Journal of Electronics and Informatics (ISSN: 2582-3825)
www.irojournals.com/iroei/

A Safe and Reliable Approach to Transfer Health Records using Searchable Key Proxy Re-Encryption

Dr. I. Parvin Begum[1], Dr. S. Kalaivani[2], D. Nasreen Banu[3]

[1,2,3]Assistant Professor, Department of Computer Applications, B.S.Abdur Rahman Crescent Institute of Science and Technology, Vandallur, Deemed University, Chennai-600048

E-mail: [1]parvin@crescent.education, [2]kalaivani@crescent.education, [3]nasreen@crescent.education

Abstract

In the delivery of high-quality healthcare services, the exchange of computerized clinical data holds significant importance. To safeguard the confidentiality of client's sensitive information, it is imperative to adhere to stringent privacy and security regulations when sharing this data with others. Consequently, the adoption of proxy re-encryption servers serves as an effective and reliable means of transmitting computerized medical information. This encryption method is currently recognized as the sole approach that is both unidirectional and recursive, allowing third parties to modify encrypted ciphertext intended for one party so that it can be deciphered by another. This technique is referred to as proxy re-encryption. In order to empower patients with control over who can access their healthcare data, the system operates as an intermediary between them and a database server. Prior to transferring files to the information server, individuals who own them can utilize their keys to encrypt the files, thus ensuring the security of the data stored there. The test results demonstrate the system's proficiency in supporting secure data sharing. These proxy re-encryption mechanisms guarantee the confidentiality and accessibility of data, offering end-to-end security and privacy for electronically stored health information. While prioritizing patient privacy, the system aims to enhance collaboration among providers and facilitates data sharing between the sender and receiver using their respective keys. In this context, a unidirectional system operates in a one-way, providing a higher level of security, making it a suitable choice for untrusted

DOI: https://doi.org/10.36548/jei.2023.4.002
Received: 16.09.2023, received in revised form: 12.10.2023, accepted: 28.10.2023, published: 10.11.2023

environments where message transport is necessary without granting the receiver rights to respond to it.

Keywords: Proxy Re-Encryption, Cryptography, Healthcare Services, Cipher Text, Encryption, Decryption, Clinical Data

1. Introduction

Proxies are commonly employed for strengthening information security against various threats and for optimizing system performance, including tasks like load balancing and caching identical requests to enhance speed. A proxy functions as an intermediary between the client and the server, offering a secure gateway to resources while shielding the server from reversible encryption methods [1]. This reversibility means that if the same re-encryption key is used to decode messages from User1 to User2 and vice versa, it could inadvertently grant the receiving party authorization to initiate contact with the sender. Consequently, in such systems, the generation of these re-encryption keys hinges on mutual trust and consensus between the sender and receiver, who employ their respective keys for this purpose [2-4].

2. Literature Survey

The proposed framework ensures data integrity, confidentiality, and availability, and is resistant to various attacks, such as replay attacks and impersonation attacks. The authors also provide a detailed analysis of the security and efficiency of the proposed framework, demonstrating its practical feasibility for real-world healthcare applications. Overall, the review concludes that PRE is a promising technique for secure transmission of clinical data, and further research is needed to develop more efficient and effective PRE-based schemes for clinical data transmission [16].

They provide a detailed analysis of the performance and security of PRE- based EHR transmission, comparing it with other encryption techniques such as homomorphic encryption and attribute-based encryption. The authors conclude by identifying potential directions for future research in this area, such as the integration of block chain and smart contracts to enhance the transparency and accountability of PRE-based healthcare data exchange, and the development of standardized protocols and benchmarks for evaluating the performance and security of PRE techniques [17].

3. Problem Definition and Methodology

Encryption: Encryption involves the conversion of plaintext into an encoded format known as ciphertext, which is unintelligible to unauthorized individuals. Encryption offers a secure means of transmitting sensitive information over insecure communication channels. The ciphertext can only be transformed back into the original plaintext by authorized parties who possess the decryption key. Encryption operates by employing an algorithm to obfuscate the data into ciphertext, a process that can only be reversed with the corresponding decryption key. The algorithm used for encryption is usually complex and mathematically based, making it difficult for unauthorized users to decipher the cipher text without the key [9-12]].

