IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.03

Privacy Preserving Health Care Data Sharing with Data Mining

Bandari Ravi
Assistant Professor, Department of Computer Science & Engineering,
Guru Nanak Institute of Technology, Hyderabad, India
raviyadav.bandaru@gmail.com
https://orcid.org/0009-0002-6598-2001
Pettam Akshara, Yellanki Rohithvas, S Krishna
Students, Department of Computer Science & Engineering,
Guru Nanak Institute of Technology, Hyderabad, India
aksharapettam@gmail.com, rohithvas262004@gmail.com , krishnayadavs947128@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10082
Research Article | Open Access | Double-Blind Peer-Reviewed| ArticleID: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10182
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijirae.com/volumes/Vol13/iss-04/03.AEAP26.APAE10082.pdf
Article Citation:Bandari,Pettam,Yellanki,Krishna(2026),Privacy Preserving Health Care Data Sharing With Data Mining, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 04 of 2026 pages 742-750 **Doi:>** https://doi.org/10.26562/ijirae.2026.v1304.03 **BibTeX Key:Bandari@2026Privacy**
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2026, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1304.03 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: The growing importance of data in healthcare has heightened the need for privacy-preserving data sharing, particularly in systems where health records are distributed across a database. Despite widespread recognition of the benefits of data sharing for both research and patient care, concerns about privacy and security remain a major barrier. This study explores current attitudes toward data sharing healthcare professionals across clinical and non-clinical roles. By combining descriptive statistics and data mining techniques, we assessed trust in existing privacy-preserving tools such as data anonymization, encryption, and access control mechanisms, and evaluated openness to adopting proposed advanced solutions, including differential privacy, and secure multi-party. Findings reveal a cautious with many professionals showing readiness, primarily motivated by the potential to improve patient outcomes rather than purely research interests. These insights contribute to the development of targeted policies and innovative frameworks aimed at Enabling secure, privacy-conscious data sharing in the healthcare sector.

Keywords: Privacy-Preserving Data Sharing, Healthcare Data Privacy, Data Anonymization, Differential Privacy, Secure Multi-Party Computation, Data Security in Healthcare

I.INTRODUCTION

The rapid digital transformation of the healthcare sector has led to an exponential increase in the generation and storage of medical data across distributed environments such as hospitals, clinics, and research institutions. While the efficient sharing of healthcare data plays a crucial role in improving patient care, enabling advanced research, and supporting data-driven decision-making, it also raises significant concerns regarding data privacy, security, and unauthorized access. This paper focuses on designing and developing a robust healthcare data sharing system that integrates advanced privacy-preserving techniques such as data anonymization and homomorphic encryption. These techniques enable secure data processing and analysis without revealing the original sensitive information. Additionally, the system incorporates role-based access control to regulate user permissions and ensure that only authorized individuals can access specific data. Audit and logging mechanisms further enhance system transparency and accountability by monitoring user activities. By enabling secure data mining on protected healthcare data, the proposed system aims to extract meaningful insights that can improve healthcare services, support medical research, and enhance patient outcomes, all while adhering to strict privacy and security standards.

II. LITERATURE SURVEY

S.Xu et al. (2024) This paper proposes a privacy-preserving and redactable healthcare blockchain system (PRHBS) to address challenges related to data immutability and regulatory requirements such as the "right to be forgotten" under GDPR. The system enables controlled data redaction while maintaining blockchain integrity. It integrates advanced cryptographic techniques including chameleon hash functions, attribute-based encryption, and puncturable encryption to ensure data confidentiality and flexible key distribution [1]. The proposed model provides fine-grained data control and secure sharing in multi-user environments. Experimental results show that the system achieves comparable performance while offering enhanced functionality over existing solutions.

L.Liu et al. (2024) This study presents a comprehensive survey and research framework for privacy-preserving and secure industrial big data analytics (IBDA). It highlights challenges arising from multisource, heterogeneous, and untrusted data environments in the Industrial Internet [2]. The paper proposes a layered architecture including functional, security, and system models to support secure data analytics.

It also identifies key research areas such as data fusion, privacy protection, and blockchain integration. The framework provides guidance for developing efficient and secure big data analytics systems in industrial applications.

R.Canaway et al. (2024) This paper examines the use of primary healthcare electronic records for research and identifies barriers to effective data utilization. It highlights issues such as privacy concerns, legal and ethical challenges, lack of trust, and insufficient incentives for data sharing among healthcare providers [3]. The study emphasizes the importance of transparency, strong governance frameworks, and secure data handling mechanisms. It suggests that addressing these challenges can enable better use of healthcare data for research, improve patient care, and support population health studies.

III. EXISTING SYSTEM

Data Anonymization and De-identification: One of the most commonly used methods, anonymization involves removing personally identifiable information (PII) from database [4,5]. This reduces the risk of re-identification but often comes at the cost of data utility. Furthermore, advanced data reconstruction techniques have demonstrated that anonymized data can sometimes still be re-identified, especially when combined with other database. These systems track access to data and help in accountability. They deter misuse but are reactive rather than preventive measures.

Existing System Disadvantages:

- RBAC struggles with handling exceptions and special cases. ϖ RBAC is its lack of context awareness.
- Lacks integration between coding and non-coding region analysis, requiring multiple tools for complete genomic studies.

PROPOSED SYSTEM

The proposed system provides a secure and privacy-preserving healthcare data sharing framework that enables safe exchange of medical data across different healthcare entitie[6,7]s. It uses data anonymization to protect patient identity and advanced encryption techniques such as homomorphic encryption to perform computations on encrypted data without revealing sensitive information. The system also implements role-based access control to ensure that only authorized users can access specific data. Additionally, audit and logging mechanisms are included to track system activities and maintain security. Overall, the system improves data privacy and addresses the limitations of existing healthcare systems.

Proposed System Advantages:

- Ensures data privacy using anonymization and encryption.
- Provides secure data sharing with controlled access.
- Uses Advanced Homomorphic encryption for data privacy.

