e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707236|

DSAS A Secure Data Sharing and Authorized Searchable Framework for E-Healthcare System

Manohar V N[1], Praveen K S[2]

Student, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[1]

Associate Professor, Department of Master of Computer Applications, East West Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: In e-healthcare system, an increasing number of patients enjoy high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, one of the important issues is that the encrypted PHRs prevent effective search of information, resulting in the decrease of data usage. Another issue is that medical treatment process requires the doctor to be online all the time, which may be unaffordable for all doctors (e.g., to be absent under certain circumstances). In this paper, we design a new secure and practical proxy searchable re-encryption scheme, allowing medical service providers to achieve remote PHRs monitoring and research safely and efficiently. Through our scheme DSAS, (1) patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of PHRs; (2) only authorized doctors or research institutions have access to the PHRs; (3) Alice (doctor-in-charge) is able to delegate medical research and utilization to Bob (doctor-in-agent) or certain research institution through the cloud server, supporting minimizing information exposure to the cloud server. We formalize the security definition and prove the security of our scheme. Finally, performance evaluation shows the efficiency of our scheme

I. INTRODUCTION

In recent years, the digital transformation of healthcare systems has brought about numerous benefits, including enhanced accessibility to medical records and improved patient care. However, ensuring the security and privacy of sensitive health data remains a critical challenge. To address this issue, the Secure Data Sharing and Authorized Searchable (DSAS) framework emerges as a promising solution.

DSAS integrates advanced encryption techniques with efficient search functionalities, enabling healthcare providers to securely share and access patient information as authorized. This framework not only safeguards sensitive data from unauthorized access but also facilitates seamless collaboration among healthcare professionals.

II. LITERATURE SURVEY

Yasnoff proposed a e-healthcare storage framework to eliminate the potential for loss of an entire centralized dataset from a single intrusion while maintaining reasonable search performance. A reliable, searchable and privacy-preserving e-healthcare system was proposed by Yang et al. based on searchable encryption to protect sensitive healthcare files on cloud storage and enable cloud server to search on the encrypted data under the control of patients. Boneh et al., gave the first PEKS construction for e-healthcare system in the public key environment. Later, Abdalla et al. revisited the concept of PEKS and proposed the consistency notion. Baek et al. extended PEKS which removes secure channels between a user and the cloud server, which make the patients communicate with doctors with a secure way.

We propose a proxy-invisible condition-hiding proxy re-encryption scheme with keyword search to address the issues of inefficiency and condition privacy in the e-healthcare system. Encrypting is considered to be a simple and efficient solution to guarantee data confidentiality, but it also makes search over encrypted data extremely difficult. Searchable encryption technology realizes the search operation of encrypted data without decryption, and solves the problem that users cannot control remotely because of data encryption. Hence, searchable is necessary in the e-healthcare system. In this proposed system, we aim to design an efficient, searchable and privacy-preserving e-healthcare system.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707236|

In the proposed system we design a secure data sharing and authorized searchable scheme for e-healthcare system where patients continuously collects PHRs with sensors from physical environments and sends these encrypted PHRs to his doctor-in-charge for seeking for medical treatment. In some case, doctor A wants to share some but not all these PHRs to doctor B. To achieve access authorization, A generates a re-encryption key based on his private key and the public key of B. In order to prevent privacy disclosure, we generate a conditional re-encryption by embedding a trapdoor in the re-encryption key so that the cloud server can only convert cipher text under the designated condition. Moreover, the cloud server is responsible for storing the encrypted data and providing keyword search services and also acts as a proxy to perform re-encryption for data users. When a keyword search request with a trapdoor is received from B, the cloud server performs information retrieval over the encrypted PHRs.