Proxy Re-Encryption : Proxy re-encryption is a cryptographic method enabling a third party, referred to as a proxy, to convert ciphertext originally encrypted under one key into ciphertext encrypted under a distinct key, all without disclosing the actual plaintext. In simpler terms, it empowers a proxy to re-encrypt messages exchanged between two parties employing different public keys, all without necessitating the proxy to decrypt the message. The proxy re-encryption process revolves around three entities: the sender, the proxy, and the recipient [5-8].

The steps involved in proxy re-encryption are as follows:

1. The sender employs the recipient's public key to encrypt the plaintext message, resulting in ciphertext.
2. The sender transmits the ciphertext to the proxy.
3. The proxy restructures the ciphertext from the recipient's public key to its own public key, all without decrypting the ciphertext.
4. The proxy forwards the re-encrypted ciphertext to the recipient.
5. The recipient employs their private key for decryption, effectively recovering the original plaintext.
6. The primary benefit of proxy re-encryption is its capacity to establish secure communication between two parties who employ different public keys, eliminating the necessity for direct public key exchange. Additionally, it empowers the proxy to

manage access to the ciphertext and, if required, to revoke access by re-encrypting it with a new key.

Decryption: It involves the conversion of encrypted text back into plain text, utilizing a decryption key that allows for this transformation. Decryption, the reverse procedure of encryption, enables specific individuals to access and read the original message. To encrypt data, a decryption algorithm and key are essential. The decryption key typically comprises a mathematical formula or a set of instructions that reverses the encryption process, facilitating the conversion of encrypted text into plaintext and restoring the original content [13-15].

4. Proposed System

This architectural design provides a comprehensive overview of the research, elucidating the organization of the developed system, including its various modules, their externally observable characteristics, and the interconnections between them. The Proposed proxy re-encryption scheme for E-healthcare data sharing deals with the problem of overhead and delay of previously proposed proxy re-encryption schemes. These proxy re-encryption schemes provide end-to-end security and privacy protection for electronic health records, while ensuring data integrity and availability. The system aims to improve collaboration and data sharing among healthcare providers while ensuring patient privacy. The figure.1 below depicts the system architecture diagram for the entire system.

Advantages:

- PRE enables the encryption of data in such a way that it remains confidential during transmission and storage.
- PRE can enhance the security of a system by protecting against attacks such as man-in-the-middle attacks, and unauthorized access.
- PRE can help protect the privacy of data by allowing it to be shared only with authorized users.

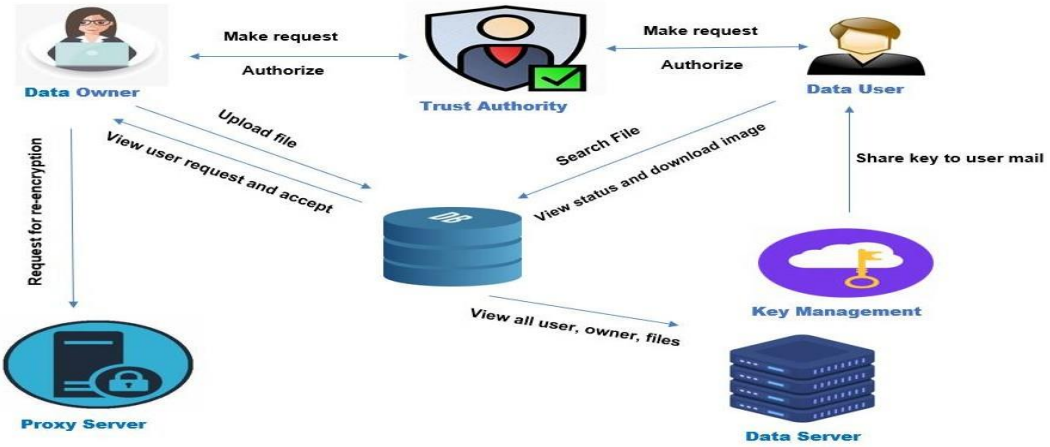


Figure 1. Architecture Diagram

4.1 Design and Development

Design Tools

- HTML (Front End)
- Java (Back End)
- MYSQL (Data Base)
- NETBEANS(IDE)

The implementation process includes: Data Owner, Data User, Trust Authority, Data Server, Proxy Server and Key Management.

HTML (Front End)

The front end of the application is developed using the HTML (Hyper Text Markup Language) , the user interface is built using the HTML, which serves as the backbone of the website that includes the user interface, the search interface, search functionalities, encryption and decryption, proxy re-encryption and the user authentication.

