IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303281 |

A Protected Information Sharing and Approved Accessible Structure for E-Medical Care Framework – Dsas

C Malathi[1], B Sai kumar[2], S Mansoor[3], S Harshavardhan[4], D Sravani[5]

Assistant Professor, Department of CSE, AITS, Tirupati, India [1]

Student, Department of CSE, AITS, Tirupati, India [2, 3,4,5]

ABSTRACT: Facilitating the secure exchange of encrypted personal health records (PHRs) among healthcare professionals or research institutions. Involved in clinical studies, an increasing number of patients within the e-healthcare system can access high-quality medical services. However, a primary challenge lies in the difficulty of effectively searching for information within scrambled PHRs. This is addressed by reducing the amount of data used and by ensuring the availability of doctors online, which can be costly for some professionals. To tackle these issues, a novel, secure intermediary re-encryption approach is proposed, enabling healthcare Facilitate secure remote monitoring and research of Personal Health Records (PHR) by engaging reliable service providers. The proposed scheme ensures the privacy of PHRs by allowing access to the data is limited to authorized doctors or research institutions only. with the ability for designated clinical decisions by the overseeing physician. Furthermore the information gathered by healthcare devices undergoes encryption prior to its transmission to the cloud server. Limiting access to the information to authorized entities. The concept of security is formalized, and the efficacy of the proposed solution is demonstrated through performance analysis.

KEYWORDS: Healthcare, proxy re-encryption, proxy invisibility, encryption.

I. INTRODUCTION

Currently, the widespread commercial adoption of e-healthcare sensor networks is facilitated by the rapid progress in wearable technology, sensors, and artificial intelligence, indicating a level of maturity in these technologies. A mobile platform integrated with an e-healthcare sensor network has demonstrated significant benefits for individuals seeking efficient and high- quality medical care. Through sensor devices embedded in patients' devices, a wealth of personal healthcare data is collected, enabling health care professionals to enhance diagnostic accuracy and cater to patients' needs more effectively. Additionally, leveraging such data, analysts and researchers in the medical field can conduct in-depth analytics to gain insights into diseases and develop more efficacious treatments. However, the storage of these data in third-party cloud services introduces security risks, including the potential for data breaches, as neither patients nor medical practitioners have direct access to the data when it is outsourced. Thus, preserving the confidentiality and privacy of outsourced data is paramount in such an environment. For instance, certain healthcare facilities amass extensive Personal Health Records (PHRs), which are stored on cloud servers, with authorization granted to entities like the Centers Utilize data from the (CDC).While doctors are authorized to utilize data mining techniques for disease prevention and control, traditional data mining methods inevitably pose a risk of disclosing private patient information. A significant challenge lies in securely storing and retrieving PHRs. Ensuring heightened security and privacy protocols for both data storage and access is imperative within the e-healthcare system.

II. RECENT WORKS

[1] H. Shi at al., "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions,"2005, pp. 205–222. We have identified and rectified several inconsistencies in the generation of false positives within the realm (PEKS). Our proposed improvements involve a comprehensive redefinition of absolute uniformity, addressing both computational and statistical aspects. We showcase the computational uniformity of the system and introduce an innovative statistically uniform scheme Furthermore, we introduce a secure Partially Homomorphic Encryption Key Scheme (PEKS) that guarantees consistency when transitioning from an anonymous Identity-Based Encryption (IBE) scheme.

[2] G. Ateniese at al. Enhanced protocols for proxy re- encryption, accompanied by practical implementations, have

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303281 |

been developed to bolster the security of distributed storage systems. ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, 2006. We introduce a set of highly secure proxy re-encryption methods that outperform previous approaches in terms of efficiency. The primary advantages of our systems lie in their uni-directionality, where Alice can delegate to Bob without requiring reciprocal delegation, and in the delegators' ability to withhold some secret key information.