III. SYSTEM DESIGN

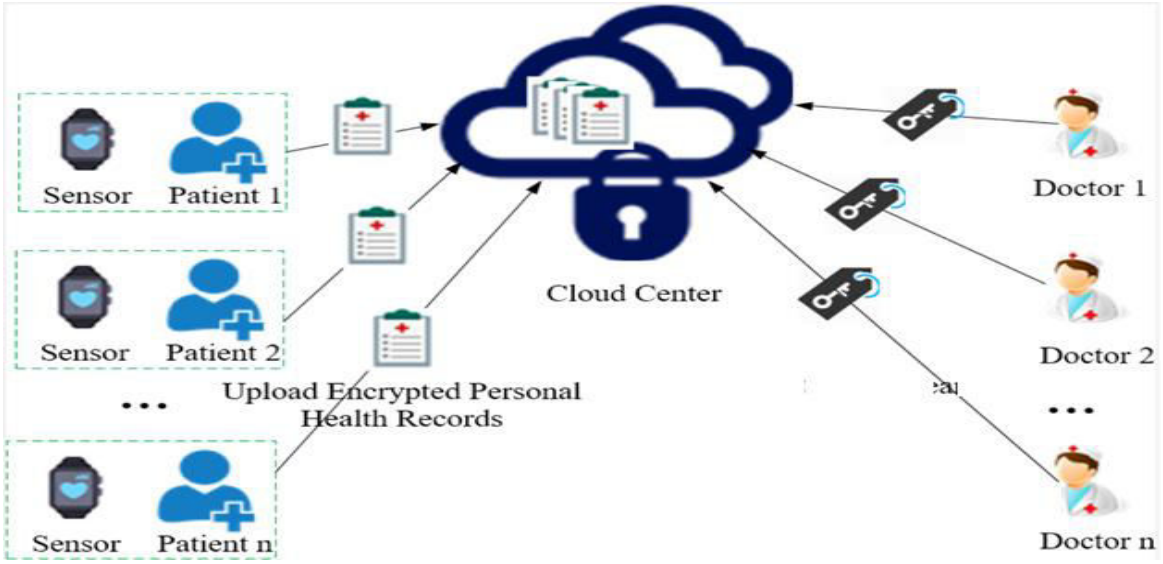

Figure 1: System Architecture

IV. RESULTS AND OUTCOMES

Dataset Collection and Preparation:

- The current implementation of the DSAS system is suitable for small-scale deployments.
- Future work can focus on improving the scalability of the system to support large-scale e-healthcare systems with a high volume of patients and medical records.

Feature Selection and Engineering:

- The DSAS system can be integrated with emerging technologies such as blockchain, AI, and IoT to enhance its functionality and security
- Future research can focus on developing more advanced privacy-preserving techniques to ensure that patient's personal healthcare records are protected even in the case of a breach or attack.

Outcome of the Detection:

- This can involve collaboration with healthcare providers, policymakers, and regulatory bodies to ensure that the system meets legal and ethical requirements and is compatible with existing healthcare systems.
- Future work can focus on developing a user-friendly interface for doctors and patients to access and manage the PHRs, making it easier to use and reducing the risk of human

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707236|

Snapshots:

