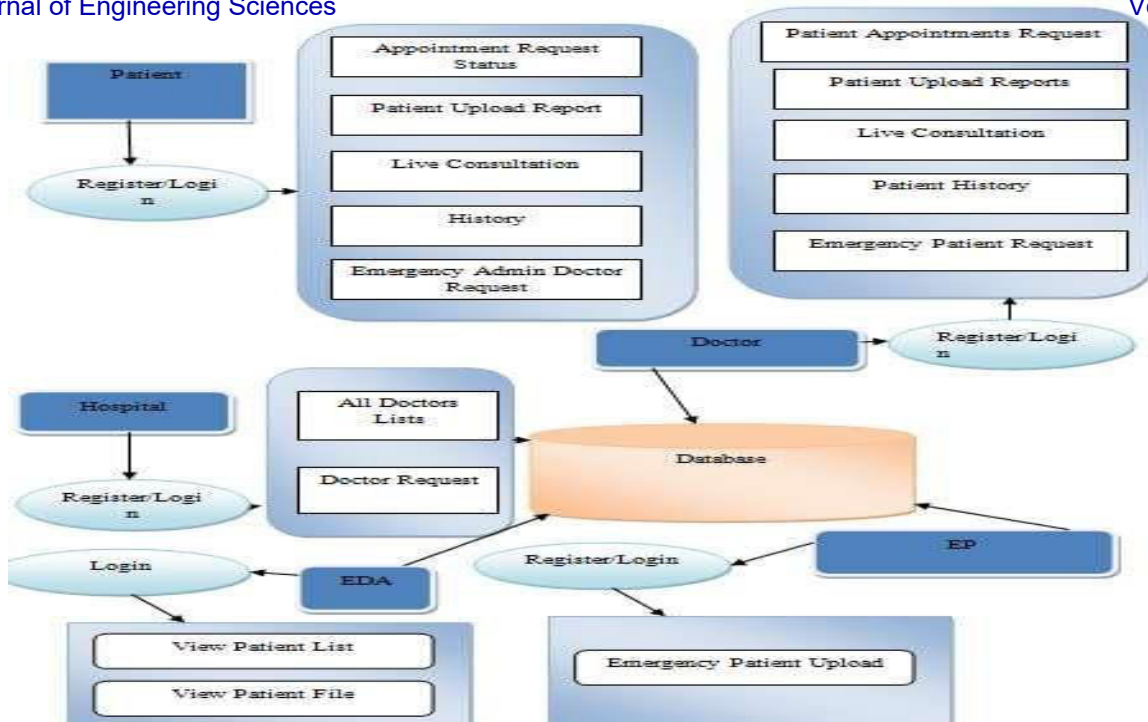
The healthcare industry is drawn to the advances in cloud applications. The study of electronic health records, or EHRs, is becoming more and more significant in the scientific journals. The need for security and privacy must be carefully considered because EHRs include sensitive data.

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. SYSTEM ARCHITECTURE:



