

---

## DSAS-A SECURE DATA SHARING AND AUTHORIZED SEARCHABLE FRAMEWORK FOR E-HEALTHCARE SYSTEM

V Lakshmi Chaitanya<sup>1</sup>, K. Guru Prasad<sup>2</sup>, V. Sai Ganesh<sup>3</sup>, B. Sai Kumar Reddy<sup>4</sup>,  
D. Vasanth Babu<sup>5</sup>, P. Nithin<sup>6</sup>

<sup>1,2,3,4,5,6</sup>Department of Computer Science & Engineering, Santhiram Engineering College, Nandyal-518501,  
AndhraPradesh, India.

Corresponding Author: chaitanya.cse@srecnandyal.edu.in,

DOI: <https://www.doi.org/10.58257/IJPREMS33571>

---

### ABSTRACT

In the domain of e-healthcare, the exchange of encrypted Personal Healthcare Records (PHRs) among patients and medical professionals has greatly enhanced access to high-quality medical services. Nonetheless, a notable challenge persists in efficiently searching for information within encrypted PHRs, alongside the cost implications linked to ensuring continuous online availability of doctors for remote monitoring and research purposes. This study introduces a novel and secure Proxy Searchable Re-Encryption method, known as DSAS, with the aim of facilitating effective and secure remote PHR monitoring and research.

DSAS prioritizes the privacy and confidentiality of PHRs by restricting access solely to authorized doctors and research institutions. Furthermore, it enables the delegation of medical decisions by the primary healthcare provider, ensuring that patient records undergo encryption before being uploaded to a cloud server. This approach facilitates remote access for secondary healthcare providers or research institutions, thereby limiting direct access to sensitive information stored on the cloud server. The security of the proposed scheme is rigorously formalized, and performance analysis confirms its effectiveness.

---

### 1. INTRODUCTION

A mobile platform integrated with an e-healthcare sensor network has proven to be invaluable for individuals seeking effective and high-quality medical care. These sensor devices, embedded within patients' gadgets, gather a wealth of personal healthcare information, allowing healthcare providers to make more accurate diagnoses and tailor treatments to address patients' specific needs. Additionally, analysts and researchers in the field of medicine can leverage this data to conduct comprehensive analytics, gaining deeper insights into diseases and developing more effective remedies.

However, storing such sensitive data in third-party cloud storage introduces security risks, including the potential for data leaks. This risk arises because neither patients nor medical professionals have direct access to the information when it is stored externally. For example, some healthcare facilities store vast amounts of Personal Healthcare Records (PHRs) on cloud servers and grant organizations like the Centers for Disease Control and Prevention (CDC) permission to utilize them. To mitigate the risk of data leaks, it is essential to encrypt all PHRs before storing them in the cloud.

While encryption provides robust data security and addresses privacy concerns, it also presents challenges in terms of user experience. Standard encryption algorithms, which rely on plaintext, can hinder the retrieval of encrypted data, making it difficult to query such information. To overcome these limitations, researchers have turned to searchable encryption (SE) cryptosystems. In the context of e-healthcare systems, patients use searchable encryption technology to encrypt prospective keywords as indices before uploading them to the cloud server alongside encrypted PHRs. Authorized healthcare providers or research institutions can then use an encrypted keyword search by transmitting a trapdoor generated with a specific term to the cloud server.

In summary, leveraging searchable encryption technology in e-healthcare systems allows for secure storage and retrieval of sensitive medical data while addressing privacy concerns and mitigating the risk of data leaks. This approach ensures that authorized users can access relevant information without compromising the confidentiality of patient records stored in the cloud.

### 2. EXISTING SYSTEM

In the existing system, blockchain technology serves as a secure and decentralized solution for storing and sharing patient health information. It empowers patients to have greater control over access to their data and guarantees that every transaction is securely recorded on an immutable ledger.

---

**Disadvantages of the existing system:**

1. Complexity: Developing and implementing a secure e-Healthcare data sharing and searchable framework can be complex and resource-intensive.
2. Privacy Risks: Despite security measures, there's a persistent risk of breaches or unauthorized access to sensitive patient data.
3. Technical Challenges: Creating a system allowing authorized searches while maintaining data security and privacy presents technical complexities.
4. Regulatory Compliance: Meeting strict regulations like HIPAA poses a challenge for ensuring framework compliance.
5. Usability Issues: Complex security measures may hinder system usability, impacting healthcare professionals' workflow.

**3. PROPOSED SYSTEM**

In the proposed system, establishing a robust authorization and authentication mechanism is crucial for safeguarding the security and privacy of patient data. This mechanism acts as the foundation of the system, determining who has access to sensitive medical information and under what circumstances. By implementing stringent authentication protocols, the proposed system aims to mitigate the risk of unauthorized access and uphold patient confidentiality.

Various authentication methods can be employed to achieve this objective, including password-based authentication, two-factor authentication (2FA), and biometric authentication. Password-based authentication involves users providing a unique combination of characters or phrases to verify their identity. While widely used, this method may be vulnerable to security risks like password guessing or brute force attacks if not properly managed.

Two-factor authentication adds an extra layer of security by requiring users to provide two forms of identification before granting access. This could entail combining something the user knows (e.g., a password) with something they have (e.g., a mobile device for receiving a verification code). By necessitating multiple forms of verification, 2FA significantly enhances system security and reduces the risk of unauthorized access.

Biometric authentication utilizes unique physical or behavioral characteristics of individuals, such as fingerprints, iris patterns, or facial recognition, to verify identity. Offering high levels of security and convenience, this method eliminates the need for users to remember passwords or carry additional devices. However, biometric authentication may raise privacy concerns regarding the storage and processing of biometric data.