IV. SYSTEM ARCHITECTURE

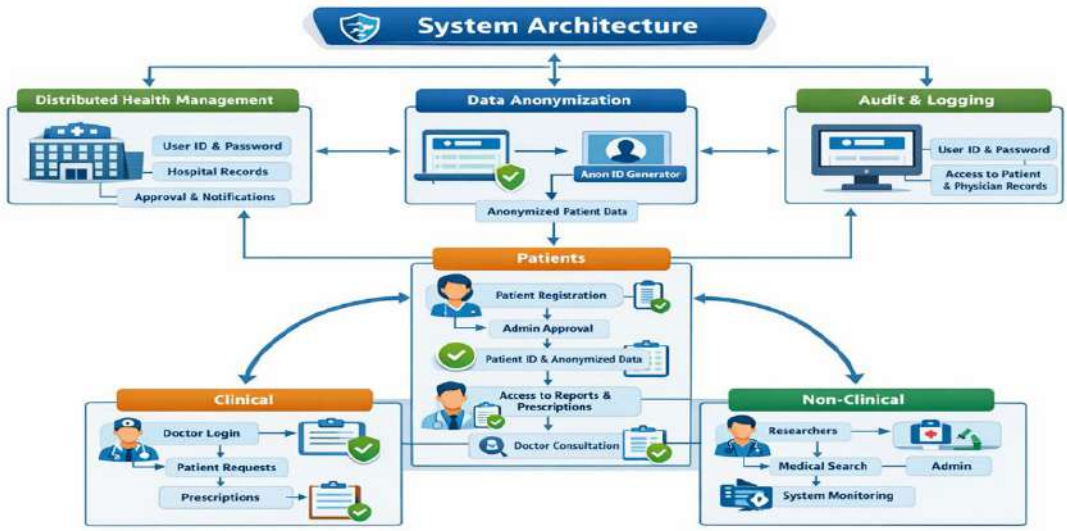

Fig 1: System Architecture

The system architecture defines the overall structure of the healthcare system by showing its main components and their interactions. It includes modules such as Distributed Health Management, Data Anonymization, Audit & Logging, Patient Management, and Role Management, each handling specific functions like data access, privacy, and user control[8]. The system follows a layered approach where users interact through a secure interface, business logic processes requests, and the data layer manages records. This architecture ensures security, scalability, and efficient data sharing.

Methodology

Modules Name:

- Distributed Health Management
- Data Anonymization
- Audit & Logging Module
- Patients
- Role Management

1. Distributed Health Management: This module manages secure access to distributed hospital data using user authentication. Hospitals register with required details and obtain approval before accessing the system.

It enables secure sharing of healthcare information across multiple locations while maintaining data privacy. The module also supports communication through distributed health notices, improving coordination among healthcare institutions.

2. Data Anonymization: This module protects patient privacy by transforming sensitive information into anonymized data. A unique patient ID is generated to replace personal details such as name and contact information. Only authorized users can access this system through secure login. It ensures safe data usage for analysis and research while maintaining confidentiality and compliance with regulations.

3. Audit & Logging Module: This module tracks all system activities to ensure transparency and security. It records actions such as data access, updates, and downloads along with timestamps and user details. Only authorized auditors can access these logs. This helps detect unauthorized activities, supports compliance, and maintains accountability across the system.

4. Patients: This module handles patient registration, authorization, and interaction with healthcare services. After admin approval, a unique patient ID is generated and data is anonymized. Patients can upload and access medical reports, receive prescriptions from doctors, and download them securely. It ensures privacy, secure communication, and efficient healthcare service delivery.

5. Role Management: This module manages access and responsibilities of different users in the system.

- **Clinical (Doctor):** Doctors register, get hospital approval, and log in securely. They review patient reports, provide diagnosis, and issue prescriptions. This ensures proper treatment and secure communication between doctor and patient.
- **Non-Clinical (Researchers & Admin):**
  - **Researchers:** Access anonymized data to analyse medical information, study treatments, and evaluate medication effectiveness. Their access is limited to research purposes only.
  - **Admin:** Controls system operations, approves patient data access, and monitors hospital and patient performance through graphical reports. This ensures system efficiency, security, and proper governance.

V. IMPLEMENTATION

The implementation phase represents the practical realization of the proposed privacy-preserving healthcare data sharing system. It involves converting the system design into a working model using appropriate technologies, tools, and programming techniques. The system is implemented to ensure secure data sharing, privacy preservation, and efficient data management across distributed healthcare environments. It integrates multiple advanced technologies such as cloud computing, data anonymization, encryption techniques, and role-based access control to maintain confidentiality and integrity of healthcare data. The implementation follows a modular approach, where each module is developed independently and later integrated to form a complete system.

Algorithm Used

Existing Algorithm

The existing system uses Role-Based Access Control (RBAC) to manage user permissions in healthcare environments. In RBAC, access rights are assigned to roles rather than individual users, and users gain permissions based on their assigned roles. This approach simplifies access management, improves security, and supports regulatory compliance by ensuring users can only access information relevant to their responsibilities. However, RBAC has several limitations in dynamic healthcare scenarios. It lacks context awareness, meaning it does not consider factors such as time, location, or emergency situations while granting access. For example, during emergencies, healthcare professionals may require immediate access to patient data beyond their assigned roles, but RBAC's static nature may restrict such access. This rigidity can delay critical decisions and reduce system flexibility. Additionally, managing roles in complex systems can become challenging, leading to inefficiencies in large-scale healthcare environments [9].