Java (Back End)

The backend of the website is developed using Java the constituents of the backend are the server, database, search engine, API, key management, security measures, authentication and authorization, Proxy Re-Encryption Service, and scalability in order to afford the volume of data flow and monitoring to detect as well as respond to the issues in the security

MYSQL (Data Base)

MySQL is a popular open-source relational database management system (RDBMS) based on structured query language. It is used in the proposed approach for the purpose of web database to store the details form single record information to entire details of the patients.

Net Beans

Net Beans is a popular and widely used integrated development environment (IDE) for developing Java applications. It establishes the connectivity across the java application and the relational database used.

4.2. Classification of Proxy Re-Encryption

Proxy re-encryption schemes (PRE) can be categorized into the following two groups:

- One –way Scheme
- Two-way Scheme

(i) Unidirectional schemes are : (i) IB-PRE-Identity-based proxy re-encryption , (ii) CPRE, (iii) CP-ABE-Ciphertext policy attribute based Proxy re-encryption, (iv) Key private Proxy re-encryption, (v) Time based Proxy re-encryption.

(ii) Bidirectional Scheme are: Type and threshold PRE

A method for enabling identity- and type-based proxy re-encryption has gained attention due to the challenge of managing multiple delegations of decryption privileges. Consider a scenario where a message's delegator wishes to grant different users access to various parts of the message. Relying on the proxy to use this method for re-encrypting specific portions of the ciphertext seems like a viable solution. However, if the proxy makes a mistake, this approach can fail. Alternatively, using a unique set of keys for each recipient is a more effective but impractical approach. Built upon the Boneh-Franklin Identity-Based Encryption technique, this identity-based proxy re-encryption framework allows for the implementation of distinct access control policies for cipher texts for various receivers based on their decryption criteria. Communications are categorized into different groups depending on the intended receivers' decryption requirements. The primary advantage lies in the concept of conditional proxy re-encryption (CPRE), where only cipher text that meets specific criteria set by the

sender can be re-encrypted and subsequently accessed by the receiver. This concept is especially valuable in situations where fine-grained control over data transfer is necessary and where predefined conditions must be met.

Furthermore, the security of the method against Chosen Ciphertext Attacks (CCA) has been demonstrated. The technique has undergone refinements, enabling it to operate in various scenarios, as opposed to the original conception, where it was limited to just one condition. The requirements can encompass a wide range of criteria set by the involved parties and the algorithm's adaptability to meet those requirements.

When dealing with a scenario where a predefined set of numbers or attributes plays a crucial role, Attribute Proxy Re-Encryption Schemes (A-PBE) offer an enhanced solution. Moreover, this approach simplifies the management of user authentication, especially in situations involving the duplication of users during an engagement. The figure. 2 shows the overall system architecture.

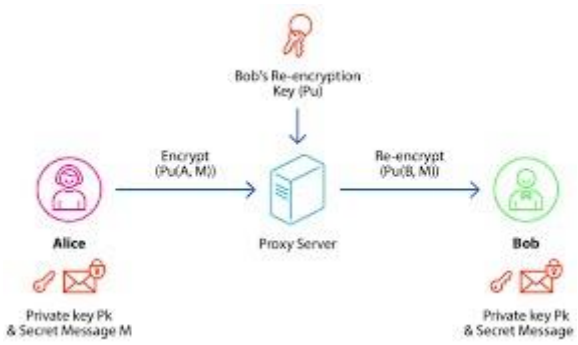


Figure 2. Proxy Encryption Scheme [18]

proxy re-encryption, bidirectionality refers to the ability to perform re-encryption in both directions. When re-encryption supports two-way operations, it is categorized as a bi-directional scheme. This characteristic finds applications in various scenarios, such as secure file systems.

Secure file systems naturally benefit from the use of proxy re-encryption, primarily because PRE often operates under an assumption of untrusted storage. Many distributed file systems address the challenge of creating confidential storage using untrusted components by implementing cryptographic storage. In this setup, the confidentiality of data is achieved as the content of the stored files are encrypted. After that, these encrypted files can be safely stored

on untrusted file servers, enabling data sharing without giving server administrators access to the content's plaintext.

Access control is simple with a single-user crypto file system since there are no key distribution problems because the user creates all of the keys needed to protect the content. In situations where group sharing is included in encrypted storage, however, members of the group must work together with the content owner to acquire decryption keys in order to access files. Access control key distribution in encrypted storage systems, such as the CNFS or SWALLOW object store, frequently depends on an out-of-band method.