In addition to authentication, the proposed system must incorporate a robust authorization mechanism to define and enforce access control policies. Access control policies specify which users or user groups are permitted to access specific resources within the system and what actions they can undertake. Role-based access control (RBAC) is a widely used authorization model that assigns roles to users based on their responsibilities and privileges, allowing for precise control over access permissions.

By integrating these authentication and authorization mechanisms into the proposed system, healthcare providers can ensure that only authorized individuals, such as medical professionals or patients themselves, can access patient data. This not only safeguards patient privacy and confidentiality but also fosters trust among stakeholders and facilitates compliance with data protection regulations.

**4. WORKING PRINCIPLE**

DSAS, a secure data sharing framework tailored for e-healthcare, employs encryption to secure patient records prior to their transfer to a protected cloud server. This encryption ensures that sensitive medical information remains confidential during storage and transmission. Authorized users can conduct searches on encrypted data using specialized techniques that maintain privacy. The system is equipped with robust access controls to restrict data access to authorized personnel only. Additionally, it incorporates audit trails to track data access and modifications, enhancing accountability. Continuous monitoring for security updates further strengthens the system's resilience against potential threats and vulnerabilities.

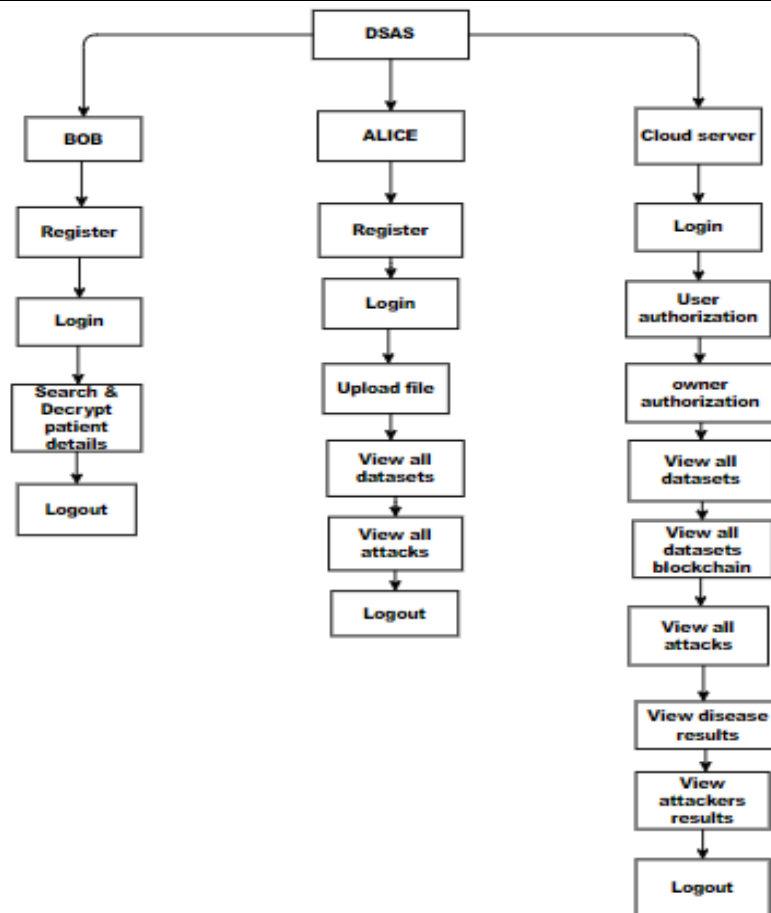


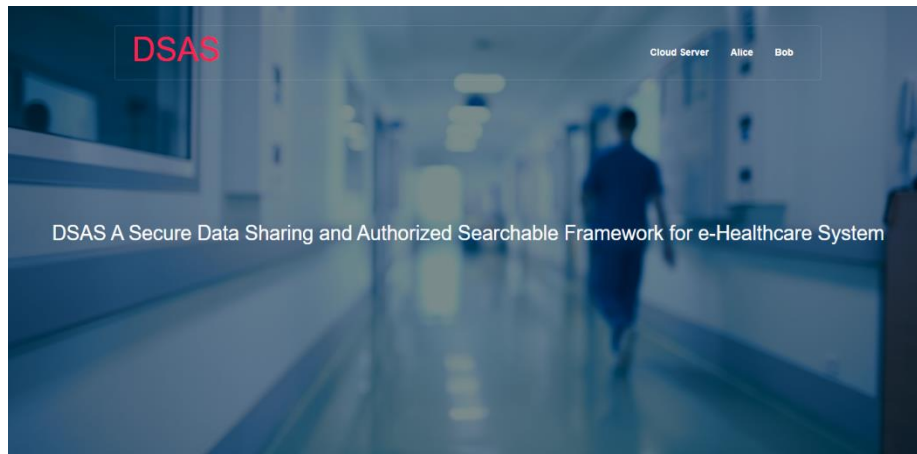
Fig 1: Project flow

#### Advantages of the Proposed System:

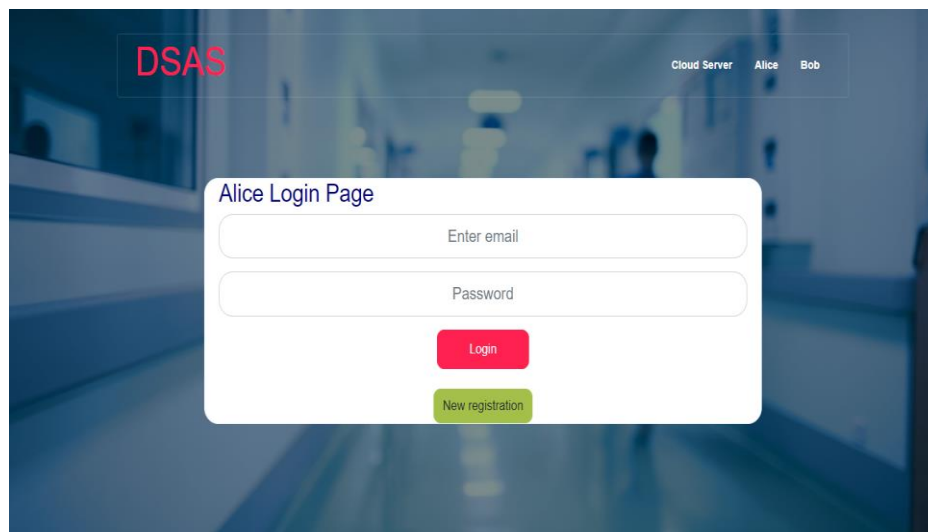
1. Enhanced Security: The system's robust authorization and authentication mechanisms bolster security by restricting access to authorized individuals, thereby minimizing the risk of unauthorized access and data breaches.
2. Improved Patient Privacy: Stringent authentication protocols ensure patient privacy and confidentiality by permitting access only to authorized healthcare professionals or individuals with legitimate reasons for access, thereby safeguarding sensitive medical information.
