International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Data Security and Privacy with User Revocation in E Health

**A Raihana[1], Nivithra V[2], Priyadharshini B[3], Rithika S[4]**

[1]Assistant professor, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India.
[2,3,4]Student, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India.

**ABSTRACT**
Block chain technology has the potential to completely transform healthcare management systems by enhancing data security, interoperability, and integrity because to its decentralized and unchangeable structure. Sensitive patient information is more difficult for bad actors to breach thanks to the SHA-256 algorithm, which improves data security. Interoperability between diverse healthcare systems is facilitated by smart contracts and standardized data formats. However, issues with user adoption, scalability, and regulatory compliance also face block chain implementation in the healthcare industry. This study offers important insights into the changing environment of healthcare data management by highlighting the possible advantages and challenges of integrating block chain technology in healthcare management systems.

**Keywords:** Block Chain, Health, Security, EHR

## 1. INTRODUCTION

### 1.1 BLOCKCHAIN

Distributed ledger technology (DLT) in the form of block chain makes transactions safe, transparent, and impervious to tampering. Its use in the world of cryptocurrencies, like Bitcoin, is the most well-known. Block chain,
however, has the potential to completely transform a number of other sectors, including healthcare. Electronic health records (EHRs) storage and sharing is one possible use case for blockchain technology in the healthcare industry. Electronic Health Records (EHRs) are digital representations of a patient's medical history, including diagnosis, treatments, and prescription drugs. EHRs are essential for providing high-quality treatment, but they are also susceptible to hackers. Block chain has multiple ways to improve EHR security.

### 1.2 HEALTH

A ubiquitous and invaluable aspect of human life, health encompasses not only the absence of disease but also an individual's complete physical, mental, and social well-being. It is a basic human right and a requirement that transcends social, cultural, and economic boundaries. Our understanding of health has evolved throughout time, moving from a purely biological perspective to one that adopts a more holistic approach and considers the intricate relationships that exist between social, mental, and physical components. A dynamic and ever-evolving field of study and practice, the pursuit of health, whether at

the individual or societal level, takes into account a number of complex factors, such as access to healthcare, the quality of healthcare services, preventive measures, and the wider determinants of health. The groundwork for an extensive investigation of health is laid by this introduction, which emphasizes the importance of health in our lives, its many facets, and the variety of methods available for obtaining and preserving good health.

### 1.3 SECURITY

A vital component of human existence, security is essential to the welfare of people, groups, and society as a whole. It is the guarantee of safety from a plethora of possible dangers and hazards that can interfere with our daily routines. Every aspect of our everyday lives is impacted by security, from the locks on our doors to the encryption on our digital communications. It includes maintaining social order, protecting private information, and ensuring one's physical safety. Security challenges have become more intricate in a more interconnected and dynamic world, requiring a thorough grasp of the constantly changing environment of dangers and the implementation of solutions to mitigate them. This introduction lays the groundwork for a thorough examination of the complex field of security, highlighting the importance of security in our daily lives, the dynamic nature of threats.

### 1.4 ELECTRONIC HEALTH RECORDS (EHRS)

EHRs, or electronic health records, have become a major influence in modern healthcare, changing the way that patient data is collected, maintained, and disseminated. They signify a fundamental change from conventional paper-based medical records to digital systems that improve healthcare data accessibility, accuracy, and efficiency. EHRs are intended to be all-inclusive databases that hold a person's test results, treatment plans, medical history, and more, providing medical professionals with a comprehensive picture of a patient's health journey. An overview of the vital role electronic health records (EHRs) play in healthcare is given in this introduction, which also highlights the importance of EHRs in facilitating interoperability across healthcare systems, enhancing clinical decision-making, and expediting patient treatment. A more thorough examination of EHRs will highlight the ways in which these electronic health records can improve patient outcomes, improve the provision of healthcare, and give people more control over their own health.

## 2. LITERATURE REVIEW

### 2.1 TRENDS AND OPPORTUNITIES IN BLOCKCHAIN TECHNOLOGY IN THE HEALTHCARE INDUSTRY

According to what Hassan Mansur [1] et al. have suggested in this study, the healthcare industry is greatly impacted by the notable rise in the application of block chain technology in healthcare. This report evaluated prior efforts in order to bridge the gap between block chain technologies and the healthcare industry. The distribution of datasets, venues, keywords, and citations were all analyzed bibliometric ally to determine the trend of block chain technology in healthcare. E-health and telecare medical information system case studies were also examined and assessed for security and privacy. This study covered a number of potential future issues, including standards, block chain size, universal interoperability, and scalability and storage capacity. The reasons for using block chain technology in the healthcare sector were emphasized in this work.

