e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

AUTHORIZED SEARCHABLE FRAMEWORK FOR E-HEALTHCARE SYSTEM

P. Chandra Sekhar*1, Kammala Vinay*2, Mogulla Ragender*3, Gouri Rohith*4

*1Assistant Professor, Department Of Computer Science & Engineering, Guru Nanak Institute Of Technology, Ibrahimpatnam, RR District, Telangana, India.

*2,3,4Student, Department Of Computer Science & Engineering, Guru Nanak Institute Of Technology, Ibrahimpatnam, RR District, Telangana, India.

DOI: https://www.doi.org/10.56726/IRJMETS64829

ABSTRACT

The paper addresses key challenges in e-healthcare systems, where encrypted personal healthcare records (PHRs) enhance privacy but hinder effective data utilization. Additionally, the need for doctors to be online during treatment is often impractical.

The proposed solution, **DSAS (Dynamic Secure Access Scheme)**, is a secure proxy searchable re-encryption scheme that ensures:

1. **Privacy and Confidentiality**: PHRs are encrypted before uploading to the cloud server, safeguarding patient data.
2. **Controlled Access**: Only authorized doctors or research institutions can access the encrypted PHRs.
3. **Delegation of Responsibilities**: The doctor-in-charge (Alice) can delegate access to a proxy (Bob) or research institutions through the cloud server, minimizing data exposure.

The scheme formalizes security definitions and provides rigorous proofs of its security. Performance evaluations validate the efficiency of DSAS, ensuring safe, practical, and effective remote monitoring and research of PHRs in e-healthcare systems.

I. INTRODUCTION

E-healthcare sensor networks, fueled by advancements in artificial intelligence and wearable technologies, enable the collection and utilization of personal healthcare records (PHRs) for efficient medical treatment and research. By leveraging sensor devices, these networks allow doctors to diagnose patients more effectively and researchers to analyze illnesses and develop improved treatments. However, the outsourcing of PHRs to third-party cloud servers poses significant security risks, including data leakage and loss of control over sensitive information. This necessitates robust privacy and confidentiality measures.

Encrypting PHRs before storage is a widely used method to protect data confidentiality and prevent unauthorized access. However, traditional encryption methods make querying encrypted data inefficient, complicating the retrieval of relevant information for authorized users. This challenge is particularly critical for medical institutions and researchers who rely on extensive data analysis for disease control and prevention.

To address these issues, **Searchable Encryption (SE)** systems have been introduced. SE enables the cloud server to perform secure keyword-based searches on encrypted data using a trapdoor mechanism, ensuring that only authorized users can access specific records without revealing sensitive details. This approach balances security and usability, allowing efficient storage, management, and retrieval of PHRs while safeguarding patient privacy in e-healthcare systems.

II. LITERATURE SURVEY

1. TITLE: " From single-input to multi-client inner-product functional encryption

YEAR: 2019

DESCRIPTION: We present a new generic construction of multi-client functional encryption (MCFE) for inner products from single-input functional inner-product encryption and standard pseudorandom functions. In spite of its simplicity, the new construction supports labels, achieves security in the standard model under adaptive corruptions, and can be instantiated from the plain DDH, LWE, and Paillier assumptions. Prior to our work, the only known constructions required discrete-log-based assumptions and the random-oracle model. Since our new scheme is not compatible with the compiler from Abdalla et al. (PKC 2019) that decentralizes the

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

generation of the functional decryption keys, we also show how to modify the latter transformation to obtain a decentralized version of our scheme with similar features.

2. TITLE: Two-input functional encryption for inner products from bilinear maps.

YEAR: 2018

DESCRIPTION: Functional encryption is a new paradigm of public-key encryption that allows a user to compute f(x) on encrypted data CT(x) with a private key SKf to finely control the revealed information. Multi-input functional encryption is an important extension of (single-input) functional encryption that allows the computation f(x1,...,xn) on multiple ciphertexts CT(x1),...,CT(xn) with a private key SKf. Although multi-input functional encryption has many interesting applications like running SQL queries on encrypted database and computation on encrypted stream, current candidates are not yet practical since many of them are built on indistinguishability obfuscation. To solve this unsatisfactory situation, we show that practical two-input functional encryption schemes for inner products can be built based on bilinear maps. In this paper, we first propose a two-input functional encryption scheme for inner products in composite-order bilinear groups and prove its selective IND-security under simple assumptions. Next, we propose a two-client functional encryption scheme for inner products where each ciphertext can be associated with a time period and prove its selective IND-security. Furthermore, we show that our two-input functional encryption schemes in composite-order bilinear groups can be converted into schemes in prime-order asymmetric bilinear groups by using the asymmetric property of asymmetric bilinear groups