3. Reduced Risk of Data Breaches: The implementation of multi-factor authentication adds an additional layer of security, decreasing the likelihood of data breaches even if one authentication factor is compromised.
4. Compliance with Regulations: The system aids healthcare providers in adhering to regulations such as HIPAA by limiting access to authorized users, thereby avoiding potential penalties and legal repercussions.
5. Enhanced Accountability: Through authentication and authorization mechanisms, the system enables effective monitoring of user access, fostering accountability and transparency within the system.
6. Flexible Authentication Options: The system offers flexibility in authentication methods, accommodating various security requirements and user preferences to ensure a seamless user experience.
7. Improved User Experience: With intuitive authentication processes and user-friendly interfaces, the system prioritizes a seamless user experience, enhancing usability and accessibility for healthcare professionals and authorized users.
8. Mitigation of Insider Threats: Authentication and authorization mechanisms mitigate insider threats by restricting access based on predefined roles and permissions, thereby minimizing the risk of unauthorized access or misuse of sensitive information.
9. Protection Against Credential Theft: Multi-factor authentication provides protection against credential theft, making it challenging for attackers to gain unauthorized access to the system and patient data.
10. Scalability and Adaptability: Designed to scale and adapt to evolving security threats and technological advancements, the system accommodates changes to authentication mechanisms and access control policies, ensuring long-term effectiveness and resilience.

## 5. RESULTS

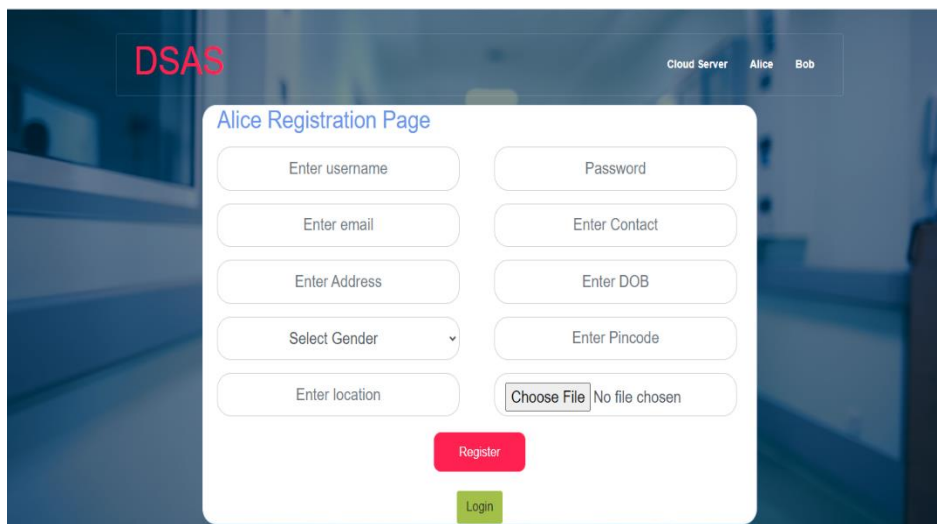
The DSAS framework guarantees heightened data security and patient privacy within e-healthcare systems through the deployment of robust encryption, authentication, and access control measures. It facilitates seamless data sharing, permits authorized searches on encrypted data, and ensures adherence to regulatory standards. DSAS fosters accountability, usability, and transparency, effectively mitigating insider threats and fostering trust among stakeholders. Moreover, its scalability and adaptability enable it to keep pace with evolving security requirements and technological advancements.