HOME PAGE

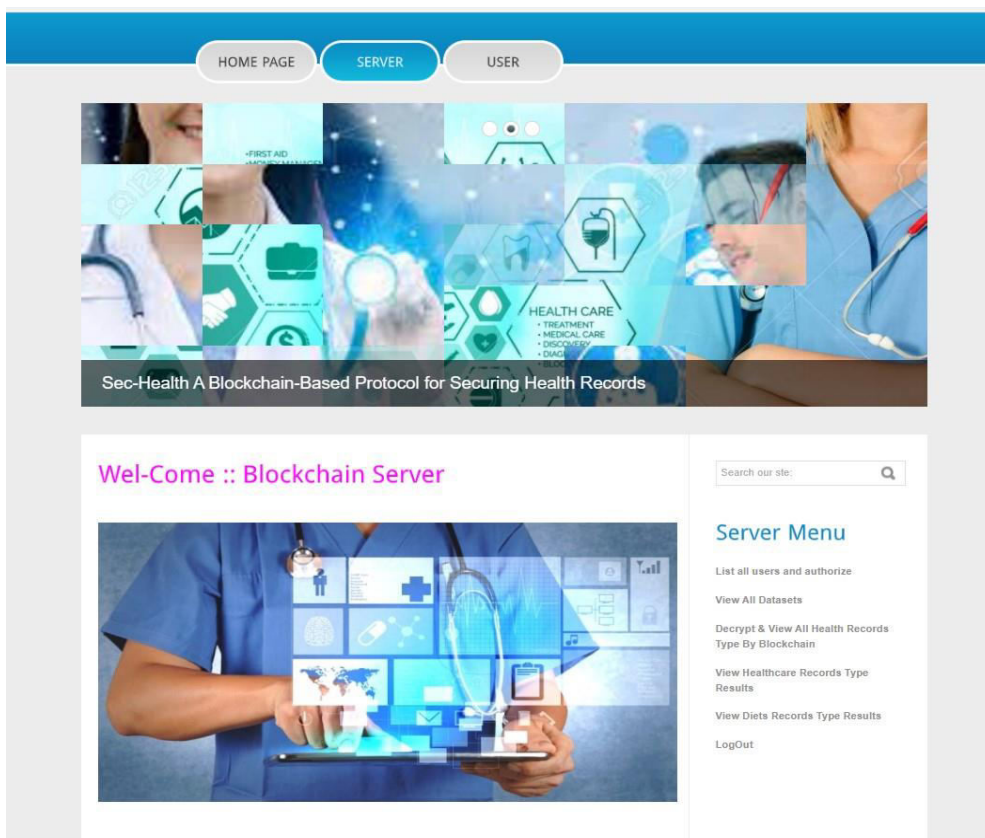


Fig. Home Page

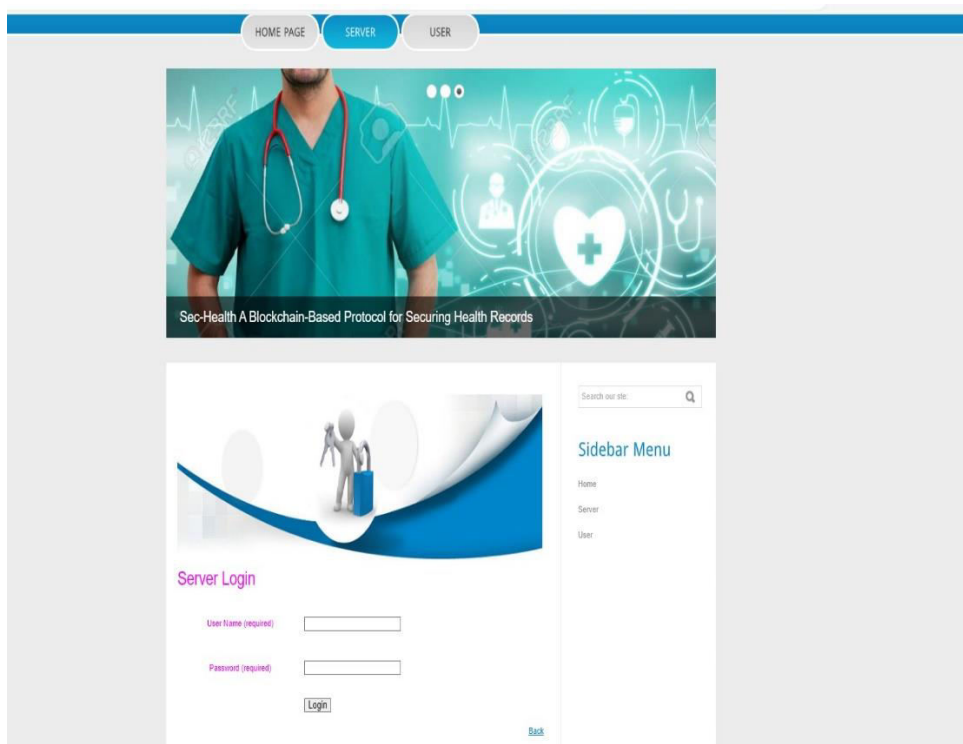


Fig . Server Page Login

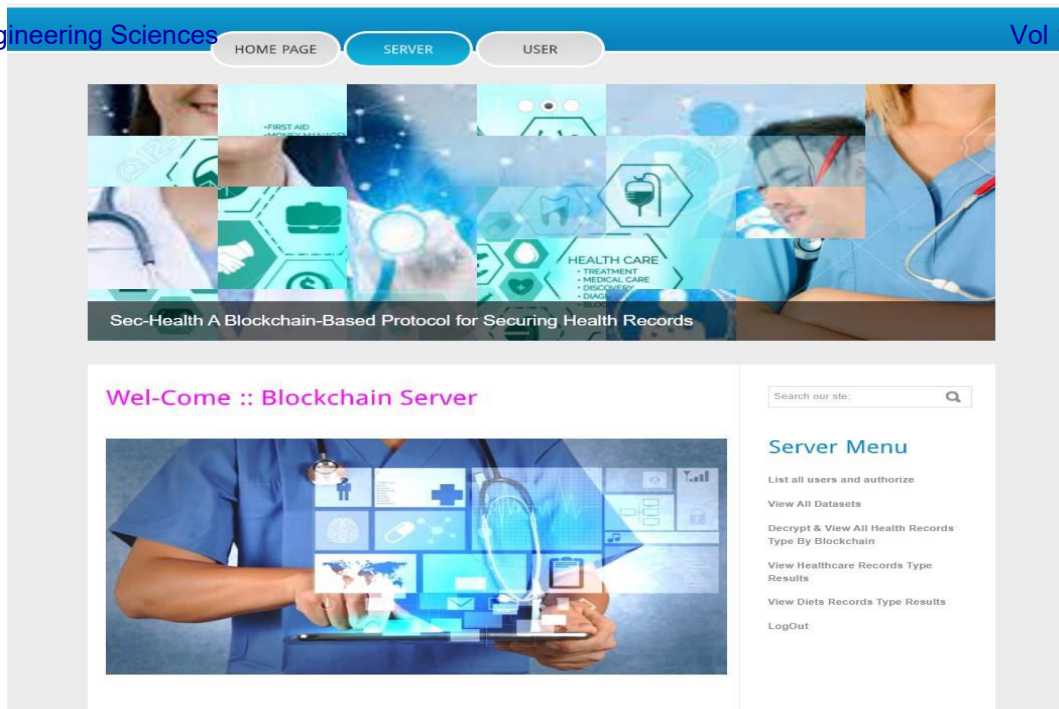


Fig . Server Page

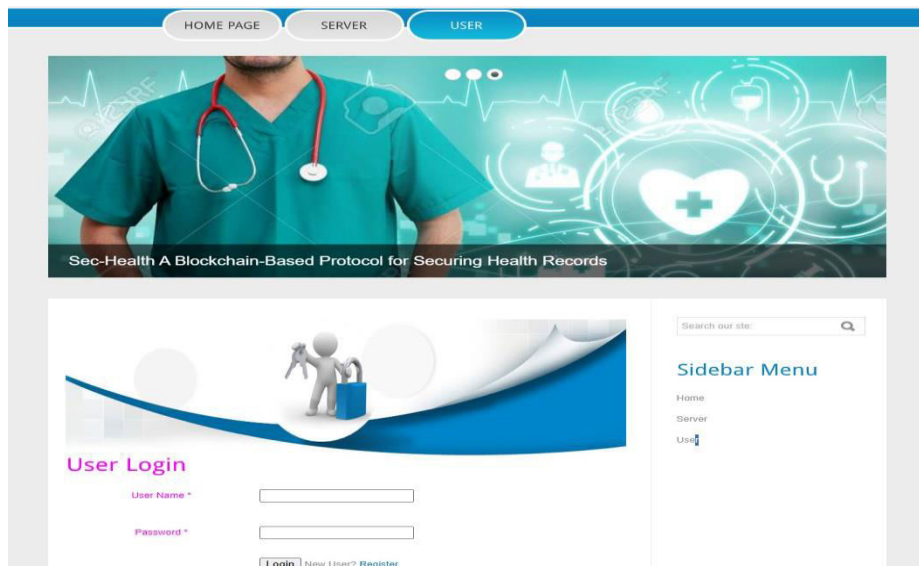


Fig . User Page Login





Fig. User Page

## 8. 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.

## 9. FUTURE ENHANCEMENT:

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 form the block chain. Finally, we plan to investigate a new version of Sec-Health in the context of quantum networks/internet..

## 10. 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](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.