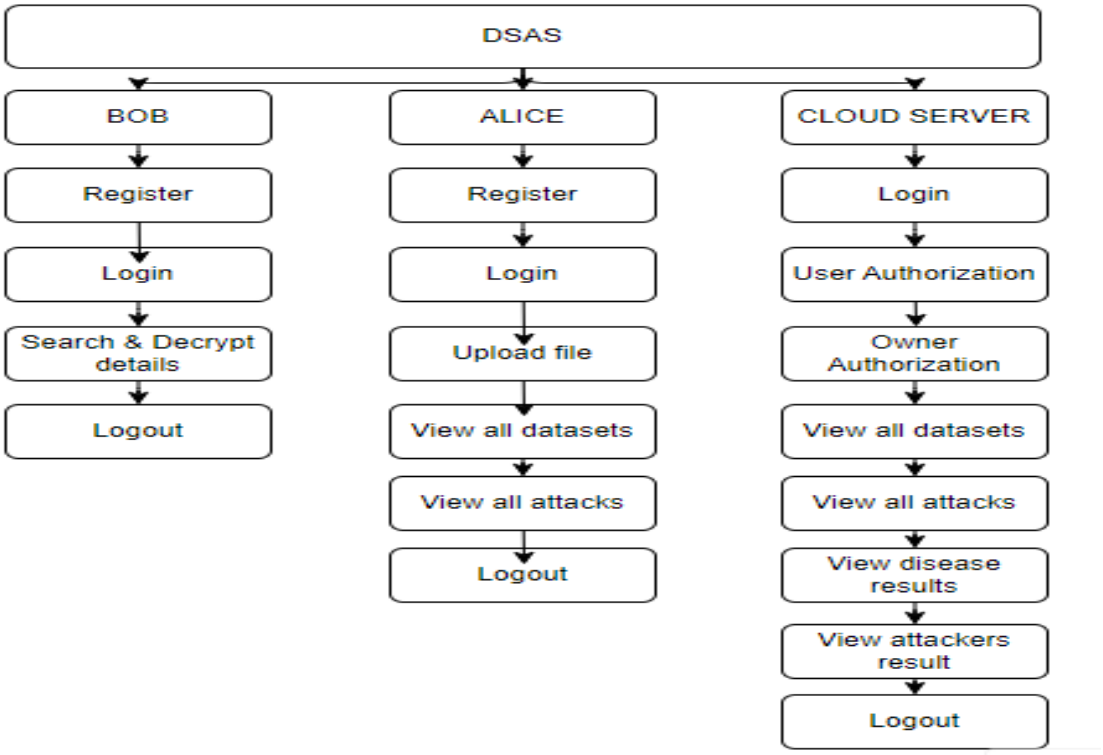
[3] J. Baek at al. "The reconsideration of keyword search in public key encryption." in Proc. Int. Conf. Compute. Sci. Appl. (ICCSA), 2008, pp. 1249–1259. We identify three crucial challenges left unaddressed in their paper. These challenges involve the management of keyword renewal, the removal of a secure channel requirement, and the accommodation of multiple keywords. We advise caution regarding the frequent utilization of keywords in the PEKS scheme, as it may pose a potential threat to its security. Furthermore, we underscore the inefficiencies inherent in the original PEKS scheme, attributed to its dependence on a secure channel

[4] T. Bhatia, A. K. Verma, and G. Sharma, "Creating a reliable incremental proxy re- encryption method to improve the secure exchange of e-healthcare information within the realm of mobile cloud computing. Published in the journal Concurrency and Computation: Practice and Experience, Volume 32, Issue 5, on page e5520 in March 2020. The given information emphasizes the extensive embrace of cloud computing within the e-healthcare industry, leading the utilization of shared resources. However, it also raises concerns about the safeguarding of data stored in cloud environments. Particularly due to the dependence on the cloud for handling computational tasks on mobile devices with limited resources.

III. PROPOSED WORK EXPLANATION

In proposed system the system must have a authorized authorization and authentication mechanism that ensures only authorized individuals can access patient data. This can be achieved through password-based authentication, two-factor authentication, or biometric authentication.

PROJECT FLOW:



Algorithm Steps:

1. Key Expansion:

The original key undergoes expansion to generate a key schedule comprising multiple round keys. Each round key is obtained through a key schedule algorithm applied to the original key.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303281 |

2. Initial Round:
The plaintext is divided into blocks (typically 128 bits in AES).
The initial round adds the round key to the plaintext. The block's each byte undergoes XOR with the corresponding byte of the round key.

3. Rounds:
AES functions by executing a series of rounds, and the quantity of rounds varies based on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each round encompasses four primary steps.

- Sub Bytes: The block experiences byte substitution, wherein each byte is exchanged Associate each byte with a designated value from a pre-established substitution box, commonly known as an S-box.
- Shift Rows: The bytes in each row of the block are subjected to a cyclic left shift. The first row remains unchanged, the second row shifts one byte to the left, the third row shifts two bytes to the left, and the fourth row shifts three bytes to the left.
- Mix Columns: The process involves treating each column within the block as a polynomial and performing multiplication modulo a predetermined polynomial. This particular step contributes to the introduction of diffusion in the system.
- Add Round Key: The block's each byte undergoes XOR with the corresponding byte of the round key.

4. Final Round:
In the previous iteration, the Mix Columns step is deliberately omitted. Instead, the Sub Bytes, Shift Rows, and Add Round Key steps are carried out following the standard procedure.