Proposed Algorithm

The proposed system uses Homomorphic Encryption (HE) to enhance data security and privacy. Homomorphic Encryption allows computations to be performed directly on encrypted data without decrypting it. The processed result, when decrypted, matches the outcome of operations performed on the original data. This ensures that sensitive patient information remains secure even during data processing and analysis. Unlike traditional encryption methods that require decryption before computation, HE enables secure data usage in encrypted form. This makes it highly suitable for healthcare systems where privacy and compliance are critical. It allows hospitals and researchers to perform data analysis, machine learning, and cloud-based processing without exposing confidential patient data. Homomorphic Encryption operates through key steps such as key generation, encryption, evaluation, and decryption. It supports secure operations like addition and multiplication on encrypted data. Overall, this approach provides stronger privacy protection, enables secure data sharing, and improves trust, making it more effective and scalable than RBAC in modern healthcare systems.

VI. EXPERIMENTAL RESULTS

Home Page

The Below figure represents the Home Page of the system, which serves as the primary interface for users. It provides an overview of the healthcare platform and highlights the importance of secure and privacy-preserving data management. The navigation bar allows users to access different modules such as distributed health management, data anonymization, audit logging, and patient services. This page enhances user experience by offering easy navigation and a clear introduction to system functionalities. This page allows new hospitals to create an account by providing necessary details such as hospital name, location, contact number and password. It ensures that only authorized healthcare institutions can access the system.

The registration process is designed to be simple and secure, enabling hospitals to join the platform and utilize distributed healthcare services efficiently.

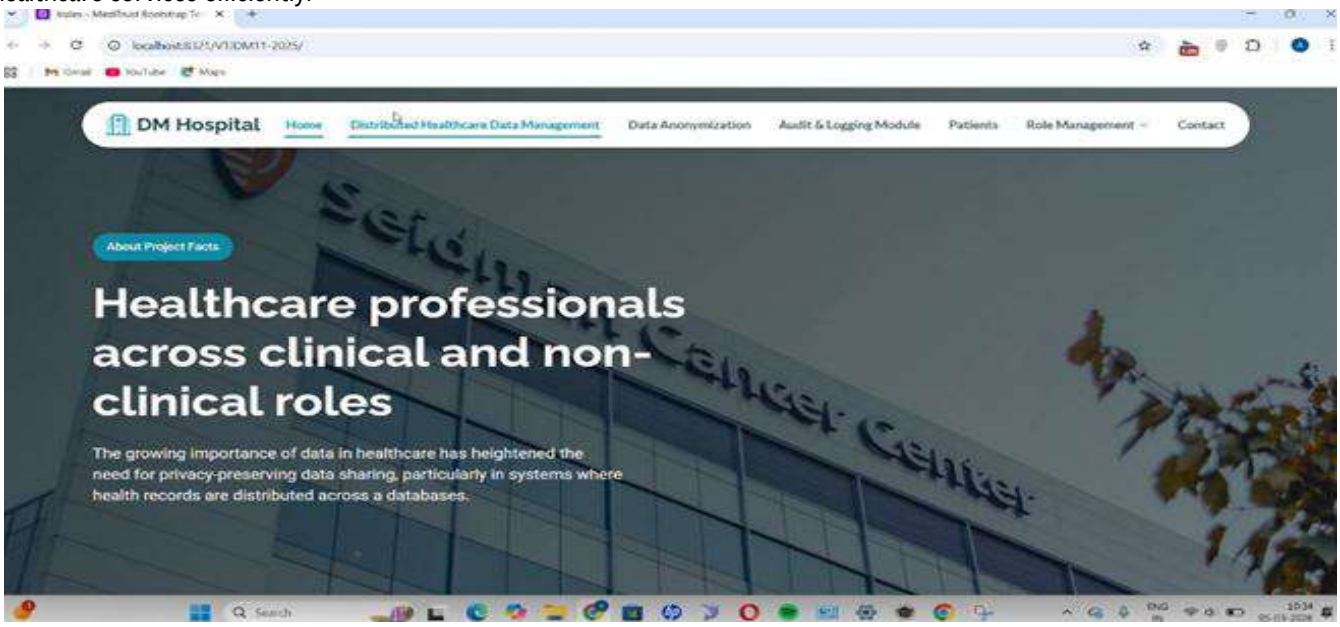

Fig: 2 Home Page

Hospital Registration Page:

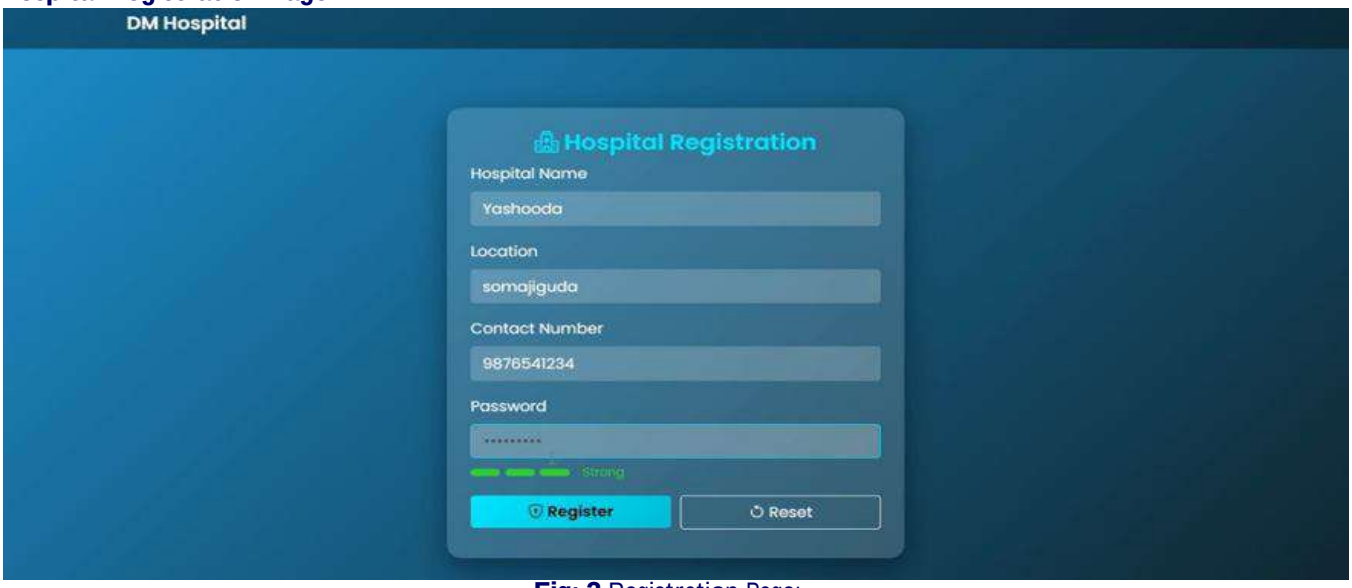

Fig: 3 Registration Page:

