Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

Blockchain Based Patient Data Management System

M.Gayathri[1], M. Narasimha Yadav[2]

[1,2]Department of Computer Science and Engineering
Tadipatri Engineering College, Tadipatri.

Abstract:
By giving encrypted private health information (PHRs) to medical institutions or physicians for research reasons, more people will obtain first-rate treatment within the electronic health system. However, a significant problem is that green data retrieval via encrypted PHRs is hindered, leading to decreased data utilization, because the treatment procedure requires the health practitioner's continuous online presence, which is not always feasible for all physicians (e.g., due to lack of access in certain situations). This work presents a revolutionary cozy and re-encryption device that enables proxy-based searches and allows healthcare providers to perform comfortable and eco-friendly remote PHR tracking and searches. (1) To preserve confidentiality, the affected person's medical data collected through devices is encrypted before being moved to a cloud server. PHR secrecy; (2) DMPs are only accessible by physicians or authorized research facilities; (3) medical responsibilities may be assigned by Alice, the responsible physician. Search and see a POP (physician agent) or a particular research enterprise using a cloud server that enables cloud access management for the statistics server. We demonstrate the security of our approach and define the security concept. Finally, an overall performance review confirms our strategy's effectiveness.

Keywords: Blockchain, Personal Healthcare Records (PHRs), E-Healthcare System, Health Management.

INTRODUCTION

Rapid advances in sensors, artificial intelligence, and wearable technologies have brought the electronic fitness sensor community to a level of adulthood for big-scale business use. Using it's going to provide you with an activity and higher hospital therapy. As a mobile platform, the electronic fitness sensor community, as proven within the parent, collects a sizable amount of private fitness data from sensors installed on sufferers' gadgets, in order that docs can quick diagnose and deal with sufferers. In addition, clinical researchers and analysts can behavior various analytical research to increase treatments and gain more statistics approximately diseases. However, those files are possibly to be saved with an outside cloud service provider, which raises safety concerns together with statistics leakage. This is vital to make sure that once the statistics is available, patients or doctors cannot trade it. Outsourced. In such conditions, the confidentiality and safety of this outsourced records need to be included.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

Blockchain is a allotted, virtual, public ledger. It turned into first used within the popular digital foreign money regarded nowadays as BITCOIN, but its functions such as its accuracy and disbursed peer-to-peer network and relaxed facts transfer make it viable for other programs. The nodes of a blockchain are cryptographically and sequentially linked. The blockchain affords the potential to allocate statistics in a decentralized way and this is an important idea. Unlike a unified structure wherein records are stored, the records of a unmarried organization, inclusive of a bank or government company, are shared via a blockchain. Faces.

The blockchain becomes decentralized as a result. This is how information is gathered and stored. Through the network and its members, every record block is constantly updated and observed. It is synchronized in an open organization by employing exceptional people, making unique copies of the data using a standard file-keeping system, and ensuring that no unmarried person or organization owns the records. Many nodes in the blockchain implementation typically employ steps (computations) to compute, validate, and confirm a previous block of a particular modern blockchain when a blockchain receives a new transaction or a modification to an existing transaction. A distinct new block is added to the transaction chain when all nodes agree that a transaction token and a hard and fast of events are valid. The chain will not contain the block at that moment if the maximum nodes do not follow the combination in the entrance log. With each block comprising several transactions, this mode of operation enables a blockchain device to function without centralized control over the blockchain. It uses sources, functions as a shared block ledger that records every transaction, and provides a decentralized, unchangeable information repository that can be utilized by all client entities. As a result, blockchain enables a public check-in of data that is verifiable, irrefutable, and more convenient, rapid, and affordable than some other centralized device.

RELATED WORK

The literature review is one of the most crucial phases in the software development process. Prior to growing the device, it is crucial to ascertain the time component, cost savings, and commercial enterprise stability. Once these are met, the next step is to determine which operating system and language can be used to expand the device. Once they start creating a device, programmers need a lot of outside help. When developing the system to expand the suggested device, the aforementioned issues are taken into account. Senior programmers, books, and the internet can all provide this assistance.