III. METHODOLOGY

3.1 METHODOLOGIES

3.1.1 MODULES NAME:

This project having the following 5 modules:

1. User Interface
2. Admin
3. Doctor
4. Patient

System Architecture

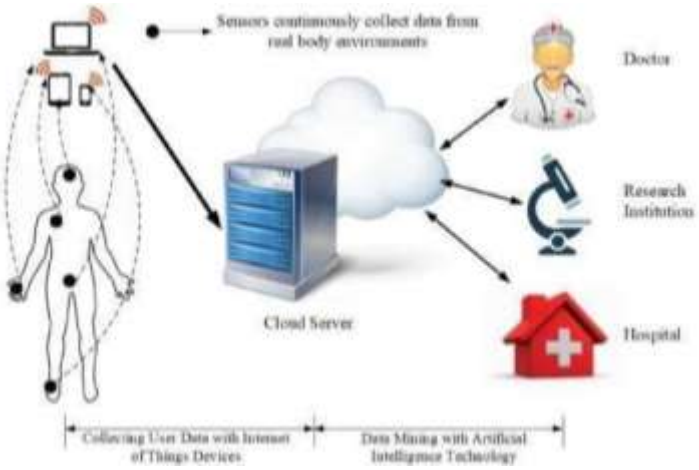

Fig 3.1: System Architecture

3.1.2 Module Descriptions

1. User Interface Design

In this module we design the windows for the project. In this module mainly we are focusing the login design page with the Partial knowledge information. Application Users need to view the application they need to login through the User Interface GUI is the media to connect User and Media Database and login screen where user can input his/her user name, password and password will check in database, if that will be a valid username and password then he/she can access the database.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

2. Admin

Admin can add the doctors into website and view the doctor and patient details. Doctor can have following operations:

1. View patients list.
2. View doctors list.
3. Add doctors.
4. Logout.

3. DOCTOR

In this project doctors will be added by admin and login into this website with the credentials which are given by admin. And view patient requests and connect with patients. And also view the patient daily activities and give the instructions to patient regarding health based on daily activities of that particular patient for fast recovery from decease. Doctor can have following operations:

1. View patient requests.
2. Connect with patients.
3. View daily activities of the patients.
4. Give instructions based on patient activities.
5. View patient details.
6. Messaging with patient.
7. Logout

4. Patient

In this project patient can register into this website for keep tracking his daily activities and send that data to doctors and getting daily instructions from connected doctors and follow their instructions for good health condition. Patient can have following operations:

1. Store daily activities by frequent patterns into website.
2. Send request for doctor. 3. Get instructions from doctor.
4. Messaging with doctors.
5. View doctor's details.
6. View uploaded frequent patterns.
7. Logout.