**Fig:2** A Secure Data Sharing and Authorized Searchable Framework for e-Healthcare System home page.



**Fig : 3** Alice login page



**Fig: 4** Alice registration page

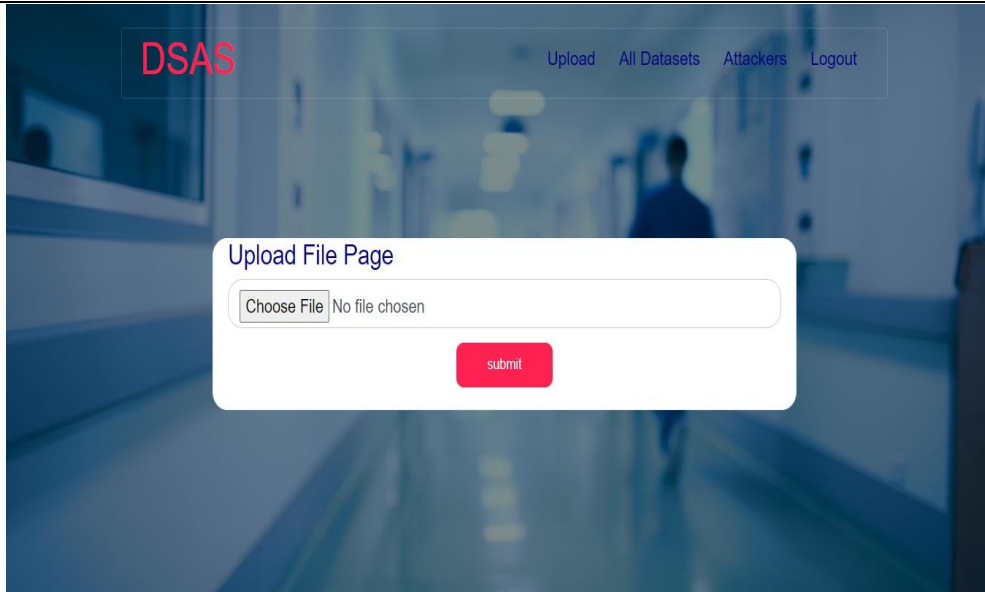
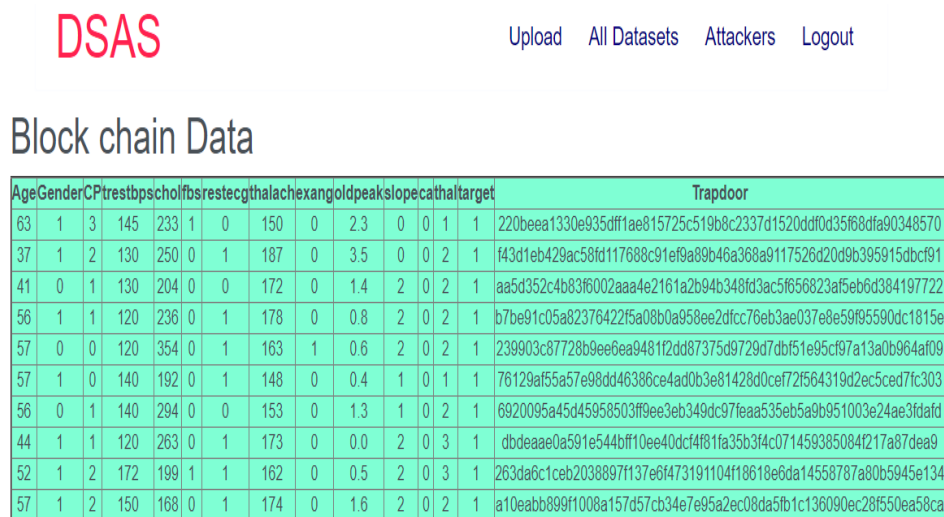


Fig :5 Upload file



Age	Gender	CP	rest	bps	chol	fbs	restecg	thal	achex	ang	old	peak	slope	ca	thal	target	Trapdoor
63	1	3	145	233	1	0	150	0	2.3	0	0	1	1	220	bee	1330e935dff1ae815725c519b8c2337d1520ddf0d35f68dfa90348570	
37	1	2	130	250	0	1	187	0	3.5	0	0	2	1	f43d1eb429ac58fd117688c91ef9a89b46a368a9117526d20d9b395915dbcf91			
41	0	1	130	204	0	0	172	0	1.4	2	0	2	1	aa5d352c4b83f6002aaa4e2161a2b94b348fd3ac5f656823af5eb6d384197722			
56	1	1	120	236	0	1	178	0	0.8	2	0	2	1	b7be91c05a82376422f5a00b0a958ee2dfcc76eb3ae037e8e59f95590dc1815e			
57	0	0	120	354	0	1	163	1	0.6	2	0	2	1	239903c87728b9ee6ea9481f2dd87375d9729d7dbf51e95cf97a13a0b964af09			
57	1	0	140	192	0	1	148	0	0.4	1	0	1	1	76129af55a57e98dd46386ce4ad0b3e81428d0cef72f564319d2ec5ced7fc303			
56	0	1	140	294	0	0	153	0	1.3	1	0	2	1	6920095a45d45958503ff9ee3eb349dc97feaa535eb5a9b951003e24ae3fdafd			
44	1	1	120	263	0	1	173	0	0.0	2	0	3	1	dbdeaae0a591e544bf10ee40dc4f81fa35b3f4c071459385084f217a87dea9			
52	1	2	172	199	1	1	162	0	0.5	2	0	3	1	263da6c1ceb2038897f137e6f473191104f18618e6da14558787a80b5945e134			
57	1	2	150	168	0	1	174	0	1.6	2	0	2	1	a10eabb899f1008a157d57cb34e7e95a2ec08da5fb1c136090ec28f550ea58ca			

