isrjournals

International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications

Volume: 5 Issue: 3 Apr,2025,ISSN_NO: 2320-7248

ENHANCING PRIVACY AND SECURITY IN CLOUD-BASED PERSONAL HEALTH RECORD SHARING THROUGH SESPHR METHODOLOGY.

Babisha.S[1], Harini.M[2], Ramya.D[3] Dr Kamal N[4*]

[123]UG Scholar-Department of Computer Science, GRT Institute of Engineering and Technology, Tiruttani, India.

[4*]Professor-Department of Computer Science, GRT Institute of Engineering and Technology, Tiruttani, India.

babishas2004@gmail.com ,mharini2330@gmail.com ,ramyadhuruvasan710@gmail.com

[4*]Corresponding Author: kamal.n@grt.edu.in

ABSTRACT:

The broad acknowledgment cloud-based administrations in the medicinal services area has brought about financially savvy and helpful trade of Personal Health Records (PHRs) among a few taking an interest elements of the e-Health frameworks. By the by, putting away the secret wellbeing data to cloud servers is helpless to disclosure or robbery and requires the improvement of philosophies that guarantee the protection of the PHRs. Along these lines, we propose a system called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR plot guarantees understanding driven control on the PHRs and jam the secrecy of the PHRs. The patients store the scrambled PHRs on the un-confided in cloud servers and specifically concede access to various sorts of clients on various bits of the PHRs. A semi-confided in intermediary called Setup and Re-encryption Server (SRS) is acquainted with set up people in general/private key combines and to create the re-encryption keys. Besides, the technique is secure against insider dangers and furthermore implements a forward and in reverse access control. Besides, we formally dissect and confirm the working of SeSPHR philosophy through the High-Level Petri Nets (HLPN).

Keywords: Cloud Computing, Personal Health Records (PHRs), Privacy, Security, SeSPHR, Encryption, Access Control, Re-encryption, Insider Threats, e-Health Systems, HLPN.

1. INTRODUCTION:

The rapid adoption of cloud-based services in the healthcare sector has significantly improved the efficiency and cost-effectiveness of managing and exchanging Personal Health Records (PHRs). Cloud technology provides a scalable and convenient platform for storing and sharing sensitive health data among various healthcare entities. However, the security and privacy of PHRs remain major concerns, as storing confidential medical information on untrusted cloud servers makes it vulnerable to unauthorized access, data breaches, and theft. To address these challenges, we propose a secure framework called SeSPHR, which ensures patient-centric control over PHRs while preserving their confidentiality. In this approach, patients encrypt their health records before uploading them to their cloud and selectively grant access to the different users based on specific policies. A semi-trusted (SRS) is introduced to manage public/private key generation and re-encryption keys, enabling a secure and efficient sharing mechanism. Additionally, SeSPHR is designed to mitigate insider threats and enforce both forward and backward access control, ensuring that access permissions can be dynamically modified as needed. The security and effectiveness of the proposed system are formally analyzed using High-Level Petri Nets (HLPN), demonstrating its reliability in securing PHRs. Performance evaluations further indicate that SeSPHR is efficient in terms of time consumption, making it a suitable solution for securely sharing PHRs in cloud environments.

2. PROBLEM OF THE STATEMENT:

With the rapid digitization of healthcare systems, Personal Health Records (PHRs) are increasingly being stored and managed on cloud platforms. Cloud computing offers scalability, accessibility, and cost-effectiveness for managing large volumes of health data. However, this convenience comes at the cost of serious privacy and security challenges. PHRs typically contain highly sensitive and confidential information, such as medical history, prescriptions, lab reports, and diagnostic results. When these records are stored or shared through the cloud, they become vulnerable to a wide range of threats, including:

- Unauthorized access and data breaches
- Malicious insiders or third-party misuse
- Data tampering and integrity issues
- Lack of patient control over who accesses their data
- Inadequate encryption and weak access control mechanisms.