The assignment improvement department's primary duty is to examine and review all of the challenge improvement's requirements. The most important step in the software development process for any task is literature evaluation. Time constraints, resource needs, labor, economics, and organizational electricity must be recognized and assessed before extending the equipment and related layout. Once those requirements have been satisfied and properly examined, the next step is to identify the operating system required for the project, the software program specifications of the specific machine, and any software that must be continued. a phase that is comparable to increasing the tools and associated capabilities.

In terms of stability, we identify and address some gaps (the degree to which keyword searches yield false positives) for public key encryption. (PEKS). We establish statistical and computational expansions of the current concept. With the right balance, we present the Euro crypt 2004 scheme by Bone et al. We propose a new statistically sound method that is computationally secure. I concur. In addition, we provide a

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

seamless transition to the unnamed IBE program. In contrast to the previous project, the PEKS initiative ensures equilibrium. Ultimately, we support three extensions to the core concepts highlighted here, comprising anonymous HIBE, public-key identification-based encryption with ad hoc keyword search, and keyword-searchable encryption [1]. An application named Atom was introduced by Blaise, Blumer, and Strauss (BBS) in 1998. Proxy re-encryption involves a trustworthy proxy transforming Alice's ciphertext into Bob's ciphertext without accessing the original plaintext. We anticipate that swift and safe re-encryption will become a standard approach for managing encrypted file systems. Despite being simple to grasp, various security issues have prevented widespread adoption of BBS re-encryption. Dangers. We present a new re-encoding that builds upon existing artworks by Todis and Ivan. We showcase how proxy re-encryption can be utilized to regulate access to a secure storage system and methods that implement a strong security framework [2]. A framework called “Public Keyword Encryption with Keyword Search” (PEKS) developed by Bone, Di Crescenzo, Ostrovsky, and Persiano allows for the encrypted searching of keywords while maintaining the security of the original data. In this paper, we discuss two essential PEKS schemes, "secure channel deletion" and "key-word replacement," which Bone et al. do not address in this study. We express that employing "cozy channel deletion" results in the genuine PEKS. That plan is ineffective. We are creating an effective PEKS device to tackle this issue of secure communication. It removes the secure link. We concur that caution should be taken in considering the possibility that this instance might conflict with PEKS [3]. Cloud computing has provided a common pool of resources accessible to all for the benefit of various players and partners in the e-health sector. Concerns about security have inevitably increased unexpectedly due to the implementation of cloud computing. The limited resources of mobile devices hinder their outsourced data security. Implementing solutions requires transitioning the entire IT approach to the cloud. Usually, any modifications to the loaded record compel the mobile client to fully encrypt and reprocess the hash value. In this document, we aim to suggest a robust unpaired intermediate approach for re-encryption that eliminates the need for certificates and operates in relation to the number of modifications made over time instead of the duration of the document needing updates. In the document, swap responsibilities. The suggested plan shows improvements in the energy usage and rotation timing of the data transfer device. The suggested framework is founded on a systematic approach applied through the Z3 solver [4].

Doctors can gain significant and rapid access to private medical information. Choices and lives are recorded and preserved. Cloud computing provides immediate, on-demand access to a collection of shared resources and virtual services for various participants in the e-health sector, including patients, healthcare providers, insurers, and others. Moreover, the incorporation of cloud computing into digital fitness frameworks raises worries regarding a wide array of security challenges linked to data outsourcing. Consequently, the cryptographic evaluation of the QIN initiative is performed in a way that infringes upon their privacy. Initiative. We offer a lightweight and convenient one-way elliptic curve-based certificate-free proxy re-encryption method for safely sharing mobile private fitness data with an efficient public cloud intended for low-energy mobile devices. Patients can utilize certificate-free proxy re-encryption to encrypt records with their public keys before outsourcing to the cloud and utilizing the cloud. The semi-reliable residential proxy server re-encrypts the encrypted text as expected. Without comprehending anything about the ciphered message or the public key of the receiver. We showcase its security by

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

systematically testing it against a particular cyber-attack on a random oracle model. Our suggested method is more effective than current systems and is appropriate for low-power mobile devices [5].