Fig:6 All data set

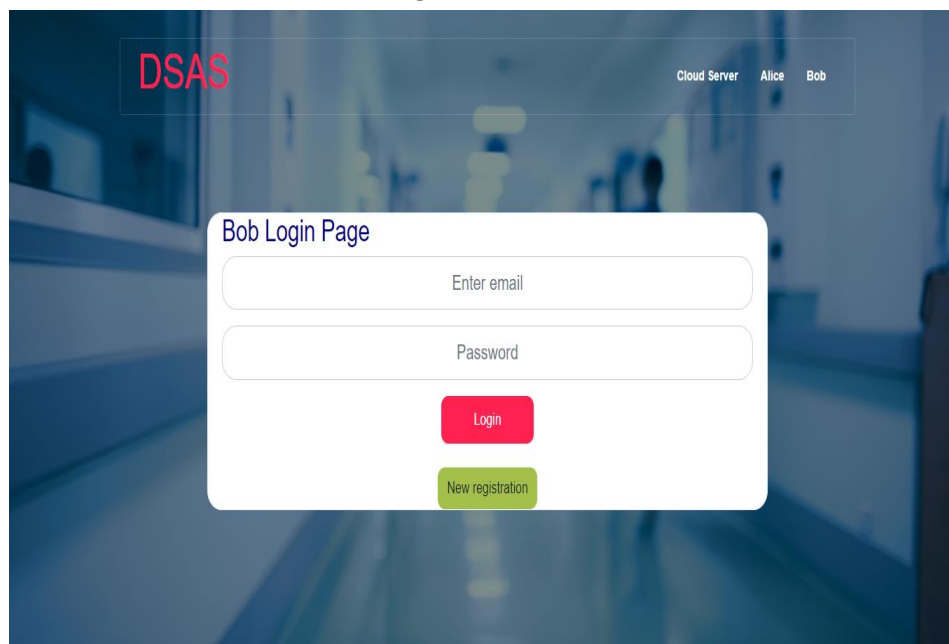


Fig:7 Bob login page

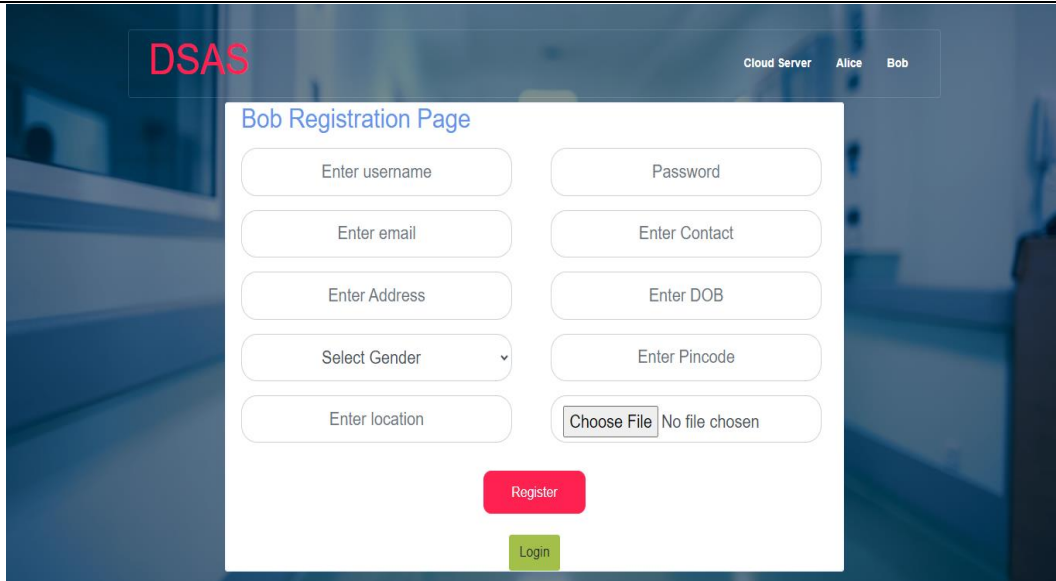


Fig: 8 Bob registration page

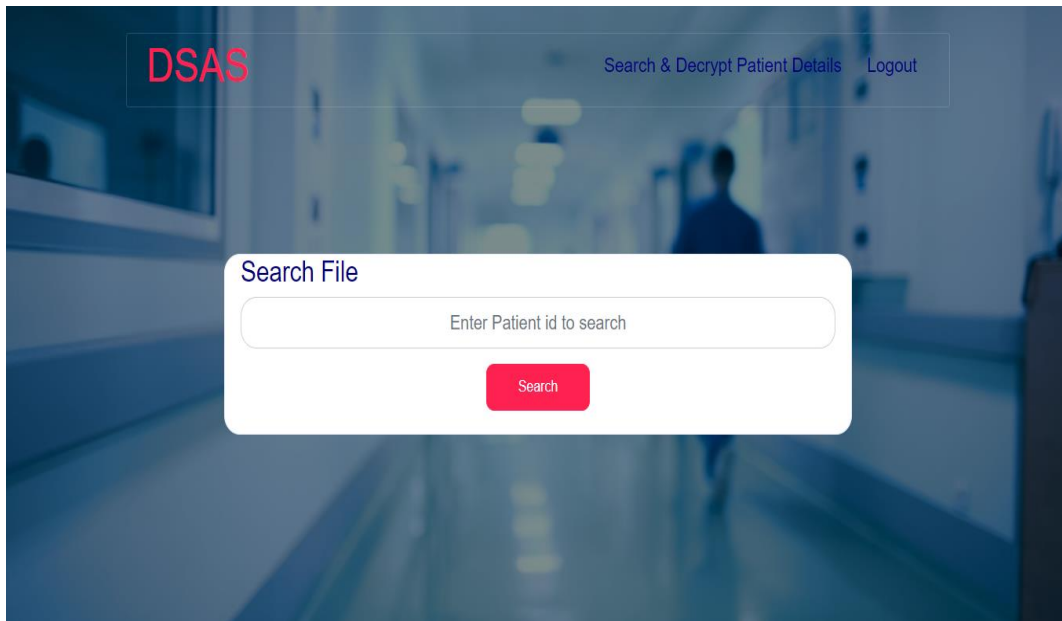
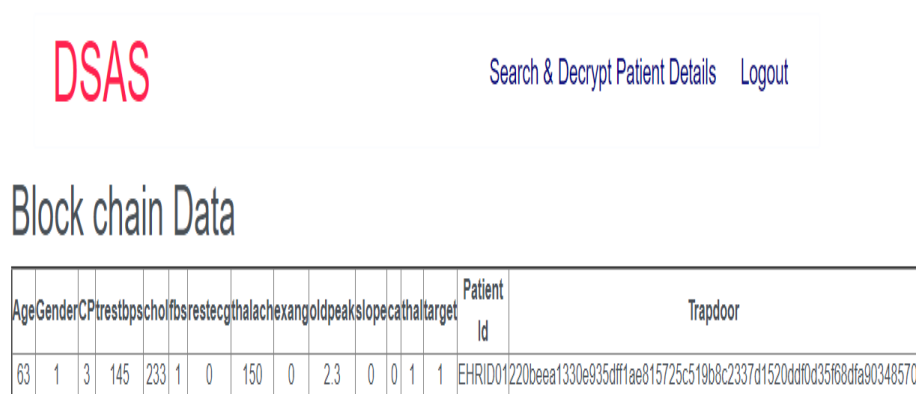