Alternatively, certain systems like Cepheus, uses servers with the trusted access control to handle key distribution. In this model, significant trust is placed in the administrator of the server. In the event that the operator is shown to be unreliable, there is a risk of abuse because the server's key material might be utilized to decrypt any data that is kept on the system.

4.2.1. Improved Proxy Applications

To discuss "enhancements," it's important to first understand the advantages and limitations of previous schemes. Below is a compilation of what we consider to be the most valuable characteristics of proxy re-encryption protocols:

1. Unidirectional: Authorization from A → B blocks re-encryption taking place from B → A.

2. Non-interactive: Alice can generate re-encryption keys using Bob's public key without the need for input from a trustworthy third party[18].

3. Proxy invisibility: This is an essential feature that the original BBS scheme provided. Because the proxy functions transparently under the BBS system, neither the delegates nor the sender of an encrypted message needs to be aware of the proxy's presence. While it's undeniably a desirable attribute, transparency in the BBS scheme means that delegation transitivity and participant master secret retrieval are made possible. In our forthcoming schemes that are based on pairing, less robust form of transparency known as "proxy invisibility" was introduced. Specifically, the sender is reminded of the proxy's involvement and give them the choice of encryption generation with the permission to be accessed only by the recipient to whom it is intended (referred to as a 1st level encryption) or by any of the recipient's delegates (2nd level encryption). However, we can ensure that no delegate will be

able to discern between a re-encryption of a ciphertext meant for a different party and a first-level encryption (calculated using their public key). This is presuming that there is nothing in the encrypted communication that would help the delegate draw this distinction.

Advantages:

- PRE facilitates the encryption of data, ensuring its confidentiality during both transmission and storage.
- PRE may boost the safety of a system by defending it from attacks like man-in-the-middle attacks and illegal entry.
- By enabling data exchange exclusively among designated individuals, PRE can assist in upholding the confidentiality of that data.

4.2.2. Data Flow Diagram

The flow and transformation of information as data moves from the input to the output are visually represented in a data flow diagram. Data flow diagram shown in figure.3 serves the purpose of clearly communicating the system requirements and pinpointing significant alterations to the system design.

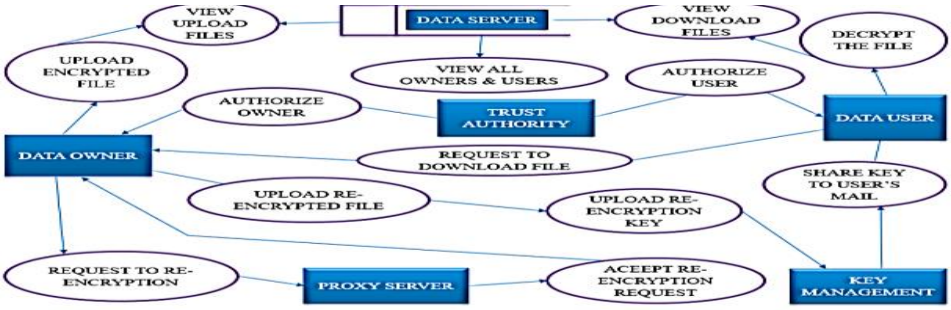


Figure 3. Data Flow Diagram

4.2.3. Sequence Diagram

The sequence diagram depicted below in figure.4, is constructed using the Unified Modeling Language (UML), is a visual representation designed to depict the exchange of messages between objects as part of an interaction. In a sequence diagram, the elements

represent a set of objects and illustrate the messages sent and received during the course of the interaction.