EXISTING SYSTEM

Yasnoff suggested a digital framework for storing fitness records to reduce the risk of a centralized database being compromised by individuals from the same area while ensuring adequate search efficiency. Yang et al. proposed a relaxed, searchable, and secure electronic fitness system. Its basis is searchable encryption, which safeguards sensitive health information stored on cloud servers and allows the search of encrypted records of affected individuals. Bone et al. introduced the main PEKS public key framework for a digital health device environment. Subsequently, Abdullah et al. modified the PEKS concept and introduced a coherence concept. Peck and colleagues' extended PEKS

Disadvantages

- Although encryption protects data confidentiality, can be used to address privacy concerns, and stops malevolent users and cloud servers from attacking, it also causes user annoyance.
- Conventional encryption techniques, for instance, make it challenging to query these encrypted data due to their inefficiency. Techniques for information retrieval using plaintext the amount of sensitive data in the current e-healthcare system presents serious security and efficiency issues. Because of an inefficient information retrieval mechanism and inadequate fine-grained access restriction.
- Doctors must always be available under the current system.
- Should the doctor be unavailable, medical there would be no therapy.

REQUIREMENT ANALYSIS

Evaluation of the Rationale and Feasibility of the Proposed System

The key objective of this machine is to autonomously detect pancreatic tumors. Contrast-enhanced computed tomography (CT) is commonly utilized for the staging and evaluation of pancreatic cancer. Conventional manual techniques capture only basic abilities. Nevertheless, traditional convolutional neural networks are unable to fully leverage relevant contextual information, resulting in subpar recognition outcomes. This paper presents an innovative and effective framework for detecting pancreatic tumors, aimed at fully utilizing contextual information across different scales.

PROPOSED SYSTEM

We recommend a proxy re-encryption method that conceals the proxy's invisibility. Privacy encryption is easily viewed as a keyword search to resolve the domain and accessibility challenges of the digital health device. It is an effective method to ensure data privacy, but it complicates the process of searching through encrypted information. Traceable encryption allows for searching encrypted data without the need to decrypt it and addresses the issue of users being unable to manage data encryption remotely. Therefore, research capability may be extremely important in electronics. Healthcare system. The aim of the proposed device is to create a functional, searchable, and secure electronic fitness platform.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

We are creating a casual records substitute system and verification apparatus for the suggested system. A research initiative for an electronic fitness gadget where patients consistently transmit PHRs with environment sensors encrypted with PHRs to their healthcare provider for treatment inquiries. In certain cases, Dr. A intends to share a portion of those PHRs with Dr. B, but not the entirety. A generates a re-encryption key upon receiving access approval. Both his private and public keys. To safeguard privacy and the disclosure of statistics, we create a backdoor that allows for conditional re-encryption. Consequently, the sole action the cloud server can perform is convert the encrypted text into a re-encryption key within the specified context. The cloud server is responsible for storing encrypted data, enabling keyword search functions, and acting as a proxy server to re-encrypt user metrics. An error occurs when the phrase "cloud server" is present in a search query from B, affecting the ability to access data from encrypted PHRs. In the end, B can acquire the scientific data and decipher the encryption solely with his private key.

Advantages

- Data privacy.
- Conditional authorization.
- Condition-hiding.
- Proxy invisibility.
- Collusion resistance.

SELECTED METHODODLOGIES

The proposed method for hiding the proxy invisible kingdom involves keyword searches to address privacy and inefficiency issues in the electronic health system. Encryption is regarded as a simple and efficient method to ensure data privacy; however, it also enables the analysis of encrypted information. It might be quite difficult. The development of reachable encryption involves the capability to demand unencrypted data and addresses the issue of users managing it remotely through data encryption. Consequently, pursuit is essential within the digital fitness device. The proposed system aims to create a digital fitness platform that is confidential, easily searchable, and eco-friendly.

Blockchain:

Blockchain is a common, immutable ledger that simplifies the process for a business network to monitor assets and document transactions. An asset can be intangible (like intellectual property, patents, copyrights, and trademarks) or tangible (such as a house, vehicle, cash, or property). In a blockchain network, any valuable asset can be tracked and traded, reducing risks and expenses for everyone involved. Data is the groundwork of commerce. The data must be as precise and prompt as feasible. Blockchain serves as an effective tool for delivering these records, as it offers immediate, shareable, and verifiable information stored in an unchangeable ledger that is most accessible for legal community members. A blockchain network can monitor orders, bills, invoicing, production, and more. Furthermore, since individuals possess distinct viewpoints on reality, you might observe every facet of a transaction from beginning to end, which boosts your self-assurance, creates new possibilities, and enhances your effectiveness.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