Many existing systems fail to strike the right balance between data availability (ensuring authorized users can access the data when needed) and data protection (ensuring that unauthorized parties cannot access or alter the data). Moreover, healthcare providers and patients often lack the technical knowledge to manage complex security settings , further increasing the risk of exposure.

As the adoption of cloud-based health services continues to rise, these concerns have become more pressing. There is a critical need for a robust, user-friendly, and intelligent mechanism that ensures:

- Secure storage of PHRs in the cloud.
- Efficient and encrypted data sharing among authorized stakeholders (doctors, hospitals, patients, etc.).
- Fine grained access control to restrict data access based on roles and permissions.
- Auditability and traceability of access and data sharing events.

3. MODULE DISCRIPTION:

3.1. ADMIN MODULE:

In this Module, a User must Authorised in our application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users... Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information.

3.2. UNIQUE ID AND KEY VERIFICATION:

In this module, when every provider must have a unique hospital details and doctor list. when a User comes under in an application and accepts the Provider for further Proceeding Comes under in the booked Provider alone.

3.3. REPORTS UPLOAD:

In this module, when a User booked his Provider along with Hospitality Functions and Doctor Specialist in an application... Once a User come back for further Process, they made a counselling to Particular Doctor.

3.4. DOCTOR COUNSELLING:

We consider the server to be semi-trusted, that means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges.

3.5. USER ENTRY CHECKING:

In this Module, we had implemented main goal of the Project it denotes security for viewing our personal information to all roles in an application...To prevent that we had proposed to use Attribute Based Encryption Algorithm for the access to encrypt the Selected Details to Restrict to view by others.

3.6. DATABASE REPORT SEARCH:

In this module, admin can able to view overall users report, Users personal Records and User Counselling Records....In Such Case, user had made encrypted their information it will visualization in cipher text format and age display in the K-Anonymity Format.

4. PROPOSED SYSTEM:

We propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs.
A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High-Level Petri Nets (HLPN). Performance evaluation regarding time consumption indicates that the SeSPHR methodology has potential to be employed for securely sharing the PHRs in the cloud.

ADVANTAGES: We present a methodology called SeSPHR that permits patients to administer the sharing of their own PHRs in the cloud. The SeSPHR methodology employs the El-Gamal encryption and proxy re-encryption to ensure the PHR confidentiality. The forward and backward access control is also implemented in the proposed methodology. Formal analysis and verification of the proposed methodology is performed to validate its working according to the specifications.

PROPOSED WORKING:

Setup: The SRS initializes the system with cryptographic parameters and distributes public keys.

Key Distribution: Private keys are generated based on user identity.

Data Encryption: The patient encrypts PHR before uploading to the cloud-ensuring confidentiality.

Delegation: When a patient wants to share their record, they request the SRS to generate a re-encryption key for a specific user.

Re-Encryption: The cloud server uses this key to convert the ciphertext into a form that only the authorized data user can decrypt.

Decryption: The data user uses their private key to retrieve the original PHR.

Access Control: SRS dynamically manages and enforces access policies such as revoking access or limiting past/future visibility.

isrjournals

International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications

Volume: 5 Issue: 3 Apr,2025,ISSN_NO: 2320-7248

5.1. ARCHITECTURE DIAGRAM:

The flowchart represents a secure cloud-based Personal Health Record (PHR) system involving hospitals, patients, and researchers. Hospitals can register, log in, and manage patient data by adding scan records, medical records, and viewing old records. All sensitive data is encrypted before being stored in a centralized cloud database. Patients authenticate using OTP to access or approve decryption. Hospitals can send queries and view replies securely. Researchers, after registration and login, can also view and reply to queries. The system ensures privacy and security through encryption, OTP-based verification, and role-based access control, enabling safe sharing of health data in e-Health environments.