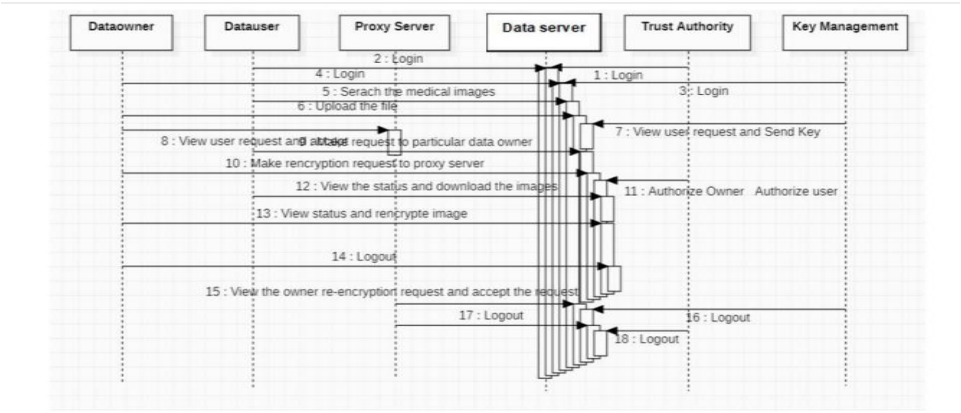


Figure 4. Sequence Diagram

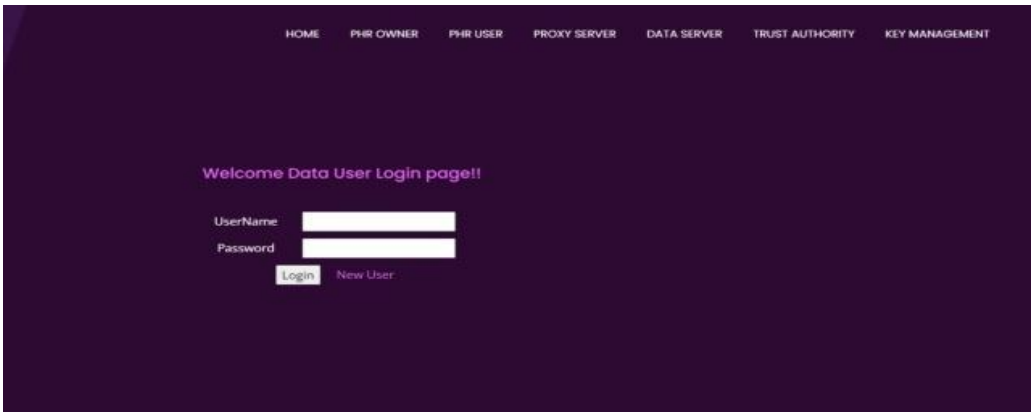
5. Result and Discussion

The figure .5 a-e presents the user interface developed to access the health records using searchable key proxy re-encryption and illustrates the steps involved in accessing the files safely.

(a)

Proxy Server

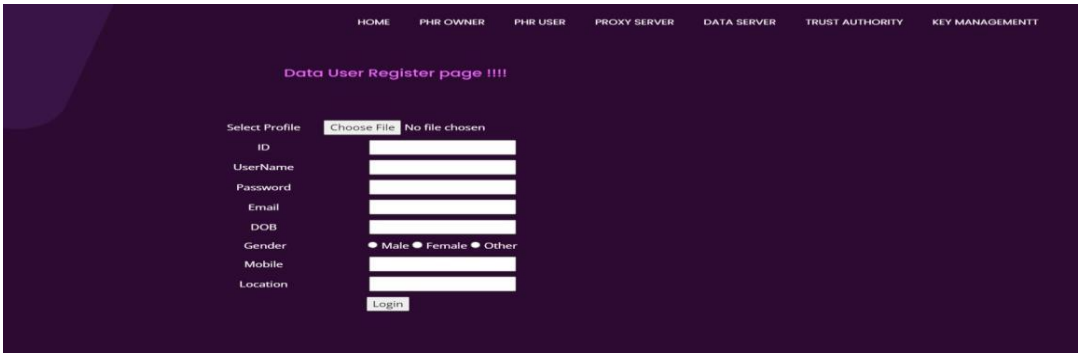
Step 1: Login the account with correct credentials.



(b)