Fig:9 Search and decrypt patient details



Age	Gender	CP	rest	bps	chol	fb	rest	cg	thal	ach	xang	ld	peak	slope	ca	thal	target	Patient Id	Trapdoor
63	1	3	145	233	1	0	150	0	2.3	0	0	1	1	EHRID01220beea1330e935dff1ae815725c519b8c2337d1520ddf0d35f68dfa90348570					

Fig:10 View result

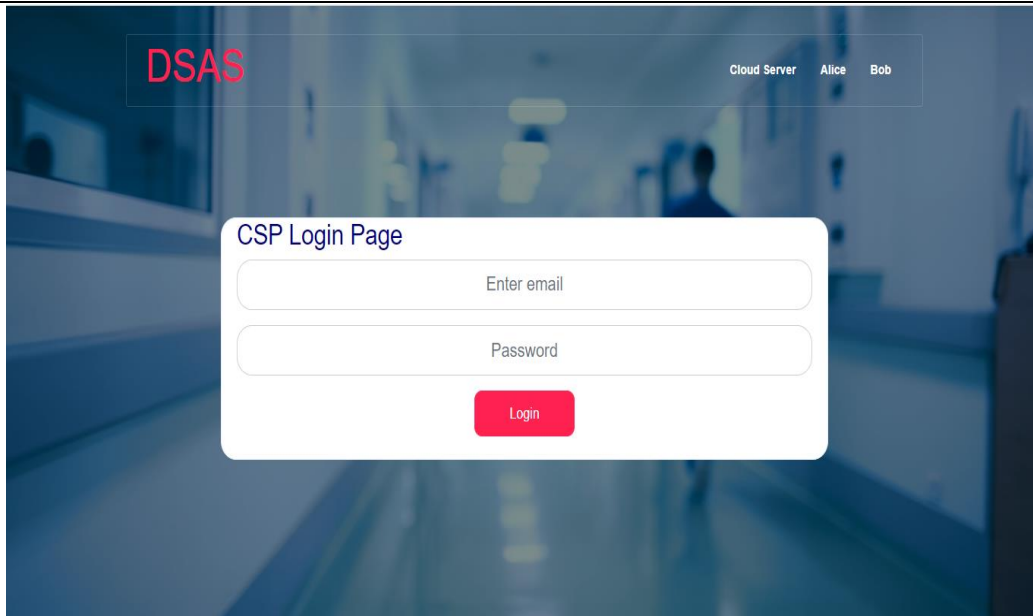


Fig:11 Cloud login page

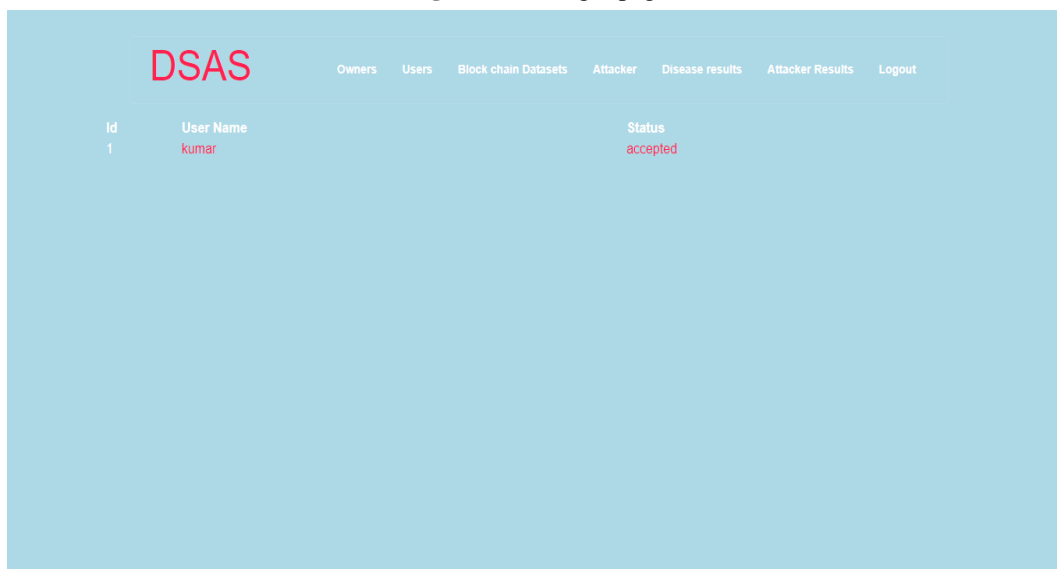


Fig: 12 Owner request

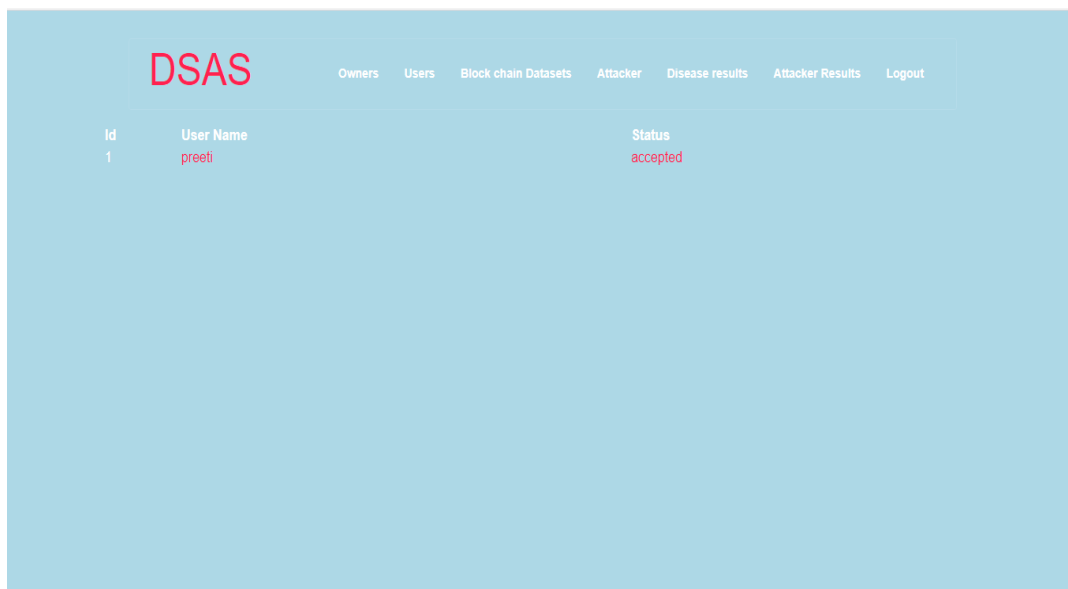


Fig:13 User request

## 6. CONCLUSION

The proxy-invisible condition-hiding proxy re-encryption system we developed in this work allows keyword search and may be used to secure data exchange and delegation in systems for e-healthcare. With our new system, a physician named Alice (the delegator) can create a conditional authorisation for a physician named Bob (the delegate) by providing a re-encryption key. Bob may now access the PHRs that were originally encrypted using Alice's public key thanks to the cloud server's ability to perform ciphertext transformation using the re-encryption key, enabling secure delegation. The cloud server may conduct searches on encrypted PHRs on the doctor's behalf without understanding the term or the underlying circumstance. We specifically accomplished the system's proxy-invisible characteristic. Also, we have discovered the system's collusion-resistance characteristic, which ensures that even if a dishonest cloud server colludes with the delegate, Alice's private key will remain safe (Bob). Our suggested system, DSAS, has been proven secure by a thorough proof, and performance analysis supports its effectiveness.

## 7. 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," in Proc. 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] Mahammad, F. S., & Viswanatham, V. M. (2020). Performance analysis of data compression algorithms for heterogeneous architecture through parallel approach. The Journal of Supercomputing, 76(4), 2275-2288.
- [8] Karukula, N. R., & Farooq, S. M. (2013). A route map for detecting Sybil attacks in urban vehicular networks. Journal of Information, Knowledge, and Research in Computer Engineering, 2(2), 540-544.