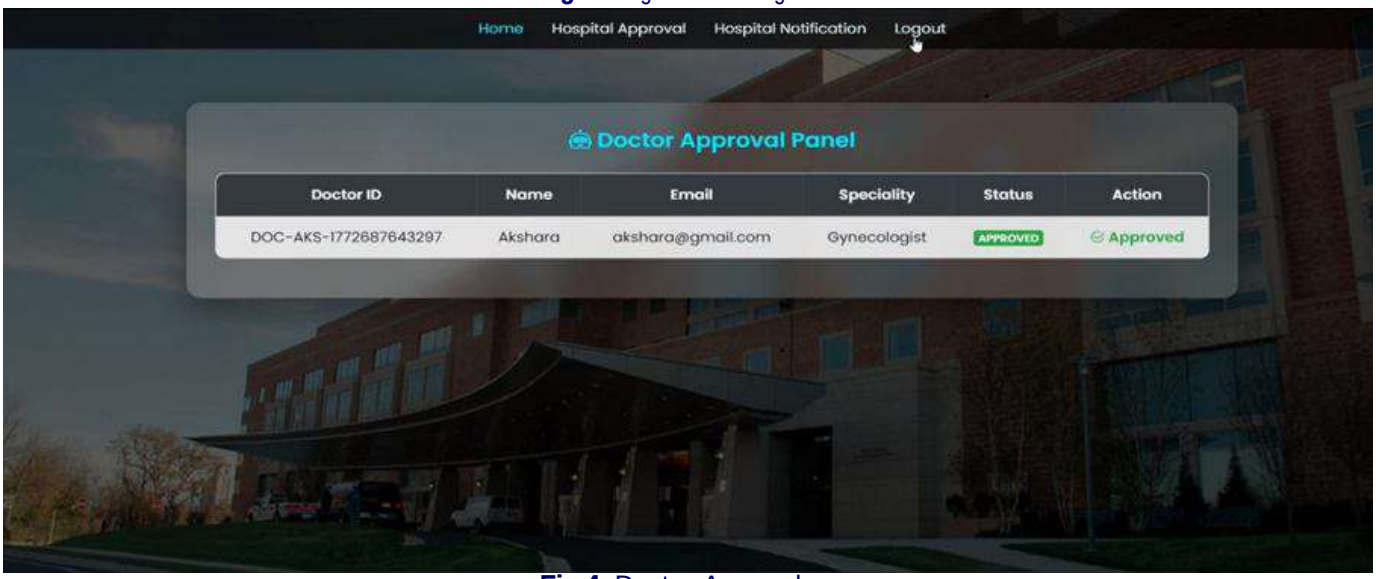

Fig 4: Doctor Approval

Doctor Approval:

The below figure represents the dashboard of distributed healthcare data management which ensures approval of all the registered doctors. By clicking upon the approve button beside the respective registered doctors updating status to approved .Only approved doctors have the access to login to Doctor Dashboard.