5. Output:
After the final round, the resulting ciphertext is obtained.
To decrypt the ciphertext, the process is reversed using the inverse operations of AES. The order of the round keys is utilized in a reversed manner.

IV. RESULTS AND DISCUSSION

Result:
Within the e-healthcare system, a new intermediary re-encryption technique addresses hurdles in accessing encrypted Personal Health Records (PHRs). It improves remote PHR monitoring and research by granting secure access solely to authorized healthcare providers. Data encryption before uploading enhances privacy. Formal security measures and performance analysis validate the effectiveness of this approach. Key terms include healthcare, proxy re- encryption, privacy, and homomorphic encryption.

Discussion:
The suggested intermediary re-encryption approach streamlines the secure transmission of encrypted Personal Health Records (PHRs) among healthcare providers, thus improving the availability of top-notch medical services in the e-healthcare domain. It effectively handles the hurdles associated with searching encrypted PHRs and guarantees privacy via encryption and access management. This method shows promise in facilitating remote PHR monitoring and research, supported by formal security protocols and performance evaluations.

V. CONCLUSION

In our research, we have developed an innovative proxy re-encryption system with a distinctive feature known as proxy invisibility. This system is designed to Improve the security of data transfer and authorization in electronic healthcare systems. One key aspect of our system is its ability to enable keyword search functionality and facilitate secure delegation among healthcare providers.
With our system, a physician like Alice can securely grant conditional authorization to another physician, such as Bob, by furnishing a re-encryption key, Bob gains access (PHRs) that were initially encrypted using Alice's public key. The cloud server facilitates this access. can perform ciphertext transformation using the provided key, ensuring secure and controlled access.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303281 |

REFERENCES

1. M.Abdalla, M.Bellare, D.Catalano, E.Kiltz, T.Kohno, T.Lange, J.Malone-Lee, G.Neven, P.Paillier, and H.Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer,2005,pp.205–222.
2. G.Ateniese, K.Fu, M.Green, and S.Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans.Inf.Syst.Secur.,vol.9,no.1,pp.1– 30,2006.
3. J.Baek, R.Safavi-Naini, and W.Susilo, "Public key encryption with keyword search revisited,"inProc.Int.Conf.Comput.Sci.Appl.(ICCSA),2008,pp.1249–1259.
4. 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.
5. T.Bhatia, A. K.Verma, and G.Sharma, "Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud," Trans. Emerg. Telecommun. Technol.,vol.29,no.6,p.e3309,Jun.2018.
6. I.F.Blake,G.Seroussi,and N.Smart, "Advances in Elliptic Curve Cryptography(London Mathematical Society Lecture Note Series(317)),vol. 19. Cambridge, U.K.: Cambridge Univ. Press,no.20,2005,p.666.
7. M.Blaze, G.Blumer, and M.Strauss, "Divertible protocols and atomic proxy cryptography," in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer,1998,pp.127–144. [8]D.Boneh, G.D.Crescenzo, R.Ostrovsky, and G.Persiano, "Publickey encryption with keyword search," Proc.Int.Conf.TheoryAppl.Cryptograph.Techn.Berlin, Germany: Springer, 2004,pp.506–522.
8. [9]D.Boneh and B.Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. TheoryCryptogr.Conf.Berlin,Germany:Springer,2007,pp.–554.
9. [10]H.Fang,X.Wang, and L.Hanzo, "Learning-aided physical layer authentication as an intelligent process,"IEEETrans.Commun.,vol.67,no.3,pp. 2260–2273, Mar. 2019.

BIOGRAPHY

Mrs. C Malathi, M. Tech (Ph.D)., is currently working as Assistant Professor in the department of CSE, Annamacharya Institute of Technology and Sciences, Tirupati.

Mr. B Sai Kumar is currently pursuing B. Tech in the stream of Computer Science and Engineering (IoT and Cyber Security including Blockchain Technology) from Annamacharya Institute of Technology and Sciences, Tirupati.

Mr. S Mansoor is currently pursuing B. Tech in the stream of Computer Science and Engineering (IoT and Cyber Security including Blockchain Technology) from Annamacharya Institute of Technology and Sciences, Tirupati.

Mr. S Harshavardhan is currently pursuing B. Tech in the stream of Computer Science and Engineering (IoT and Cyber Security including Blockchain Technology) from Annamacharya Institute of Technology and Sciences, Tirupati.

Ms. D Shravani is currently pursuing B. Tech in the stream of Computer Science and Engineering (IoT and Cyber Security including Blockchain Technology) from Annamacharya Institute of Technology and Sciences, Tirupati.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details