### 2.2 HIDING AND ENCRYPTION COMBINED FOR DATA SECURITY

In this paper, Ibtisam et al. [2] have proposed The concealment approach is one of the methods used in information security, where data is stored in another information medium and concealed so that it is not

discovered during two-way communicating. In order to protect data from hackers and detection, an algorithm for data concealment and encryption employing many methods was suggested in this research. The shape of a wave of information (one- and two-dimensional data) and its many mathematical formulas were altered using a wavelet transformer. There were two sets of data employed: the first group was used in a covert manner. The second group was taken into consideration as an encryption and embedding method. By extracting the second group's high-value features and deleting them from the mother's information wave, the data is lowered to a level that is sufficient for the modulation process. An exponential function is used to combine the two sets of data's encryption processes. Information signals that are undetected are the outcome.

**2.3 BLOCKHR: A FRAMEWORK BASED ON BLOCKCHAIN FOR THE MANAGEMENT OF HEALTH RECORDS**

Ismail Leila et al. [3] Electronic Health Records (EHRs), as this system has suggested, have gained popularity as a way for hospitals to store and handle patient data. The existing healthcare system is more accurate and economical when these records are shared. The client-server architecture used to store EHRs currently permits hospitals or cloud service providers to maintain stewardship of patient data. Furthermore, heterogeneous databases are used to disperse patient records around several hospitals. As a result, patients struggle to put together a coherent picture of their medical history so they can concentrate on the specifics of their treatment. The healthcare industry has a bright future thanks to the block chain's security characteristics and replication mechanism, which offer answers to the client-server architecture-based EHR management system's complexity, confidentiality, integrity, interoperability, and privacy problems. In this work, we provide a block chain-based framework for managing health records (BlockHR); this is a medical support system designed to help physicians diagnose and treat patients more accurately and to monitor their progress.

**2.4 A FINE GRAINED ACCESS TO MEDICAL DATA THROUGH A HIERARCHICAL MULTI BLOCKCHAIN**

According to VANGELIS MALAMAS [4] et al., there are a number of interconnected stakeholders in the health care ecosystem, each with varying and occasionally competing security and privacy concerns. It can be difficult to share medical data that is occasionally produced by remote medical devices. While there are a number of solutions in the literature that address security and privacy requirements like data privacy and fine-grained access control, as well as functional requirements like interoperability and scalability, striking a balance between them is a difficult task because there are no readily available solutions. Centralized cloud architectures, although offering scalability and interoperable access, are predicated on high trust. Conversely, decentralized block chain-based solutions usually do not support dynamic changes in the underlying trust domains, but they do offer independent trust management and data privacy. In this research, we propose a unique hierarchical multi expressive block chain architecture to fill this need. A proxy block chain allows autonomously run trust authorities to collaborate at the highest level.

**2.5 DEVELOPMENT AND USABILITY STUDY OF AN ARCHITECTURE AND MANAGEMENT PLATFORM FOR BLOCKCHAIN-BASED PERSONAL HEALTH RECORD EXCHANGE**

Lee Hsiu-An et.al. [5] Traditionally, conventional clinics in this system have provided medical services with an emphasis on treating diseases. But as the world's population ages, there is a growing disconnect between the services that clinics provide and what their patients actually require. This implies that clinics could not have the necessary resources to provide patients with the full spectrum of care, which could lead

to avoidable medical harm. In its 2016 Multimorbidity Clinical Assessment and Management Guidelines Report, the National Institute for Health and Care Excellence stressed the value of incorporating patient-centered decision-making techniques for a range of issues, with a particular emphasis on precision medicine. Precision medicine is a disease prevention and treatment approach that takes into account each person's unique genetic, environmental, and lifestyle variations. This information is utilized to identify the dynamic adjustments and individualized care plans required for both clinical and preventative healthcare. Precision medicine's primary components include historical disease data, daily vital sign data, personal health management, and the exchange of medical records.