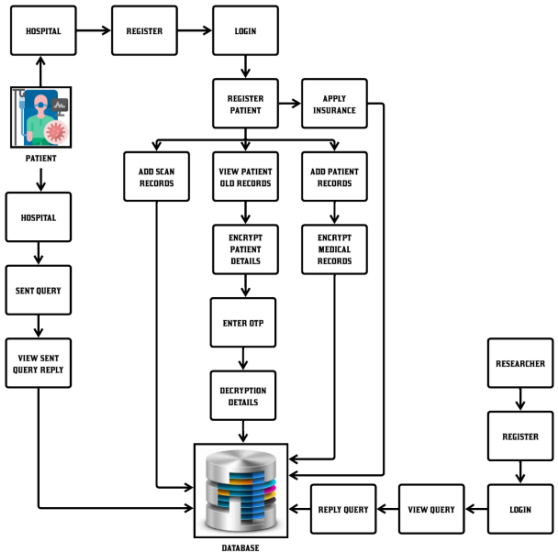

FIG. 5.1. ARCHITECTURE DIAGRAM

5.2. SEQUENCE DIAGRAM:

A sequence diagram in UML is a kind of interaction diagram that shows how processes operate with one another and in what order. A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object of the interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams in Unified Modeling Language and typically are associated with use case different entities. Sequence design to created database relationships realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams, event scenarios, and it a timing diagrams.

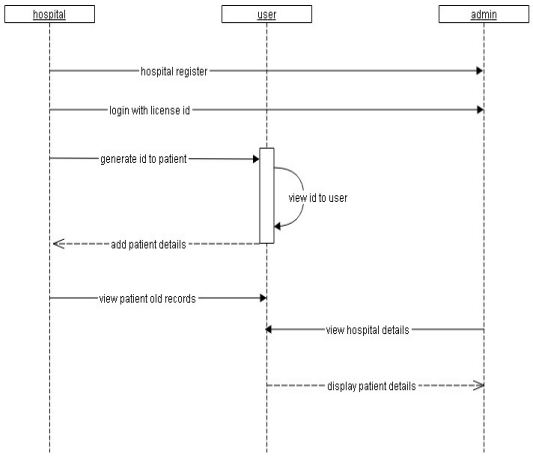

FIG. 5.2. SEQUENCE DIAGRAM

5.3. DATA FLOW DIAGRAM:

It starts with entering new patient details, followed by ID verification using both unique and hospital IDs. Once verified, the system stores the information in a database and allows data to be retrieved and displayed. Patients can add personal details and view their past medical records. The system also includes the ability to generate a secure Aadhaar ID for patients and supports secure updates via fingerprint, image, or password. Doctors have the ability to upload scan reports, which patients can then view. Furthermore, an admin user has broader access and can view both patient and hospital information.

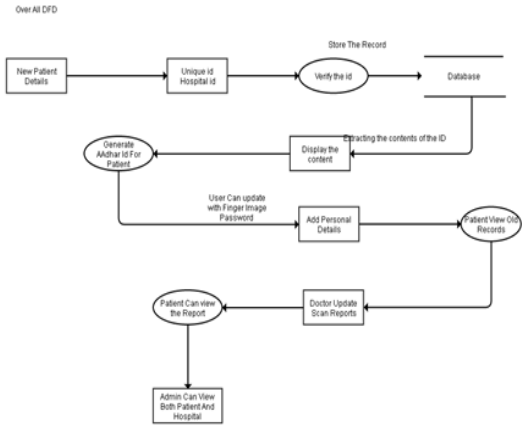

FIG. 5.3. DATA FLOW DIAGRAM

isrjournals

International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications

Volume: 5 Issue: 3 Apr,2025,ISSN_NO: 2320-7248

6. SESPHR METHODOLOGY:

SeSPHR (Secure and Efficient Sharing of Personal Health Records) is a robust and privacy-preserving framework designed to enhance security in cloud-based healthcare data sharing. It empowers patients with full control over their sensitive health data by allowing them to encrypt their Personal Health Records (PHRs) before uploading them to untrusted cloud servers. The core component of SeSPHR is the Setup and Re-encryption Server (SRS), a semi-trusted entity responsible for generating public/private key pairs and re-encryption keys.