Data Anonymization Login Page

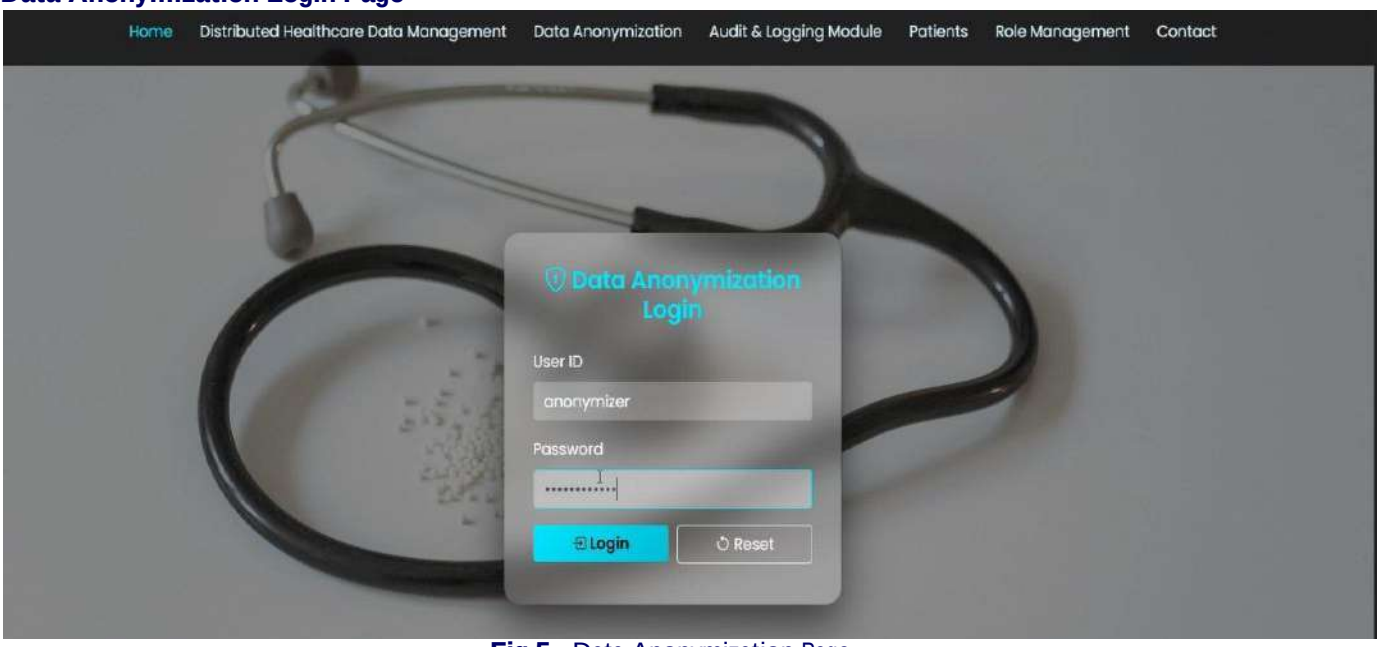

Fig 5 : Data Anonymization Page

The patient ID is generated dynamically by clicking on the "Generate ID" button provided beside each patient record. This generated ID is then used by patients to log in to the system. The approach ensures a simplified login mechanism while maintaining uniqueness of patient identification for accessing anonymized data.

Patient Dashboard – Sending request to doctors

In this page, patients can view the list of available doctors and select a doctor based on their requirement. By clicking on the "Send Request" button, the patient can send a consultation request to the chosen doctor. This feature enables easy communication between patients and doctors and ensures efficient healthcare service delivery.

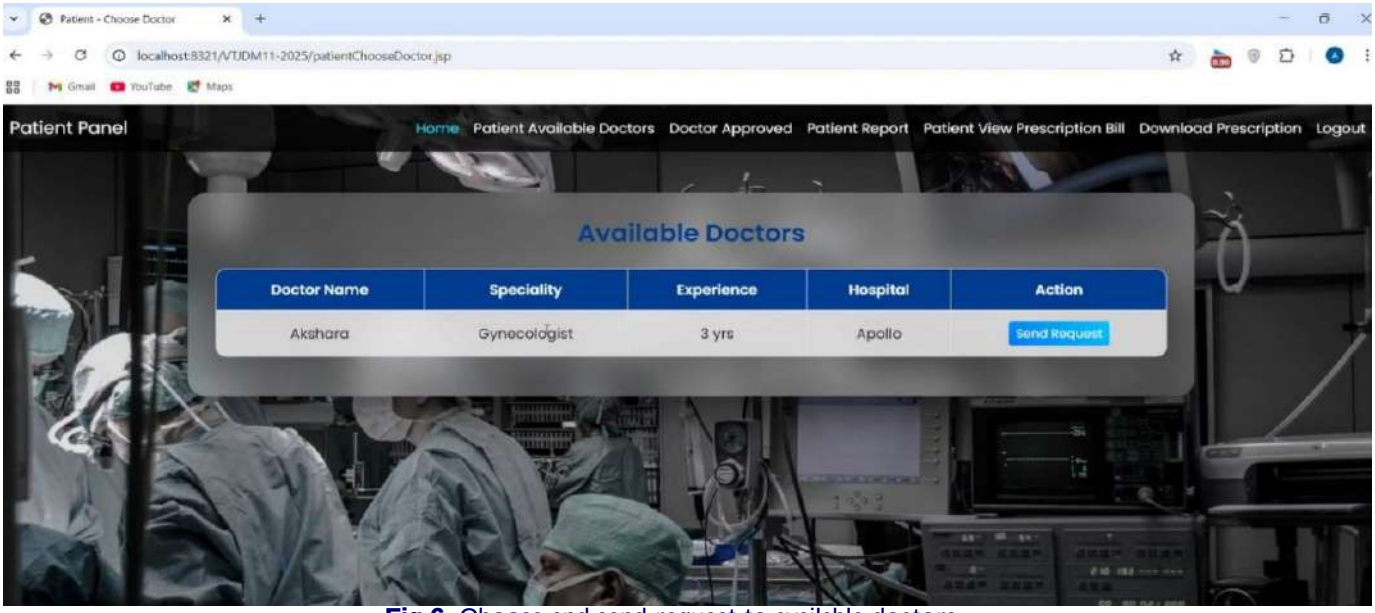

Fig 6: Choose and send request to available doctors

Doctor Dashboard – Managing Patient Requests

In this page, doctors can view the list of requests sent by patients. In the action column, options such as "Approve" and "Reject" buttons are provided to manage each request. By clicking "Approve," the doctor accepts the patient's request, while clicking "Reject" declines it. This feature helps doctors efficiently manage patient interactions and ensures proper handling of consultation requests

Patient Dashboard – Uploading Medical Report

Once the doctor approves the request, the patient can view the approved doctor's name and associated hospital details. Along with this, an option to upload a medical report is provided.

The patient is required to enter symptoms, choose the report file, and click on the upload button. This feature enables patients to share their medical information securely with the approved doctor for further consultation.

.