Blockchains are distributed databases or ledgers that are accessible to nodes within a computer network. They are famous for their main role in cryptocurrency networks, which is to uphold a secure and decentralized ledger of transactions, but their application isn't confined to cryptocurrency alone. Blockchain can be applied in various sectors to ensure that statistics remain unchangeable, a term that refers to the inability to modify data. As altering a block is impossible, consent is ideally needed when an individual or software inputs data. This function removes the dependency on 0.33 events, usually auditors or others who might impose charges and commit errors. Following Bitcoin's launch in 2009, the emergence of various cryptocurrencies, decentralized finance (DeFi) projects, non-fungible tokens (NFTs), and smart contracts has greatly broadened the use of blockchain technology.

SYSTEM ARCHITECTURE

The importance of the specifications and the mentioned request for a high level of the device correlates with how the product's overall characteristics are presented. Throughout architectural design, numerous web pages and their associated links are detailed and established. Key software components are detailed, categorized into conceptual records systems and processing modules, with explanations of their interconnections. The provided modules are detailed using the recommended structure.

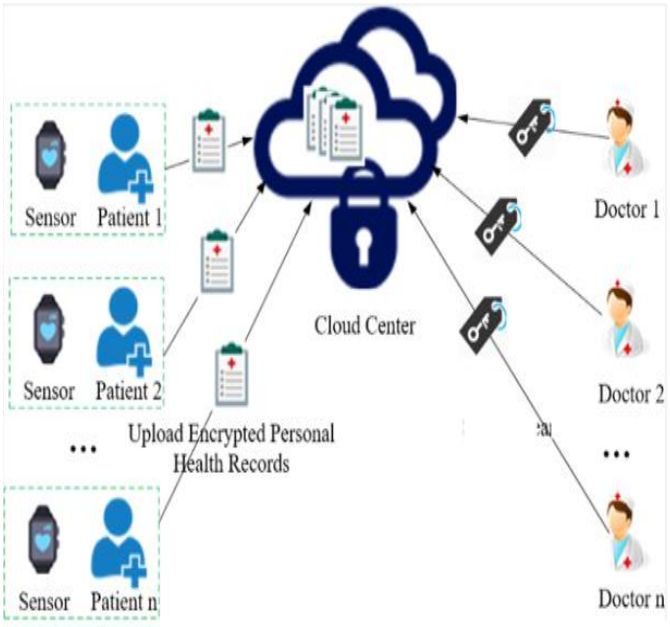


Fig 1: System Architecture

SYSTEM MODULES

1. Patient
2. Doctor
3. Cloud Server
4. Data collection and encryption phase
5. Data retrieval phase
6. Conditional authorization

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

Module Descriptions

- ***Patient module:***

A "Patient" module will be created in the main module, where a new afflicted individual can register by providing his details on a registration form. The impacted individual will no longer be able to access the laptop after registering. Only the patient can access it if the cloud server accepts the laptop; this is designed to prevent undesirable users and acts as a protection layer for the machine. This segment is responsible for managing the private scientific data (PMR) of the patients and accessing the uploaded patient records. PMRs are accumulated from encrypted records from various gadgets for storage to the cloud server. Savings. The affected person needs to upload his facts using blood within the module. Temperature, group, blood strain, and so forth. A personality is used to create each patient. An identifier for every affected person to avoid duplicates.

- ***Doctor Module:***

This module specializes in developing a new a part of the physician. He registers with the aid of filling out a registration shape along with his contact information. After registration, the medical doctor will not be able to get admission to the laptop. Same as the previous block. The cloud server is designed to make the system extra secure as best the medical doctor can access the system if he/she presents permission. The health practitioner module lets in active docs to access their patients' DMPs. They can look for patients, get entry to them securely and the confidentiality of the DMPs is preserved.

- ***Cloud Server Module:***

The cloud server module connects the affected person and the machine. Modules for medical doctors. It processes and shops encrypted PHRs. Data extraction requests. We used the Drive HQ cloud provider. A cloud file garage provider. In this phase, the cloud server is designed with the authority to approve or reject each patients and medical doctors, which additionally allows in securing the machine. It is the obligation of the service issuer to assign a affected person to a doctor in Sky. Additionally, as soon as a medical doctor makes a request for a specific patient, if any, the cloud server verifies it and accepts it as is.