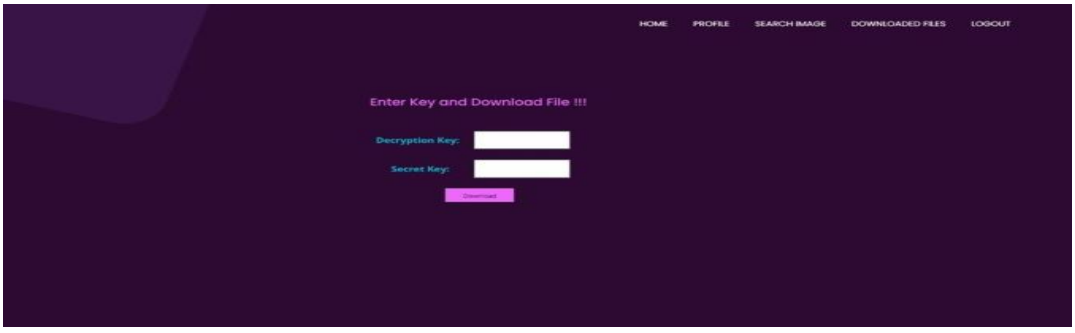
Data Owner

Step 2: Register the account with the basic information



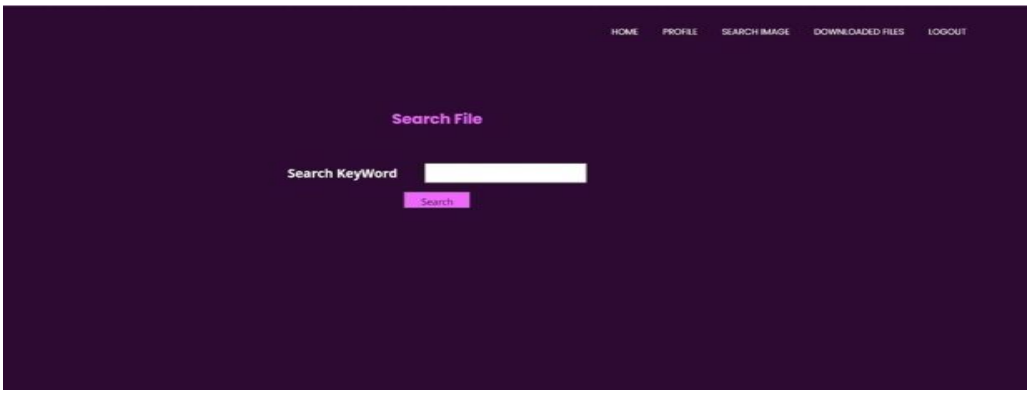
(c)

Step 3: Download the file using key



(d)

Step 4: Search the file in the server



(e)

Step 5: After re-encrypt, upload to new keys

Figure 5. (a) Home Page, (b) Login Page, (c) Registration Page, (d) User Authentication, (e) Server Page

6. Analysis

Proxy Re-Encryption (PRE) has emerged as a viable solution for ensuring secure data sharing within electronic healthcare systems, especially when patient data needs to be accessible to multiple healthcare providers while preserving patient privacy.

In this context, a proxy server serves as an intermediary between a client and a server, offering various services, including security and encryption. The degree of encryption provided by a proxy server can vary, contingent on the type of proxy server and its configuration settings. The proxy has the capacity to re-encrypt the data using a distinct key and supply the newly encrypted data (ciphertext) to authorized healthcare providers.

Proxy servers typically offer a higher level of encryption compared to other servers, such as web servers or file servers. This is because proxy servers are specifically designed to function as secure gateways between clients and servers, allowing for the configuration of protocols like SSL or TLS to encrypt data during transit between the client and the proxy server.

In contrast, web servers and file servers may not inherently provide encryption and might necessitate additional setup or third-party tools to establish secure connections. Nonetheless, recognizing the encryption level alone is not the sole determinant of security. Other elements, such as server configuration and the security of the underlying network, also contribute to the overall security of the system.

Overall, research findings indicate that PRE-based systems can effectively facilitate secure and efficient data sharing in electronic healthcare systems while upholding patient privacy.

6.1. Comparison between Existing System and Proposed System

The table.1 compares the various aspects of the existing and the proposed system to ensure the efficiency of the proposed over the existing.

Table.1 Comparative Analysis

Aspects	**Existing System**	**Proposed System**
Data Security	Relies on traditional methods and may not prevent breaches.	Significantly enhances data which may have vulnerabilities security through proxy re- encryption keys. Minimizes the risk of unauthorized access.
Patient-Centric Care	Patients have limited control over their records and may not actively participate in their healthcare management.	Empowers patients to actively manage their health records and share them with chosen healthcare providers.
Scalability	May face scalability issues in accommodating growing data volumes and changing needs.	Scalable and adaptable to the evolving needs of healthcare organizations.
Privacy Preservation	Patient privacy can be at risk due to sharing encryption with authorized users.	Prioritizes patient privacy keys and enables secure data sharing without revealing encryption keys.
Selective data Sharing	Data sharing is complex and challenging to control.	Offers granular control over data sharing, allowing selective sharing.
Efficient Data Retrieval	Data retrieval can be time-consuming, hindering timely access to patient information.	Enables efficient and secure to specific data within access to health records.