- [9] Farook, S. M., & NageswaraReddy, K. (2015). Implementation of Intrusion Detection Systems for High Performance Computing Environment Applications. International journal of Scientific Engineering and Technology Research, 4(0), 41.
- [10] Sunar, M. F., & Viswanatham, V. M. (2018). A fast approach to encrypt and decrypt of video streams for secure channel transmission. World Review of Science, Technology and Sustainable Development, 14(1), 11-28.
- [11] Mahammad, F. S., & Viswanatham, V. M. (2017). A study on h. 26x family of video streaming compression techniques. International Journal of Pure and Applied Mathematics, 117(10), 63-66.
- [12] Devi, S. M. S., Mahammad, F. S., Bhavana, D., Sukanya, D., Thanusha, T. S., Chandrakala, M., & Swathi, P. V. (2022). "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise Against Covid-19 Infection." Journal of Algebraic Statistics, 13(3), 112-117.
- [13] Devi, M. M. S., & Gangadhar, M. Y. (2012). "A comparative Study of Classification Algorithm for Printed Telugu Character Recognition." International Journal of Electronics Communication and Computer Engineering, 3(3), 633-641.
- [14] Devi, M. S., Meghana, A. I., Susmitha, M., Mounika, G., Vineela, G., & Padmavathi, M. MISSING CHILD IDENTIFICATION SYSTEM USING DEEP LEARNING.
- [15] V. Lakshmi chaitanya. "Machine Learning Based Predictive Model for Data Fusion Based Intruder Alert System." journal of algebraic statistics 13, no. 2 (2022): 2477-2483.
- [16] Chaitanya, V. L., & Bhaskar, G. V. (2014). Apriori vs Genetic algorithms for Identifying Frequent Item Sets. International journal of Innovative Research & Development, 3(6), 249-254.
- [17] Chaitanya, V. L., Sutraye, N., Praveena, A. S., Niharika, U. N., Ulfath, P., & Rani, D. P. (2023). Experimental