- ***Data collection and encryption phase:***

Through this module, sufferers' non-public scientific records are accrued from extraordinary sufferers, uploaded to the cloud and encrypted on the server. In addition, it ensures the availability, integrity and confidentiality of the PHR through implementing safety features.

- ***Data retrieval phase:***

The statistics extraction module is chargeable for processing authorized requests for clinical statistics made by using medical doctors. He reveals the relevant facts. It decrypts it and sends it returned to the physician from the cloud server. Volume. This can simplest be accomplished in the event that they have a selected decryption key. The facts is available; otherwise, the information cannot be accessed. The key within the identical document adjustments from enterprise to agency. In this way, although an organization discloses the key, the file remains secure and cannot be accessed.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

- ***Conditional authorization:***

This module is the center of the DSAS challenge, which offers a cozy, green and searchable proxy re-encryption scheme, comfortable faraway tracking and PHR inspection. This allows Alice (the number one physician) to delegate Bob's participation in scientific research and applications (the clinical agent) through the cloud server, which allows lessen data publicity to the cloud server.

RESULTS AND DISCUSSION

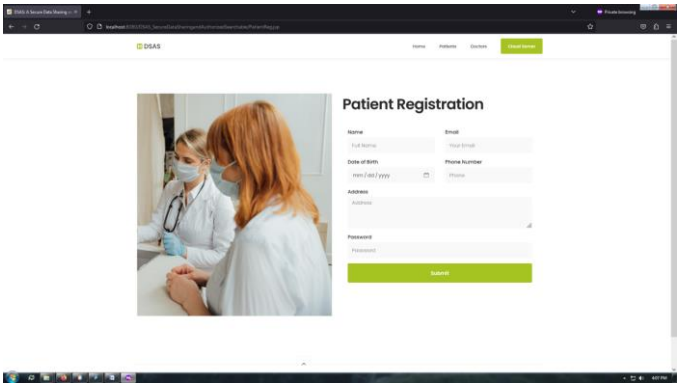


Fig 2: Figure of Patient Registration

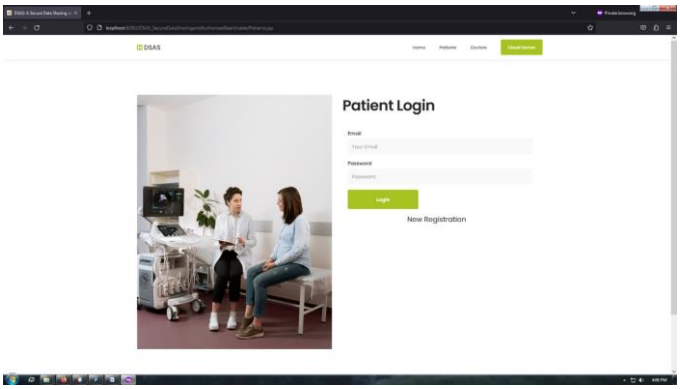


Fig 3: Figure of Patient Log in Page

Fig 4: Figure of Doctors Registration

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

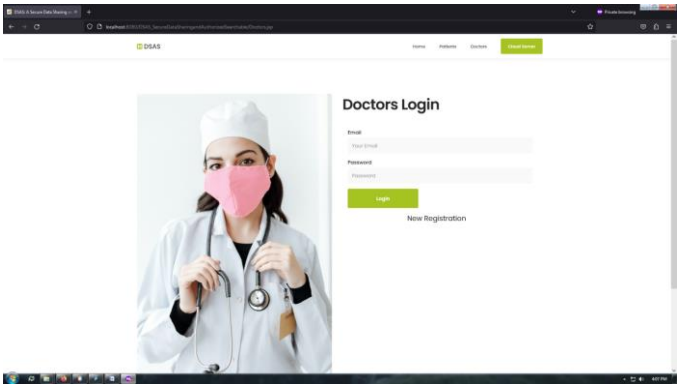


Fig 5: Figure of Doctors Login page

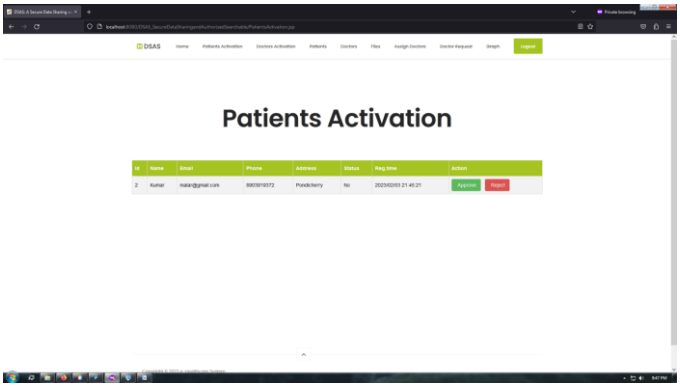


Fig 6: Figure of Patients activation

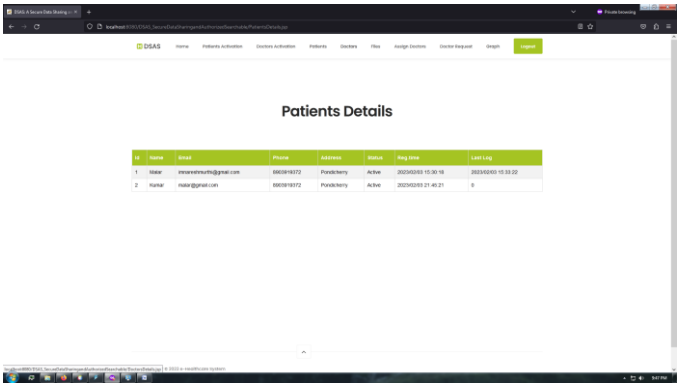


Fig 7: Figure of Patients Details Page

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

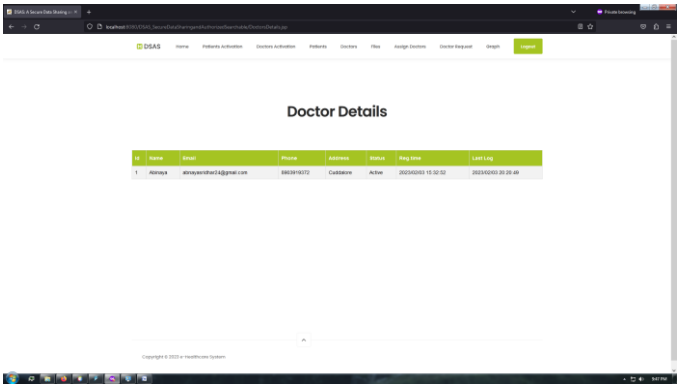


Fig 8: Figure of Doctor Details Page

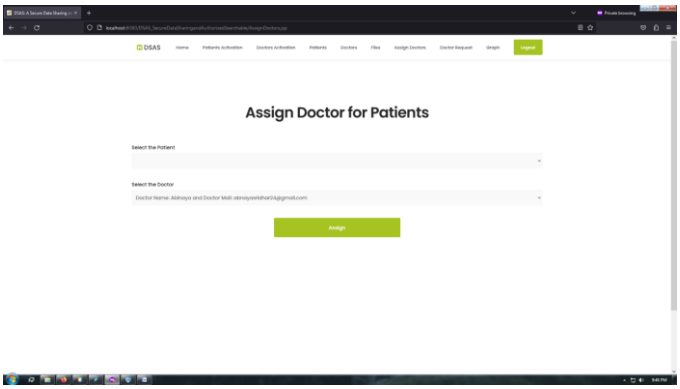


Fig 9: Figure of Assign Doctor for Patients page

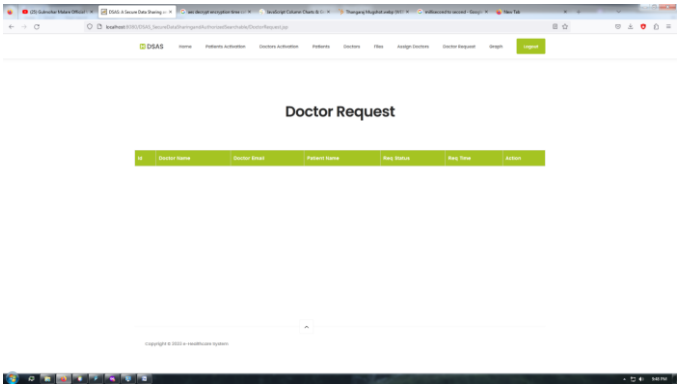
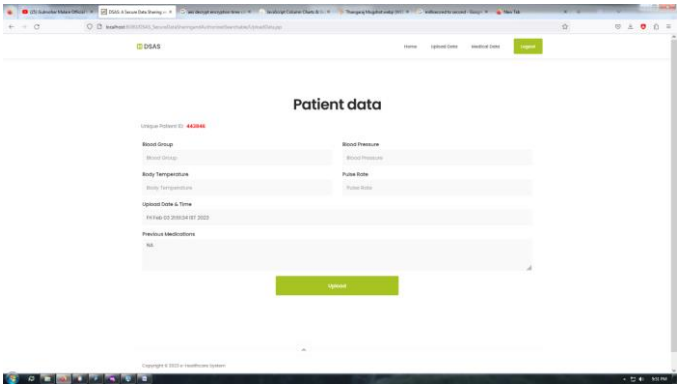