## 3. EXISTING SYSTEM

Because fog computing can reduce latency and data transfer requirements for instance, by relocating some computational tasks from cloud servers to closer proximity to users it is becoming more and more popular. One might utilize cipher text-policy attribute-based encryption (CP-ABE) to secure data and user privacy in fog-enabled application situations by achieving fine-grained access control. However, the practical implementation of such schemes is restricted by the absence of an efficient mechanism for access right revocation in typical CP-ABE schemes. Therefore, we present an effective CP-ABE approach with attribute revocation capability, called AC-FEH, that is intended to build a fine-grained access control system in fog enabled E-health. Our AC-FEH technology minimizes computational expenses for data owners and consumers by using fog nodes to handle data encryption and decryption. Our AC-FEH method lowers the computing expenses related to encryption and decryption when compared to a number of other competitive access control schemes based on CP-ABE. Additionally, we demonstrate the underlying CP-ABE scheme's selective security under the intractability assumption of the q-parallel BDHE problem.

## 4. PROPOSED SYSTEM

The suggested solution seeks to create a safe, effective, and transparent data ecosystem by utilizing block chain technology to transform the healthcare sector. Our suggested consensus methods will produce an unchangeable ledger with strong data security and integrity for patient medical records. Furthermore, the system will make it easier for medications to be tracked from producers to consumers, improving medication safety and lowering counterfeiting. It will also make it possible to store and exchange clinical trial data, which will promote cooperation and quicken medical research. The suggested solution aims to capitalize on the significant advantages of block chain technology in healthcare, while recognizing the obstacles related to acceptance, regulation, and technology.

This solution establishes a direct association between each patient and their designated doctor within a healthcare system.

The patient-doctor linking enhances security by implementing encryption measures. Upon patient registration, a unique encryption key is generated and securely shared with the designated doctor. Patient details are encrypted using this key, ensuring that only the assigned doctor with the correct encryption key can access and decrypt the information. This system automatically revokes the link between a doctor and patient if the patient's disease is marked as cured. When the doctor attempts to access patient details post-revocation, the system triggers a violation message, notifying the doctor that access is unauthorized. The access control mechanism ensures compliance with privacy regulations, restricting information retrieval once the disease is cured. A notification system alerts doctors of changes in patient status. In the end, this will enhance patient care, data management, and industry efficiency.

### 4.1 PATIENT BLOCKCHAIN RECORD

Patients ought to have command over who can get to their wellbeing data. They ought to have the option to concede or disavow admittance to their information, and have the option to follow who has gotten to it. Block chain's permanence highlight guarantees that once a patient's wellbeing data has been recorded on the block chain, it can't be messed with or erased. This is fundamental for keeping up with the honesty of patient wellbeing data. To guarantee that medical services suppliers can undoubtedly get to patient data across various frameworks and organizations, the Patient block chain record module ought to Be interoperable with other medical care frameworks.

### 4.2 DOCTOR BLOCKCHAIN RECORD

Likewise, with the patient block chain record module, block chain’s changelessness highlight guarantees that once a specialist's data has been recorded on the block chain, it can't be altered or erased. This is fundamental for keeping up with the honesty of specialist explicit data. The specialist block chain record module could give a way to medical care associations to check a specialist's subtleties. The module ought to be intended to guarantee the protection and security of specialist explicit data, while likewise permitting approved gatherings to get to it on a case by case basis. The specialist block chain record module ought to be interoperable with other medical care frameworks and organizations to guarantee consistent access and sharing of data.

### 4.3 KEY GENERATION

Key age alludes to the most common way of making a couple of cryptographic keys for use in encryption and decoding. In broad daylight key cryptography, which is regularly utilized in block chain innovation, the key pair comprises of a public key and a confidential key. The confidential key is created by choosing an irregular number that meets specific measures characterized by the cryptographic calculation. The confidential key is kept mystery and ought to never be shared.

### 4.4 DATA STORAGE:

Ensuring patient information in a fog/cloud environment requires putting in place a thorough plan to guarantee the privacy, availability, and integrity of sensitive medical data. To safeguard patient data as it travels from edge devices to fog nodes and cloud storage, this system uses end-to-end encryption. This solution use robust encryption techniques with sufficient key lengths, such as SHA 256 Encryption. Make that patient data stored in the fog/cloud infrastructure is properly protected by implementing encryption for data at rest. To transfer patient data between edge devices, fog nodes, and cloud storage, secure communication protocols like HTTPS or other secured communication channels are used.