3.2 Design and Workflow Modeling

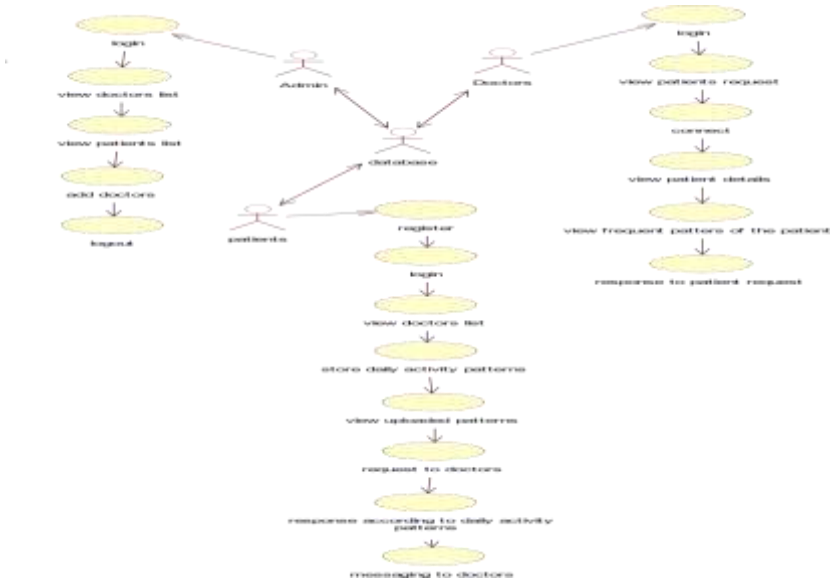

Fig 3.2: Use Case Diagram

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

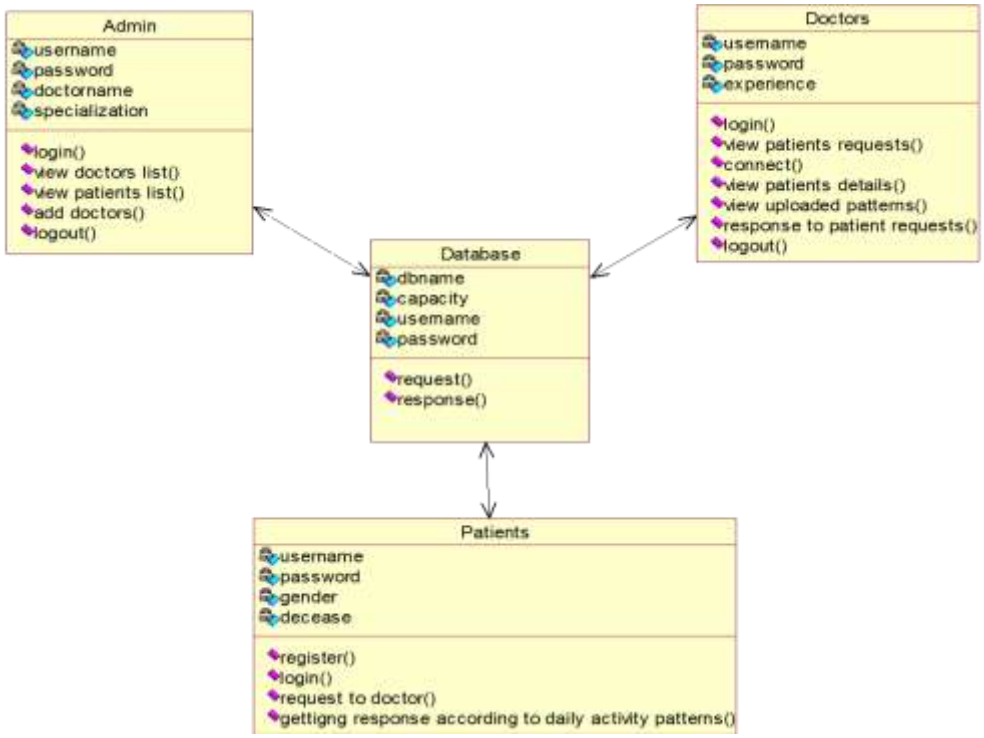

Fig 3.3: Class Diagram

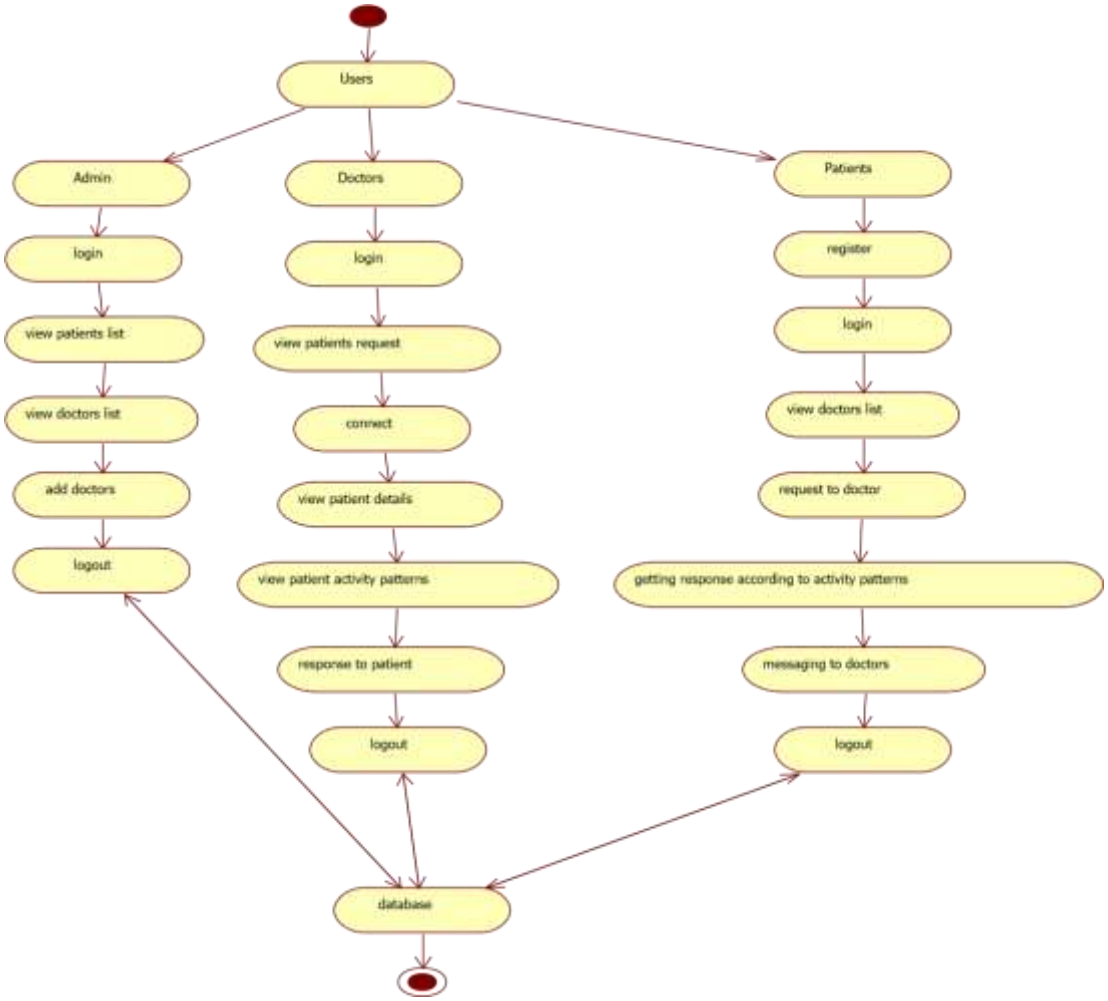

Fig 3.4: Activity Diagram

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

Use cases are used during requirements elicitation and analysis to represent the functionality of the system. Use case focus on the behaviour of the system from an external point of view. The identification of actors and use cases results in the definition of the boundary of the system, which is, in differentiating the tasks accomplished by the system and the tasks accomplished by its environment. The actors are outside the boundary of the system, where as the use cases are inside the boundary of the system.

In this class diagram represents how the classes with attributes and methods are linked together to perform the verification.

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

IV. RESULTS & DISCUSSSION

This project is implements like web application using COREJAVA and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.