6.2. Testing Phase

Regression testing: Regression testing is conducted to verify that modifications introduced to a software application, system, or process do not result in unintended adverse consequences and do not lead to the failure of existing functionality. Below are several regression testing approaches suitable for a Proxy Re-Encryption employed in the proposed.

Smoke Testing: This form of testing is executed to confirm that the core functionalities of the system are operating as intended. For instance, a smoke test was conducted following an upgrade to the Proxy Re-Encryption system to verify that the system can successfully re-encrypt data in accordance with the access policies defined for various users.

Sanity Testing: This testing approach is carried out to confirm that the alterations made to the system have not negatively impacted its pre-existing functionalities. For instance, after an upgrade to the Proxy Re-Encryption system, sanity testing is employed to verify that the existing data transmission procedures remain operational and unaffected.

Risk-based Regression Testing: In this testing methodology, test cases are ranked according to the risk posed by a potential failure. For instance, test cases linked to the transfer of medical images might receive a higher priority than test cases connected to data sharing policies, as a failure in the former could result in more significant repercussions.

Prioritization-based Regression Testing: In this testing approach, test cases are arranged in order of their significance, and the most vital ones are executed as a priority. For instance, test cases concerning patient confidentiality and data security may be accorded a higher priority than test cases associated with user interface testing.

Full Regression Testing: Comprehensive Regression Testing: This form of testing is conducted to verify that all system functionalities perform as anticipated following any modifications. For instance, a full regression test can be carried out after upgrading the Proxy Re-Encryption system to ensure that all functionalities, such as encryption, decryption, and data transmissions, are functioning accurately.

Acceptance Testing: Acceptance testing involves the confirmation that the system aligns with the user's requirements and anticipations. Typically, this type of testing is conducted by end-users or stakeholders who will be utilizing the system. Below are the steps encompassed in acceptance testing for a Proxy Re-Encryption.

User Acceptance Testing (UAT): This testing phase is conducted by end-users with the aim of ascertaining whether the system aligns with their needs and expectations. In the context of a Proxy Re-Encryption (PRE), UAT may encompass the creation of test scenarios that simulate end-users' real-world use cases. As an example, an end-user might be tasked with

encrypting a file and sharing it with another user using PRE. The UAT process evaluates the encryption and sharing procedures.

Operational Acceptance Testing: This type of testing evaluates whether the system is able to function in the real world under normal operational conditions. For a PRE, operational acceptance testing can involve testing the system's ability to handle a large number of users, files, and requests. For example, the testing team might simulate a scenario where hundreds of users are simultaneously encrypting and sharing files using PRE.

Compliance Acceptance Testing: This form of testing assesses the system's adherence to relevant laws and regulations. In the context of a Proxy Re-Encryption (PRE), compliance acceptance testing may encompass evaluating the system's capability to manage sensitive data and safeguard user privacy. For instance, the testing team might simulate a scenario in which the PRE system is utilized for storing and sharing confidential medical records. During this testing process, the system's compliance with pertinent privacy laws and regulations would be assessed.

Security Acceptance Testing: Security Vulnerability Testing: This testing approach examines the system's capacity to defend against external threats and vulnerabilities. For instance, the testing team might create a scenario in which an attacker attempts to intercept and decrypt a file encrypted using PRE. Subsequently, the testing process assesses whether the PRE system can effectively identify and thwart such attacks.

7. Conclusion

This study primarily emphasizes the development of a secure and dependable approach for transferring health records, built on the principles of searchable key proxy re-encryption. Proxy re-encryption (PRE) technology stands out as a promising solution for enhancing the security and efficiency of electronic healthcare data sharing. These techniques are instrumental in maintaining the confidentiality of sensitive user data, particularly when dealing with entrusted servers.

In summary, the integration of PRE in electronic healthcare data sharing initiatives holds substantial potential for enhancing the overall security, privacy, and efficiency of data exchange while aligning with legal and regulatory standards. Nevertheless, it is imperative to

meticulously consider the design and implementation of such systems to ensure robust security and the safeguarding of sensitive patient information.

References

[1] Chen.Z & Li.X (2022). "An Improved Proxy Re-Encryption Scheme with Verifiable Decryption for Secure Data Sharing. IEEE Transactions on Information Forensics and Security", 17, 56-67.

[2] Thomas Wang.W & Cheng.L (2021). "A Privacy-Preserving and Efficient Proxy Re-Encryption Scheme for Electronic Health Record Sharing. Journal of Medical Systems", 45(7), 1-12.