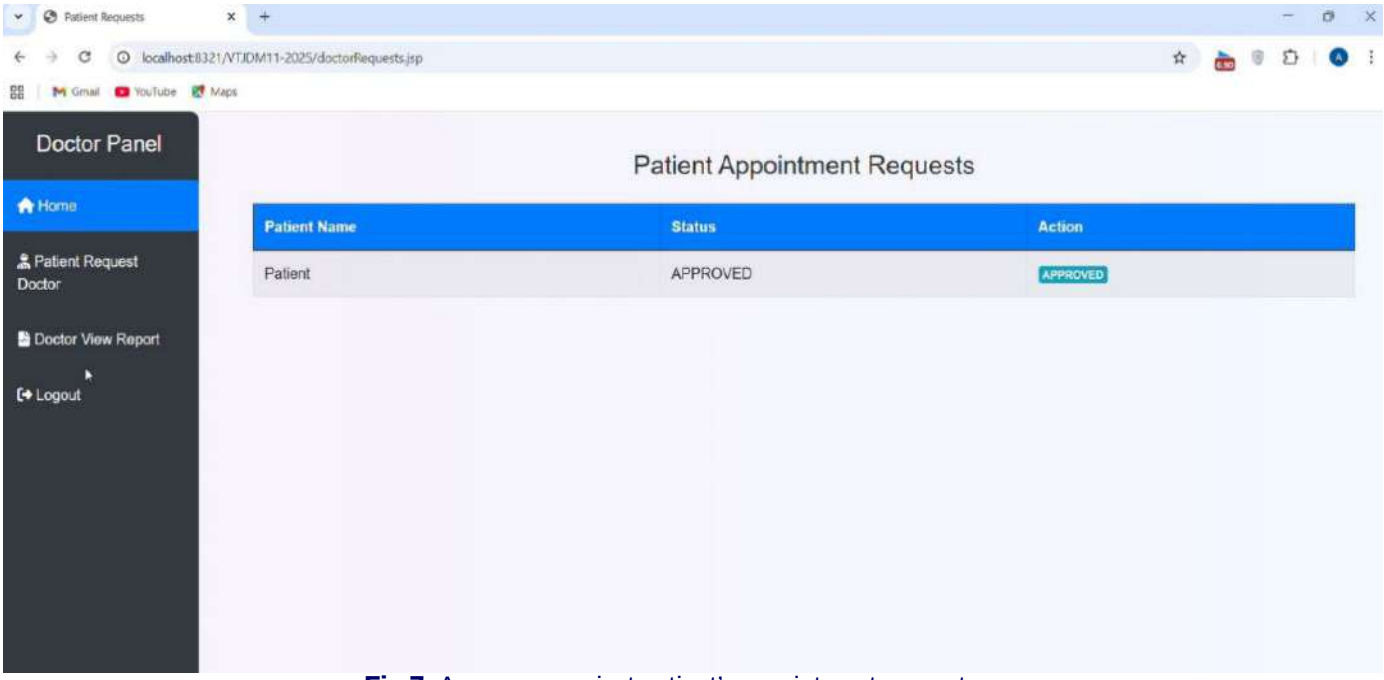

Fig 7: Approve or reject patient's appointment requests

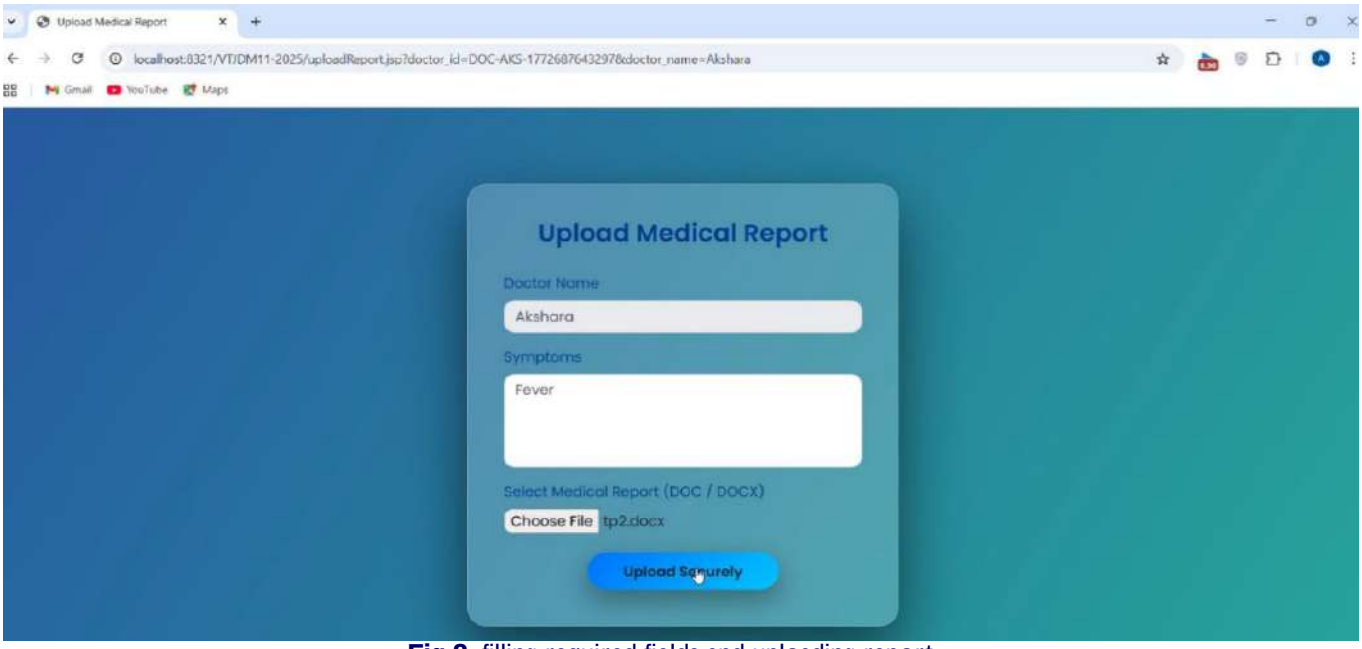

Fig 8: filling required fields and uploading report

Doctor Dashboard – Accessing Encrypted Patient Reports

The above figure represents the Doctor Dashboard for accessing patient reports. The uploaded medical reports are stored in homomorphically encrypted form to ensure data privacy and security. Initially, the doctor cannot directly view the report content. By clicking on the "Request Access" button, a permission request is sent to the patient. Once the patient approves the request, the doctor is allowed to download and view the report. This process ensures secure and controlled access to sensitive patient data.

Patient Dashboard – Viewing Prescription with Payment

The below figure represents the Patient Dashboard for accessing the prescription. After the doctor shares the prescription, the patient is required to complete the payment process before downloading it. A payment option is provided, and upon successful payment, the patient can download and view the prescription. This feature ensures controlled access to medical advice while incorporating a billing mechanism into the system.