When authorized users, such as hospitals or researchers, request access to a patient's data, the SRS provides re-encryption capabilities, transforming the ciphertext without exposing the original content.

SeSPHR supports fine-grained access control, where patients can selectively grant permissions for different portions of their health data. Additionally, it ensures forward and backward access control revoked users lose access to data (forward), and newly authorized users gain access to existing records (backward).

Secure Access Sharing:

- Hospitals and researchers can request access.
- Access is granted using re-encryption, without exposing raw data.

Forward & Backward Access Control:

- Prevents data access by revoked users (forward control).
- Grants access to the newly added users (backward control).

Defends Against Insider Threats:

- Ensures only authorized and intended parties access sensitive health data.

7. HIGH-LEVEL PETRI NET MODEL:

The High-Level Petri Net (HLPN) model for the SeSPHR methodology represents secure Personal Health Record (PHR) sharing in the cloud. It includes places like patient data input, data encryption, key generation, cloud upload, access request, and decryption. Transitions represent actions such as data encryption, key generation by the Setup and Re-encryption Server (SRS), issuing re-encryption keys, data upload, and secure access by authorized users. Tokens flow through the network indicating the system's state at each step. HLPN ensures concurrency, security checks, and access control, effectively modeling the SeSPHR process and verifying its correctness and resistance to unauthorized access.

Dynamic Access Control:

- It models forward and backward access control dynamically, reflecting real-time changes in user permissions.

Scalability Analysis:

- HLPN helps analyze how well the SeSPHR system scales with more users and data without compromising security.

Concurrency Support:

- It captures simultaneous access requests and processes them correctly without data leakage or conflicts.

8. EXPERIMENTAL RESULTS:

This result is based on the implementation of the registration of hospital and patient in the web site and the details of the user are record in the database using SeSPHR methodology.