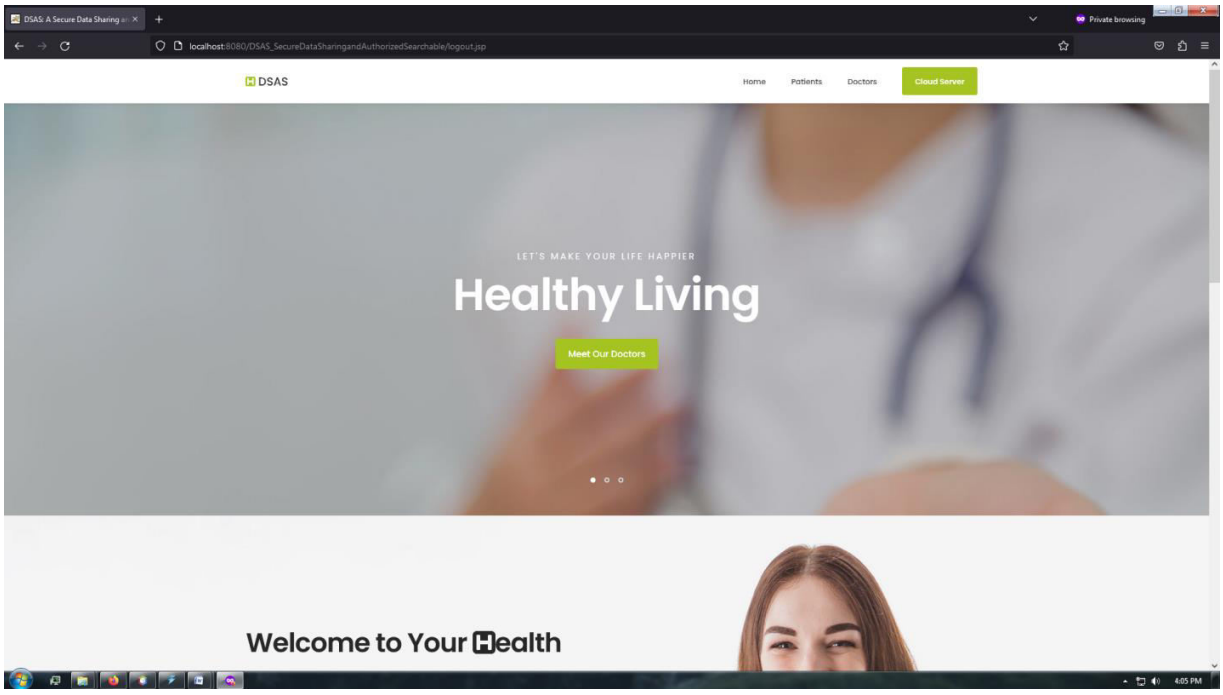

Figure 2: Home Page

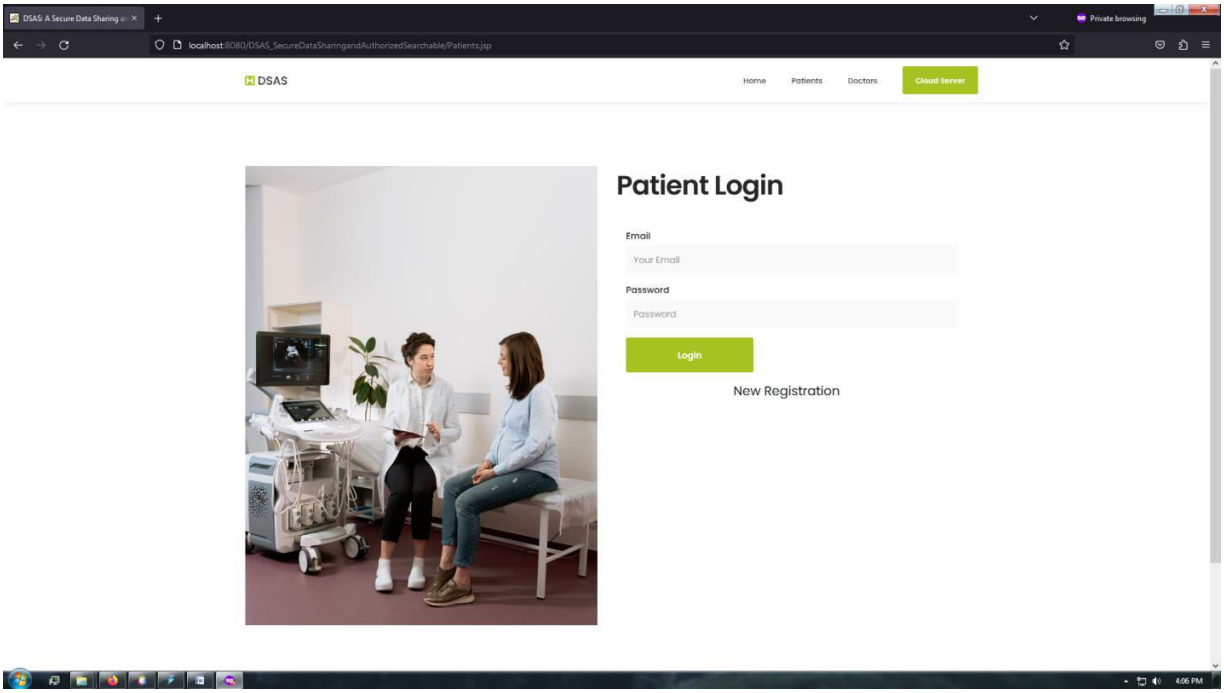

Figure 3: Patient Login

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707236|

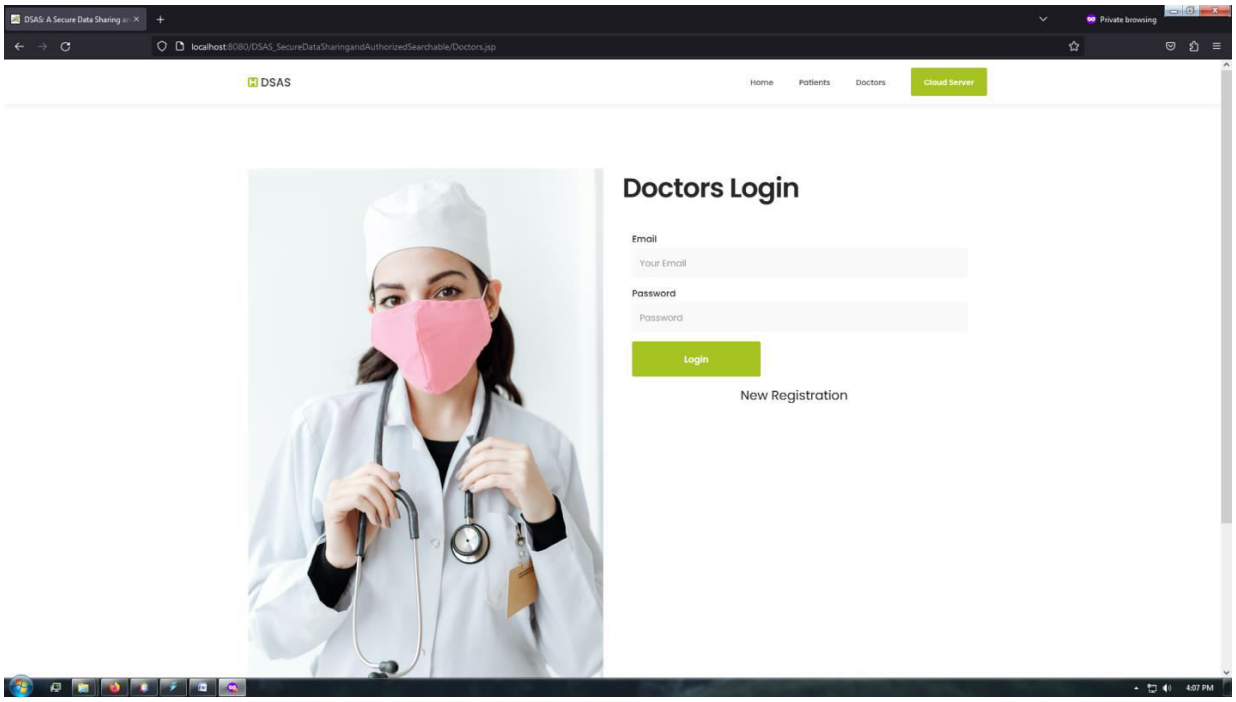

Figure 4: Doctors Login

V. CONCLUSION

In this paper, we presented a proxy-invisible condition-hiding proxy re-encryption scheme which supports keyword search that can be applied to securing data sharing and delegation in e-healthcare systems. With our new system, a doctor, Alice (delegator), may construct a conditional authorization for a doctor, Bob (delegate), by specifying a re-encryption key. With the re-encryption key, the cloud server can perform cipher text transformation so that Bob is able to access the PHRs original encrypted under Alice's public key, thus enabling secure delegation. The cloud server can operate search over encrypted PHRs on behalf of the doctor without learning information about the keyword or the underlying condition. Specifically, we achieved the property of proxy-invisible in the system. We have also obtained the property of collusion-resistance in the system, where a delegator's (Alice) private key is still secure even a dishonest cloud server colludes with the delegate (Bob). We have demonstrated security through a rigorous proof, and the performance analysis confirms that our proposed scheme DSAS is efficient and practical.

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. 205222.
[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. 130, 2006.
[3] J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption with keyword search revisited," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2008, pp. 12491259.
[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 certicateless proxy re-encryption in cloud," Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com