Fig 9: Figure of Doctor Request Page



Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

Fig 10: Figure of Patient Data page

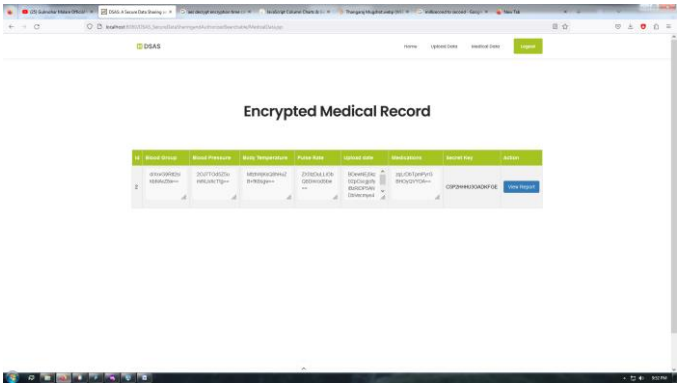


Fig 11: Figure of Encrypted Medical Record

Fig 12: Figure of Doctors Home page

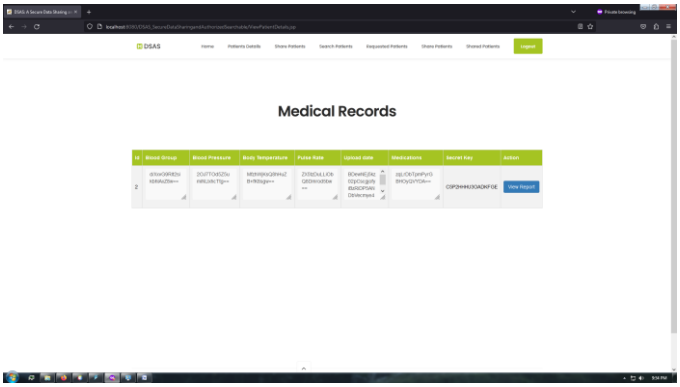


Fig 13: Figure of Medical Records

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

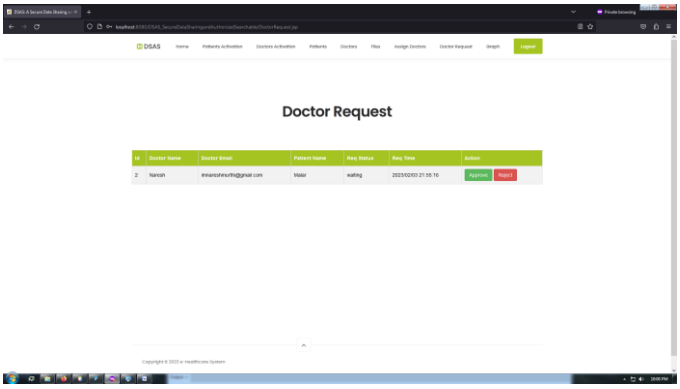


Fig 14: Figure of Doctors Request

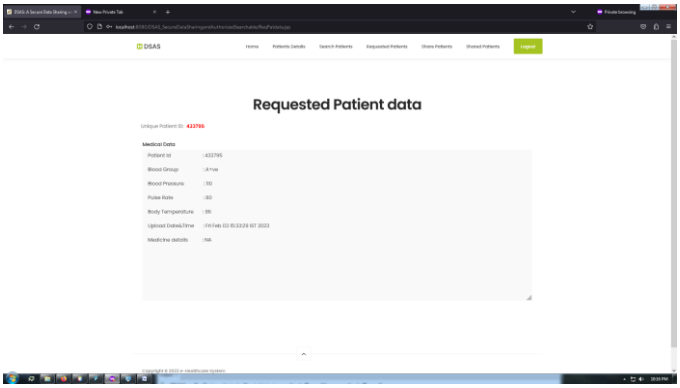


Fig 15: Figure of Requested Patient Data Page

CONCLUSION

This article presents an undetectable proxy concealing a nation known as proxy re-encryption. Electronic health systems employ sharing and delegation, utilizing a mechanism to protect data and facilitate keyword searching. Using our updated system, Bob the health practitioner can obtain conditional approval from Alice (the delegate). (The representative) supplies the essential element for re-encryption. The re-encryption key allows Bob to access the cloud server since he can decode the cipher text. The PHRs are initially encrypted using Alice's public key to ensure secure transmission. Locating encrypted PHRs is advantageous for the cloud server. You must initially notify the health professional of any underlying conditions you are unaware of. Significantly, we managed to achieve an asset that remains hidden from the proxy machine. This device includes an anti-collusion feature, meaning that even if an untrustworthy cloud server collaborates, Alice's (agent) private key will remain secure. In the presence of the representative Bob. We have demonstrated safety through extensive evidence, and comprehensive performance evaluations show that our DSAS-based software is both functional and efficient.

REFERENCES:

[1] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing,'' Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520, Mar. 2020.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 3, May-June 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i03.1377

[2] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal healthcare records using certicateless proxy re-encryption in cloud,'' Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2018.

[3] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserving high-order bi-Lanczos in cloud-fog computing for industrial applications,'' IEEE Trans. Ind. Informat., early access, May 28, 2020, doi: 10.1109/TII.2020.2998086.