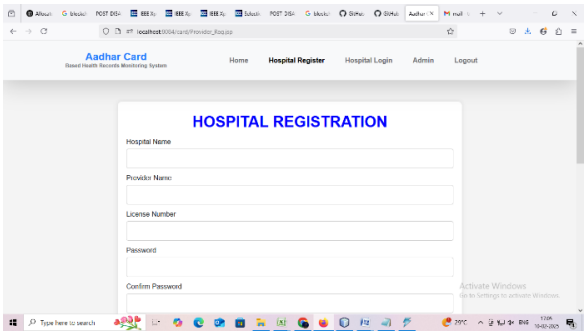

Fig.8.1. HOSPITAL REGISTER PAGE

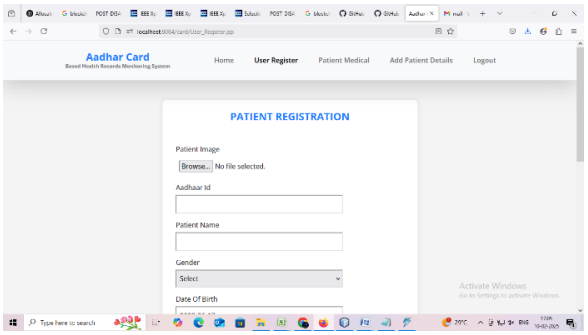

Fig. 8.2. PATIENT REGISTER PAGE

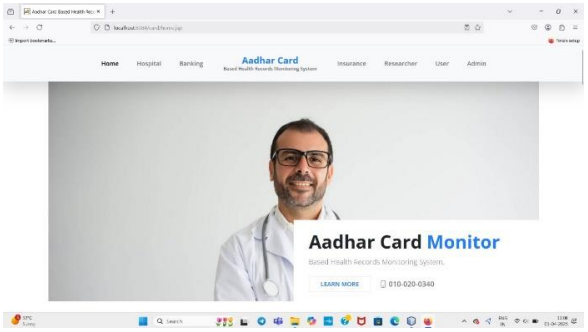

Fig. 8.3. HOME PAGE

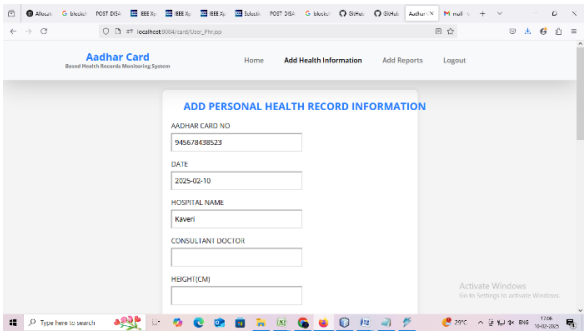

Fig. 8.4. ADD HEALTH RECORD PAGE

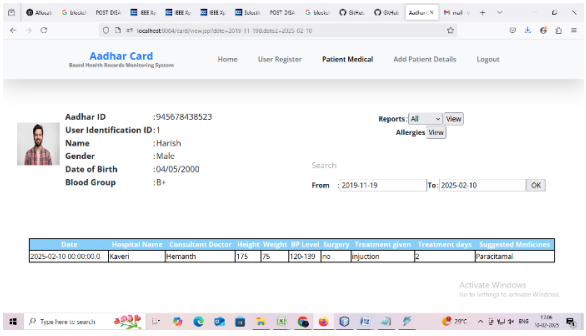

Fig. 8.5. ADD HEALTH RECORD PAGE

9. CONCLUSION & FUTURE WORK:

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively.

FUTURE WORK: The need of an online certificate authority (CA) and one unique key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

REFERENCE:

[1] Antonio Lopez Martinez, Manuel Gil Perez, and Antonio Ruiz-Martinez, “A Comprehensive Model for Securing Sensitive Patient Data in a Clinical Scenario,” VOLUME 11, September 2023.

[2] Hua Shen, “Enhancing Diagnosis Prediction in Healthcare with Knowledge-Based Recurrent Neural Networks.,” VOLUME 11, September 2023.

[3] Vishwa Amitkumar Patel, Pronaya Bhattacharya , Sudeep Tanwar , Rajesh Gupta , Gulshan Sharma , Pitshou N. Bokoro and Ravi Sharma “Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions” VOLUME 10, September 2022.

[4] Abdullah Al Mamun, Sami Azam and Clementine Gritti.,“Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction.” VOLUME 10, January 18 2022.

[5] Alaa Haddad, Mohamed Hadi Habaebi, Md. Rafiqul Islam, Nurul Fadzlin Hasbullah and Suriza Ahmad Zabidi., “Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems.,” VOLUME 10, September 2022

[6] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, ‘‘BinDaaS, ‘‘Blockchain-based deep-learning as-a-service in healthcare 4.0 applications,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[7] A. Awadabdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O’Connor, and J. Laughton, ‘‘MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchange,’’ IEEE Internet Things J., vol. 8, no. 21, pp. 15762–15775, Nov. 2021.

[8] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, ‘‘A blockchain-assisted verifiable outsourced attribute-based signecryption scheme for EHRs sharing in the cloud,’’ IEEE Access, vol. 8, pp. 170713–170731, 2020.

[9] V. Jaiman and V. Urovi, ‘‘A consent model for blockchain-based health data sharing platforms,’’ IEEE Access, vol. 8, pp. 143734–143745, 2020.

[10] S.Cao, J. Wang, X. Du,X. Zhang, and X. Qin, ‘‘CEPS: A crossblockchain based electronic health records privacy-preserving scheme,’’ in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2020, pp. 1–6.