## 4.5 BLOCK DIAGRAM

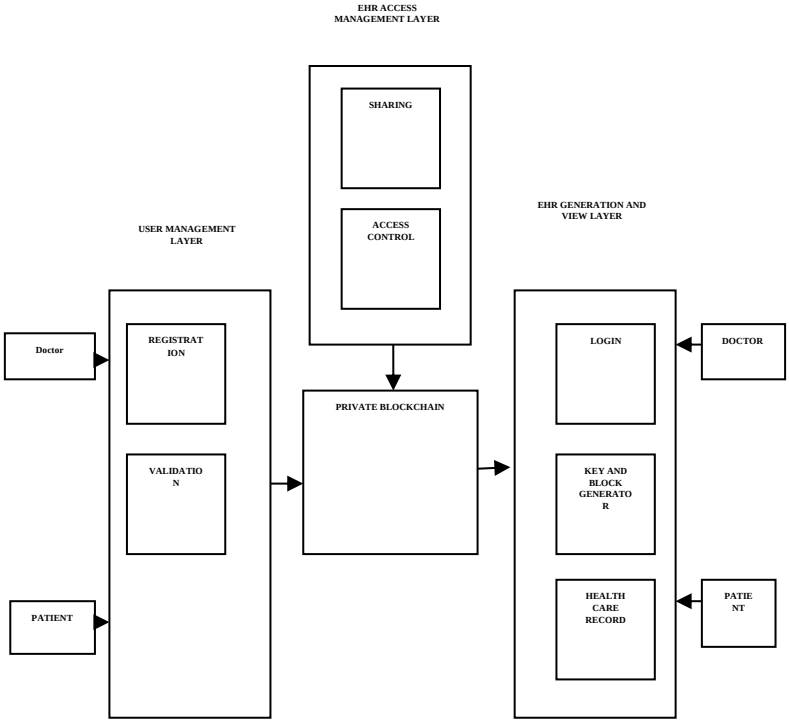


**Figure 1 block diagram**

## 4.6 SHA 256 ENCRYPTION AND HASH GENERATION

SHA-256 (Secure Hash Algorithm 256-bit) is a widely used cryptographic hash function that generates a 256-bit (32-byte) hash value. It is commonly used in block chain technology and other cryptographic applications to provide a secure way to verify data integrity. The message is padded with additional bits to ensure that the message has a fixed length that can be processed by the SHA-256 algorithm. The first step is to input the message that needs to be hashed, which can be any data, such as text, numbers, or binary data. The hash value can be used to verify the integrity of the original message, as any change to the message will result in a different hash value.SHA-256 is a one-way function, meaning that it is computationally infeasible to determine the original message from the hash value. This makes it a secure way to protect sensitive information.