Fig 4.1: Home Page

Fig 4.2: USER LOGIN PAGE

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

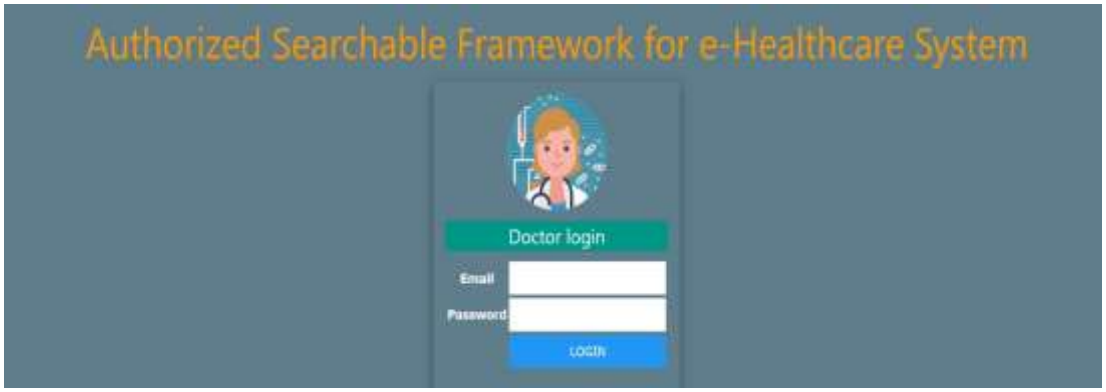

Fig 4.3: DOCTOR LOGIN PAGE

Fig 4.4: Admin Page

Fig 4.5: User welcomes Page

Fig 4.6: Doctor Welcome Page

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

Fig 4.7: Doctor's List

Fig 4.8: Getting User Details

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 (delegatee), by specifying a re-encryption key. With the reencryption key, the cloud server can per-form ciphertext 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 with-out learning information about the keyword or the under-lying 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 delegatee (Bob). We have demonstrated security through a rigorous proof, and the performance analysis confirms that our proposed scheme DSAS is efficient and practical.

VI. REFERENCES

[1] T.Kishore Babu, Raja Kiran Kolati, Pathipati Chandrasekhar, Nimmagadda MuraliKrishna, Sriharaha Vikruthi, B. Rajeswari "2024 International Conference on Expert Clouds and Applications (ICOECA)" , 2024.

[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. 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.