[3] Carlye Wu.X & Huang.X (2021). "A New Proxy Re-Encryption Scheme with Keyword Search. Journal of Ambient Intelligence and Humanized Computing", 12(6), 6021-6032.

[4] Huang.X, Jiang.Y & Wu.J (2020). "A Secure and Efficient Proxy Re-Encryption Scheme with Attribute-Based Access Control. Journal of Information Security and Applications", 50, 102378.

[5] Al-Fardan.N & Almajed.A (2020). "A Novel Secure Data Sharing Framework for Electronic Health Records Using Blockchain and Proxy Re-Encryption".IEEE Access,8, 52985-52997.

[6] Ahmed .F., Younis.M.Z., Naseer .M.M & Abbas.H., (2020) " Secured Data Sharing in Medical Cyber – Physical Systems Using Attribute –Based Re-Encryption ", IEEE Transactions on Industrial Informatics, 17(8),5864-5874.

[7] Guo.H, Liu.Y, Yang.Z & Zeng.G (2022). "Secure and efficient data sharing for mobile healthcare based on proxy re-encryption. Personal and Ubiquitous Computing", 26(2), 197-207.

[8] Chenthara S, Ahmed K, Wang H, Whittaker F. "Security and privacy-preserving challenges of e-Health solutions in cloud computing". IEEE Access, 2019, 7(99):74361–74382. 10.1109/ACCESS.2019.2919982.

[9] Raaj Anand Mishra, Anand Mishra, Anshuman Kalla, An Braeken, Madhusanka Liyanag, “Privacy Protected Blockchain BasedArchitecture and Implementation”. Information Processing & Management · January 2021.

[10] L. Jiang, D. Guo, “Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage,” IEEE Access 5 (2017) 13336–13345.

[11] Ghaznavi.A, Al-Muhtadi.N & Al-Ghamdi.A (2019). “Secure Transmission of Electronic Health Records Using Proxy e-Encryption: A Comprehensive Review”. IEEE Access, 7, 31893-31905.

[12] Mohammed Seid Yimam Martinaa, Dr. K Suresh Babu, “ ProxySecure identity-based data sharing and profile Matching for mobile healthcare social Networks in cloud computing: a review”. Journal of Engineering Volume: 8, Issue: 35, Pages: 1-5 M. (2017) 13336–13345.

[13] Guo, C. Zhang, J. Sun, and Y. Fang “A privacy-preserving attribute-based authentication system for eHealth etworks,”. Guo, C. Zhang, J. Sun, and Y. Fang, ‘‘PAAS : ’’ in Proc. 32nd Int.Conf. Distrib. Comput. Syst., Macau, China, Jun.2012, pp. 224–233.

[14] Yang, X. Liu, and R. H. Deng, ‘‘Lightweight break-glass access control system for healthcare Internet-of-Things”,IEEE Trans. Ind. Inform., to be published, doi: 10. 1109/TII.2017.2751640.

[15] An Wang, J. Ma, F. Xhafa, M. Zhang, and X., Luo, ‘‘Cost-effective secure E-health cloud system using identity based cryptographic techniques”, Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.

[16] A. Ghaznavi, N. Al-Muhtadi, and A. Al-Ghamdi, "Secure Transmission of Electronic Health Records Using Proxy Re- Encryption: A Comprehensive Review" by published in IEEE Access, 2019.

[17] Nasser Al-Fardan and Alhussain Almajed, “A Novel Secure Data Sharing Framework for Electronic Health Records Using Blockchain and Proxy Re-Encryption" by published in IEEE Access, 2020.

[18] Alsayegh, Muneera, Tarek Moulahi, Abdulatif Alabdulatif, and Pascal Lorenz. "Towards secure searchable electronic health records using consortium blockchain." Network 2, no. 2 (2022): 239-256.

Author biography

Dr.I.Parvin Begum : Myself Dr.I.Parvin Begum and i received my Ph.d (Computer Science) from Dravidian University, Andhra Pradesh, M.Phil (computer science) from Periyar University at Salem, in 2007, MCA from Madurai Kamaraj University in 2004. B.E.S (Bachelor Electronic Science) from Madras University in 2001. Currently i am working in the post of Assistant Professor, B.S.Abdur Rahman Crescent Institute of Science and Technology, Vandallur, Deemed University, totally sixteen years of teaching experience. I was published seven international journals and also published four papers in national conference. My research area is data mining and Artifical Intelligence.