[4] H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authentication as an intelligent process,'' IEEE Trans. Commun., vol. 67, no. 3, pp. 22602273, Mar. 2019.

[5] H. Fang, L. Xu, and X. Wang, ``Coordinated multiple-relays based physical- layer security improvement: A single-leader multiple-followers Stackelberg game scheme,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 197209, Jan. 2018.

[6] J. Feng, L. T.Yang, Q. Zhu, and K.-K.-R. Choo, ``Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment,'' IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857868, Jul. 2020.

[7] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, ``Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing,'' IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 45194528, Oct. 2018.

[8] D. He, M. Ma, S. Zeadally, N.Kumar, and K. Liang, ``Certificateless public key authenticated encryption with keyword search for industrial Internet of Things,'' IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 36183627, Aug. 2018.

[9] Q. Huang, L. Wang, and Y. Yang, ``Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities,'' Secur. Commun. Netw., vol. 2017, pp. 112, Aug. 2017.

[10] Q. Huang, Y. Yang, and J. Fu, ``PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social networks,'' Future Gener. Comput. Syst., vol. 86, pp. 15231533, Sep. 2018.

[11] M. Naz, F. A. Al-zahrani, R. Khalid, N. Javaid, A. M. Qamar, M. K. Afzal, and M. Shaq, ``A secure data sharing platform using blockchain and interplanetary le system,'' Sustainability, vol. 11, no. 24, p. 7054, 2019.

[12] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, ``Auditable time outsourced attribute-based encryption for access control in cloud computing,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 94105, May 2018.

[13] J. Ning, Z. Cao, X. Dong, and L. Wei, ``White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively,'' IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 883897, Sep./Oct. 2018.

[14] S. Niu, L. Chen, J. Wang, and F. Yu, ``Electronic health record sharing scheme with searchable attribute-based encryption on blockchain,'' IEEE Access, vol. 8, pp. 71957204, 2020.

[15] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, ``Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks,'' IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 37123723, Aug. 2018.