IJIRAE::International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.03

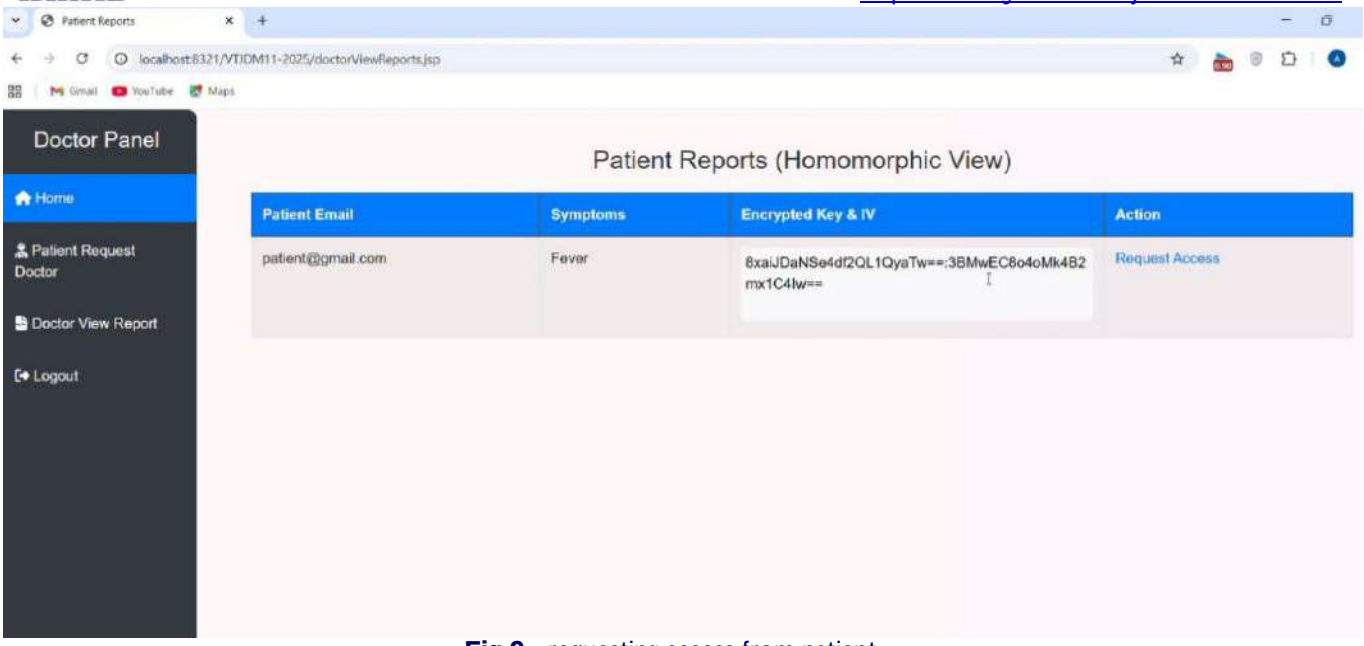

Fig 9 : requesting access from patient

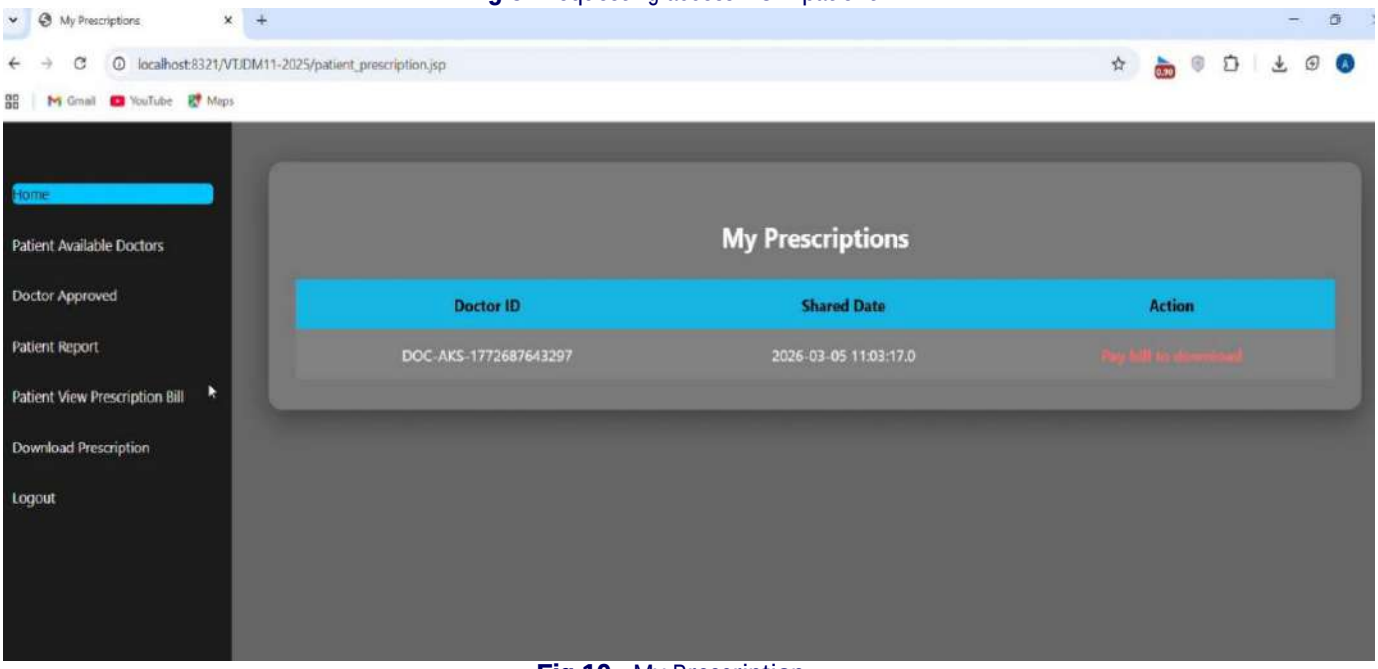

Fig 10: My Prescription

Admin Dashboard – System Monitoring

Fig 11 : Admin Dashboard

The above figure represents the Admin Dashboard of the system. In this module, the admin logs in using static credentials to access the system. The admin can view the overall progress of hospitals, patient activities, and hospital performance through visual representations such as charts and graphs. This dashboard provides a comprehensive overview of the system, helping in monitoring and managing healthcare operations effectively.