## 5. RESULT ANALYSIS

| algorithm | accuracy |
|---|---|
| CP-ABE | 75 |
| SHA-256 | 88 |

**Table 1.Comparison Table**

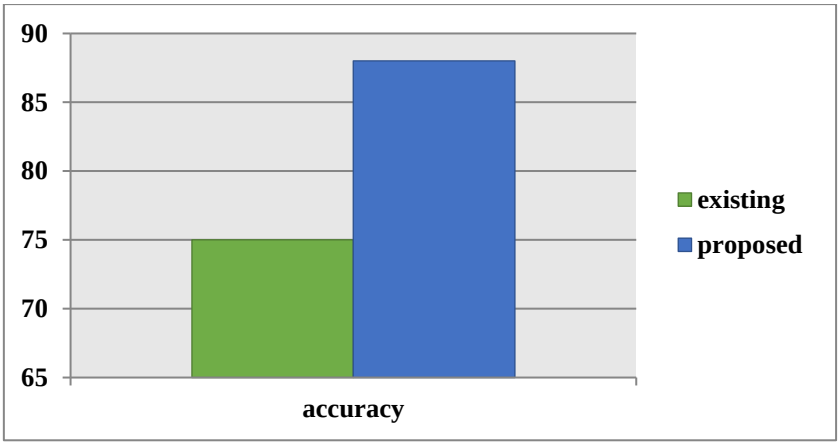


**Figure 2. Comparison graph**

The data security and integrity environment is significantly shaped by algorithms in the domains of block chain technology and healthcare management systems. With a noteworthy accuracy rate of 75%, CP-ABE (Attribute-Based Encryption) is one well-known algorithm making waves in this arena. Because it can impose access control policies based on individual attributes, CP-ABE stands out for offering an especially fine-grained level of control over who can access sensitive healthcare data. Conversely, the SHA-256 algorithm is notable for its remarkable 88% accuracy rate, highlighting its importance in improving data security in block chain systems. The cryptographic hash function SHA-256 protects sensitive patient data by producing a fixed-size hash result that is impossible to reverse computationally. The decentralized, immutable structure of block chain systems is strengthened by the combined influence of SHA-256 and CP-ABE, which supports data security and integrity in healthcare administration. In order to fully utilize block chain technology in healthcare data management, stakeholders must have a thorough understanding of the subtleties and efficacy of these algorithms.

## 6. CONCLUSION

To sum up, block chain consensus algorithms are an innovative and game-changing tool for the healthcare industry. These algorithms enable more secure and transparent collaboration between healthcare practitioners, patients, and researchers by guaranteeing data security, integrity, and interoperability. The implementation of block chain technology in the healthcare industry has the potential to improve patient outcomes, decrease administrative inefficiencies, and stimulate ground-breaking research, whether via Proof of Work, Proof of Stake, or other novel consensus mechanisms. Block chain technology and its consensus algorithms will become more and more important in influencing the future of healthcare as the sector embraces digitization and data-driven decision-making. This will eventually result in better, safer, and more effective healthcare delivery systems.

## 7. FUTURE WORK

Future research on the application of block chain consensus algorithms in healthcare should concentrate on resolving issues with scalability and regulatory compliance. Implementing and improving sharding and second-layer protocol scalability solutions will be necessary to handle the increasing amount of medical data. Furthermore, it is critical that business players, legislators, and regulatory agencies work together to create a framework that guarantees adherence to data privacy regulations and encourages the broad use of

block chain technology in the healthcare sector. Furthermore, maintaining optimal efficiency and security requires ongoing research into the creation of consensus algorithms tailored to the specific requirements of clinical trials, telemedicine, and patient records.

## 8. REFERENCES

1. "Metrics for judging blockchain-based healthcare decentralised apps," P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, in Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom), Oct. 2019, pp. 1-4.
2. "Efficient key management strategy for health blockchain," H. Zhao, P. Bai, Y. Peng, and R. Xu, CAAI Trans. Intell. Technol., vol. 3, no. 2, June 2019, pp. 114-118.
3. A. K. Talukder, M. Chaitanya, D. Arnold, and K. Sakurai, "Proof of Disease: A Blockchain Consensus Protocol for Accurate Medical Decisions and Disease Reduction," in Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.
4. "An efficient authentication strategy for blockchain-based electronic health records," F. Tang, S. Ma, Y. Xiang, and C. Lin, IEEE Access, 2019, vol. 7, pp. 41678-41689.
5. "A review of safe and privacy-preserving medical data exchange," H. Jin, Y. Luo, P. Li, and J. Mathew, IEEE Access, 2020, vol. 7, pp. 61656-61669.
6. "A decentralized blockchain-based architecture for a secure cloud-enabled IoT," by M. Marwan, A. A. Temghart, F. Sifou, and F. AlShahwan J. Mobile Multimedia, Nov. 2020, vol. 2020, pages. 389–412.
7. A safe charging method for electric vehicles with smart communities in energy blockchain, Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang IEEE Internet Things Journal, June 2019, vol. 6, no. 3, pp. 4601–4613.
8. "Performance analysis of the raft consensus algorithm for private blockchains," by D. Huang, X. Ma, and S. Zhang Jan. 2020; IEEE Transactions on Systems, Man, Cybern., Syst., vol. 50, no. 1, pp. 172–181.
9. "A comprehensive review of blockchain consensus mechanisms," by Lashkari and P. Musilek IEEE Access, volume 9, 2021, pages 43620–43652.
10. "Digital health in physicians' and pharmacists' offices: A comparative study of e-prescription systems' architecture and digital security in eight countries," by Aldughayfiq and S. Sampalli. In February 2021, OMICS, J. Integrative Biol., vol. 25, no. 2, pp. 102–122.