- Investigation of Machine Learning Techniques for Predicting Software Quality.
- [18] Lakshmi, B. S., Pranavi, S., Jayalakshmi, C., Gayatri, K., Sireesha, M., & Akhila, A. Detecting Android Malware with an Enhanced Genetic Algorithm for Feature Selection and Machine Learning.
- [19] Lakshmi, B. S., & Kumar, A. S. (2018). Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity checking in Public Cloud. *International Journal of Research*, 5(22), 744-757.
- [20] Lakshmi, B. S. (2021). Fire detection using Image processing. *Asian Journal of Computer Science and Technology*, 10(2), 14-19.
- [21] Devi, M. S., Poojitha, M., Sucharitha, R., Keerthi, K., Manideepika, P., & Vasudha, C. Extracting and Analyzing Features in Natural Language Processing for Deep Learning with English Language.
- [22] Kumar JDS, Subramanyam MV, Kumar APS. Hybrid Chameleon Search and Remora Optimization Algorithm-based Dynamic Heterogeneous load balancing clustering protocol for extending the lifetime of wireless sensor networks. *Int J Commun Syst*. 2023; 36(17):e5609. doi:10.1002/dac.5609
- [23] David Sukeerthi Kumar, J., Subramanyam, M.V., Siva Kumar, A.P. (2023). A Hybrid Spotted Hyena and Whale Optimization Algorithm-Based Load-Balanced Clustering Technique in WSNs. In: Mahapatra, R.P., Peddoju, S.K., Roy, S., Parwekar, P. (eds) *Proceedings of International Conference on Recent Trends in Computing. Lecture Notes in Networks and Systems*, vol 600. Springer, Singapore. [https://doi.org/10.1007/978-981-19-8825-7\\_68](https://doi.org/10.1007/978-981-19-8825-7_68)
- [24] Murali Kanthi, J. David Sukeerthi Kumar, K. Venkateshwara Rao, Mohamad Ahmed Ali, Sudha Pavani K, Nuthanakanti Bhaskar, T. Hitendra Sarma, "A FUSED 3D-2D CONVOLUTION NEURAL NETWORK FOR SPATIAL-SPECTRAL FEATURE LEARNING AND HYPERSPECTRAL IMAGE CLASSIFICATION," *J Theor Appl Inf Technol*, vol. 15, no. 5, 2024, Accessed: Apr. 03, 2024. [Online]. Available: [www.jatit.org](http://www.jatit.org)
- [25] Prediction Of Covid-19 Infection Based on Lifestyle Habits Employing Random Forest Algorithm FS Mahammad, P Bhaskar, A Prudvi, NY Reddy, PJ Reddy *journal of algebraic statistics* 13 (3), 40-45
- [26] Machine Learning Based Predictive Model for Closed Loop Air Filtering System P Bhaskar, FS Mahammad, AH Kumar, DR Kumar, SMA Khadar, ...*Journal of Algebraic Statistics* 13 (3), 609-616
- [27] Kumar, M. A., Mahammad, F. S., Dhanush, M. N., Rahul, D. P., Sreedhara, K. L., Rabi, B. A., & Reddy, A. K. (2022). Traffic Length Data Based Signal Timing Calculation for Road Traffic Signals Employing Proportionality Machine Learning. *Journal of Algebraic Statistics*, 13(3), 25-32.
- [28] Kumar, M. A., Pullama, K. B., & Reddy, B. S. V. M. (2013). Energy Efficient Routing In Wireless Sensor Networks. *International Journal of Emerging Technology and Advanced Engineering*, 9(9), 172-176.
- [29] Kumar, M. M. A., Sivaraman, G., Charan Sai, P., Dinesh, T., Vivekananda, S. S., Rakesh, G., & Peer, S. D. BUILDING SEARCH ENGINE USING MACHINE LEARNING TECHNIQUES.
- [30] " Providing Security in IOT using Watermarking and Partial Encryption. ISSN No: 2250-1797 Issue 1, Volume 2 (December 2011)
- [31] The Dissemination Architecture of Streaming Media Information on Integrated CDN and P2P, ISSN 2249-6149 Issue 2, Vol.2 ( March-2012)
- [32] Provably Secure and Blind sort of Biometric Authentication Protocol using Kerberos, ISSN: 2249-9954, Issue 2, Vol 2 (APRIL 2012)
- [33] D.Lakshmaiah, Dr.M.Subramanyam, Dr.K.Satya Prasad," Design Of Low Power 4- Bit Cmos Braun Multiplier Based On Threshold Voltage Techniques", *Global Journal Of Research In Engineering*, Vol.14(9),Pp.1125-1131,2014.
- [34] R Sumalatha, Dr.M.Subramanyam, "Image Denoising Using Spatial Adaptive Mask Filter", *Ieee International Conference On Electrical, Electronics, Signals, Communication & Optimization (Eesco-2015)*, Organized Byvignans Institute Of Information Technology, Vishakapatnam, 24 Th To 26th January 2015. (Scopus Indexed)
- [35] P.Balamurali Krishna, Dr.M.V.Subramanyam, Dr.K.Satya Prasad, "Hybrid Genetic Optimization To Mitigate Starvation In Wireless Mesh Networks", *Indian Journal Of Science And Technology*,Vol.8,No.23,2015. (Scopus Indexed)
- [36] Y.Murali Mohan Babu, Dr.M.V.Subramanyam,M.N. Giri Prasad," Fusion And Texure Based Classification Of Indian Microwave Data – A Comparative Study", *International Journal Of Applied Engineering Research*, Vol.10 No.1, Pp. 1003-1009, 2015. (Scopus Indexed)