VII. CONCLUSION

This study examined current attitudes toward data sharing in the Australian healthcare sector and identified level of trust and concern among healthcare professionals and organizations. We also explored the barriers and potential adoption of technological solutions to privacy-preserving data sharing, which has received limited attention in previous research. We have highlighted several limitations of this study, including the limiting effect of the sample size on measuring levels of trust and concern within some of the variables and the timing of the study possibly influencing some of the results related to barriers to adoption. The majority of respondents fell into the mid-aged bracket, and this also had the effect of some of the findings being centered on this age group. Future research should focus on expanding on the sample size, and having more data collected in different economic cycles would help provide more information about the barriers that exist. Additionally, we feel that a view of any contrasts in Australia's unique private-public healthcare practice split would be pertinent in future studies, especially with the context of cost being a major barrier.

VIII. FUTURE ENHANCEMENT

The differences between demographic groups and levels of concern, motivations for sharing private data and likelihood of adoption have been examined thoroughly in this study and provide a starting point for future research on thinking about how these groups could be engaged, motivated or communicated within the process of implementing a technological solution. We outlined our case for stronger governance and technological solutions for privacy-preserving data sharing. We feel the findings of the study support this stance and show that support for a technological solution exists in the healthcare industry in Australia Further research as well as education and support from government and industry bodies may help shape a strategy to ensure the adoption is successful. By examining current attitudes and identifying potential barriers and facilitators to technological adoption. This research has made a start in contributing to the development of effective policies and strategies to improve privacy preserving data sharing in healthcare.

ACKNOWLEDGMENT

The authors extend sincere thanks to Mr.Bandari Ravi, Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Hyderabad, for his consistent guidance and mentorship throughout this project. They also acknowledge Dr.B.Santhosh Kumar, Head of Department, for his expert supervision, and Mr. D. Srinivas, Project Coordinator, for his practical suggestions during system development. Gratitude is also expressed to the faculty and laboratory staff of the CSE Department, GNIT, and to the authors' families for their encouragement and moral support.

REFERENCES

1. S.Xu, J.Ning, X.Li, J.Yuan, X.Huang, and R.H.Deng, "A privacy preserving and redactable healthcare blockchain system," IEEE Trans. Services Compute., vol. 17, no. 2, pp. 364–377, Mar. 2024.
2. I.Lunden. (Oct. 2021). Triple Blind Secures $24M for a New Approach to Enterprise-level, Privacy-Preserving Data Sharing. TechCrunch. https://techcrunch.com/2021/10/18/tripleblind-secures-24mfor-a-new-approach-to-enterprise-level-privacy-preserving-data-sharing/
3. L.Liu, J.Li, J.Lv, J.Wang, S.Zhao, and Q.Lu, "Privacy-preserving and secure industrial big data analytics: A survey and the research framework," IEEE Internet Things J., vol. 11, no. 11, pp. 18976–18999, Jun. 2024.
4. V.Xafis, "The acceptability of conducting data linkage research without obtaining consent: Lay people's views and justifications," BMC Med. Ethics, vol. 16, no. 1, pp. 1–16, Dec. 2015.
5. Australian Digital Health Agency. (2021). My Health Record, 2021. Accessed: 2023. [Online]. Available: https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record
6. R.Canaway, D. I. Boyle, J.-A.-E. Manski-Nankervis, J. Bell, J. S. Hocking, K. Clarke, M. Clark, J. M. Gunn, and J. D. Emery, "Gathering data for decisions: Best practice use of primary care electronic records for research," Med. J. Aust., vol. 210, no. S6, pp. S12–S16, Apr. 2019.
7. Kumar,B.S., & Rukmani, K. V. (2010). Implementation of web usage mining using APRIORI and FP growth algorithms. Int. J. of Advanced networking and Applications, 1(06), 400-404.
8. B.Maram, R. Majji, G. K. D. Gopisetty, A. Garg, T. Daniya and B. S. Kumar, "Lightweight Cryptography based Deep Learning Techniques for Securing IoT Based E-Healthcare System," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1334-1341, https://doi.org/10.1109/ICACRS58579.2023.10404726
9. Purbey,S., Khan, N., Singh, B.K. et al. Adam energy valley optimization-based routing and RF-Spinalnet enabled medical data classification in IoT. Int. J. Mach. Learn. & Cyber.16 2377–2399 (2025). https://doi.org/10.1007/s13042-024-02397-9.
10. Joshi, Y., Totad, S. G., Geeta, R. B., & Prasad Reddy, P. V. G. D. (2018). Mobile agent-based frequent pattern mining for distributed databases. In S. Bhalla, V. Bhateja, A. Chandavale, A. Hiwale, & S. Satapathy (Eds.), Intelligent computing and information and communication (Vol. 673). Springer. https://doi.org/10.1007/978-981-10-7245-1_9
11. Bharamagoudar, G. R., Totad, S. G., Prasad Reddy, P., &Shobha, R. B. (2015). Zealous leadership paradigms. International Journal of Globalisation and Small Business, 7(1), 92–106. https://doi.org/10.1504/IJGSB.2015.069033
12. Geeta, R. B., Totad, S. G., Prasad Reddy, P., &Shobha, R. B. (2015). Big data structure and usage mining coalition. International Journal of Services Technology and Management, 21(4/5/6), 252–271. https://doi.org/10.1504/IJSTM.2015.073930](https://doi.org/10.1504/IJSTM.2015.073930