INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

# SECURE SHARING OF PERSONAL HEALTH RECORDS

*P. Kavya*
*B-Tech Student*

*M. Sushanth*
*B-Tech Student*

*G. Uday Kiran*
*B-Tech Student*

*Dr.B.Kavitha Rani*
*Professor*

*Department Of Information Technology*
*Cmr Technical Campus*
*Kadlakoya (V), Medchal, Hyderabad-501401*

***Abstract:*** The widespread acceptance of cloud-based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. Therefore, we propose a methodology called Se SPHR for secure sharing of the PHRs in the cloud. The se SPHR 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 Se SPHR methodology.

## 1. INTRODUCTION

Cloud Computing has emerged as an important computing paradigm to offer pervasive and on demand availability of various resources in the form of hardware, software, infrastructure, and storage Consequently, the cloud computing paradigm facilitates organizations by relieving them from the protracted job of infrastructure development and has encouraged them to trust on the third-party Information Technology (IT) services . Additionally, the cloud computing model has demonstrated significant potential to increase coordination among several healthcare stakeholders and also to ensure continuous availability of health information, and scalability . Furthermore, the cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers . Therefore, the integration of aforementioned entities results in the evolution of a cost effective and collaborative health ecosystem where the patients can easily create and manage their Personal Health Records (PHRs). Existing System: Chen *et al*. introduced a method to exercise the access control dynamically on the PHRs in the multi-user cloud environment through the Lagrange Multiplier using the SKE. Automatic user revocation is the key characteristics of the approach. To overcome the complexities of the key management, a partial order relationship among the users is maintained. However, the scheme requires the PHR owners to be online when the access is to be granted or revoked. Contrary to the scheme presented in [12], our approach does not require the PHR owners to be online to grant the access over PHRs. In- stead the semi-trusted authority determines the access privileges for users and after successful authorization, calculates the re-encryption keys for the users requesting the access. The policy in is based on cipher text and the size of the cipher text increases linearly with multi-use use whereas our policy of our

ISSN: 2057-5688

technique is based on keys and it doesn't affect the size of the cipher text. This is due to the fact that the requires the re-encryption step that is lacking in our methodology. An approach to securely share the PHRs in multi-owner setting, which is divided into diverse domains using the Attribute Based Encryption (ABE) is presented. The proposed methodology is based on the methodology originally presented in. The approach uses proxy re-encryption technique to re-encrypt the PHRs after the revocation of certain user. Proposed system: The proposed system presents a methodology called Secure Sharing of PHRs in the Cloud ( seSPHR) to administer the PHR access control mechanism managed by patients themselves. The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users. Generally, there are two types of PHR users in the proposed approach, namely: (a) the patients or PHR owners and (b) the users of the PHRs other than the owners, such as the family members or friends of patients, doctors and physicians, health insurance companies' representatives, pharmacists, and researchers. The patients as the owners of the PHRs are permitted to upload the encrypted PHRs on the cloud by selectively granting the access to users over different portions of the PHRs. Each member of the group of users of later type is granted access to the PHRs by the PHR owners to a certain level depending upon the role of the user. The levels of access granted to various categories of users are de- fined in the Access Control List (ACL) by the PHR owner.

## II.RELATED WORK

In this section, the existing works that relate to the proposed work are presented. The authors in [28] used public key encryption based approach to uphold the anonymity and unlinkability of health information in semitrusted cloud by separately submitting the Personally Identifiable Information (PII). The patients encrypt the PHRs by the patients through the public key of the Cloud Service Provider (CSP) and the CSP decrypts the record using the private key, stores the health record and the location of the file (index), and subsequently encrypts them through the symmetric key encryption. The administrative control of the patient on the PHRs is maintained by pairing the location and the master key. However, a limitation of the approach is that it allows the CSP to decrypt the PHRs that in turn may act maliciously. On the other hand, we introduced a semi-trusted authority called the SRS that re-encrypts the ciphertext generated by the PHR owner and issues keys to the users that request access to the PHRs. Chen et al. [12] introduced a method to exercise the access control dynamically on the PHRs in the multi-user cloud environment through the Lagrange Multiplier using the SKE. Automatic user revocation is the key characteristics of the approach. To overcome the complexities of the key management, a partial order relationship among the users is maintained. However, the scheme requires the PHR owners to be online when the access is to be granted or revoked. Contrary to the scheme presented in [12], our proposed approach does not require the PHR owners to be online to grant the access over PHRs. Instead the semi-trusted authority determines the access privileges for users and after successful authorization, calculates the re-encryption keys for the users requesting the access. The authors in [29] used a Digital Right Management (DRM) based approach to offer patient-centric access control. The authors employed the Content Key Encryption (CKE) for encryption and the users with the lawful license are permitted to access the health-data. First proxy re-encryption methodology was proposed in [33]. The policy in [33] is

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

based on ciphertext and the size of the ciphertext increases linearly with multi-use use whereas our policy of our technique is based on keys and it doesn't affect the size of the ciphertext. This is due to the fact that the [33] requires the re-encryption step that is lacking in our methodology. An approach to securely share the PHRs in multi-owner setting, which is divided into diverse domains using the Attribute Based Encryption (ABE) is presented by Li et al. [14]. The proposed methodology is based on the methodology originally presented in [33]. The approach uses proxy re-encryption technique to re-encrypt the PHRs after the revocation of certain user(s). In the approach, the intricacies and cost of key management have been effectively minimized and the phenomenon of on-demand user revocation has been improved. Despite its scalability, the approach is unable to efficiently handle the circumstances that require granting the access rights on the basis of users' identities. Xhafa et al. [30] also used Ciphertext Policy ABE (CPABE) to ensure the user accountability. Besides protecting the privacy of the users, the proposed approach is also capable of identifying the users that malfunction and distribute the decryption keys to other users illegitimately. An approach to concurrently ensure the fine-grained access and confidentiality of the healthcare data subcontracted to the cloud servers is presented in [10]. The expensive tasks of data files re-encryption, update of secret keys, and restricting the revoked users to learn the data contents are addressed through the proxy re-encryption, Key Policy ABE (KP-ABE), and lazy re-encryption. The cloud servers are delegated the tasks of re-encryption of data files and subsequent storage to the cloud environment. However, in the proposed framework the data owner is also assumed as a trusted authority that manages the keys for multiple owners and multiple users. Therefore, the inefficiencies would occur at the PHR owners' end to manage multiple keys for different attributes for multiple owners. Our approach avoids the overhead because the tasks of key generation and key distribution to different types of users are performed by the semi-trusted authority. The authors in [31] and [32] also used the proxy re-encryption based approaches to offer fine-grained access control. Our proposed framework permits the PHR encryption by the owners before storing at the cloud and introduces a semi-trusted authority that re-encrypts the ciphertext without learning about the contents of the PHRs. Only the authorized users having the decryption keys issues by the semi- trusted authority can decrypt the PHRs.

## III.IMPLEMENTATION

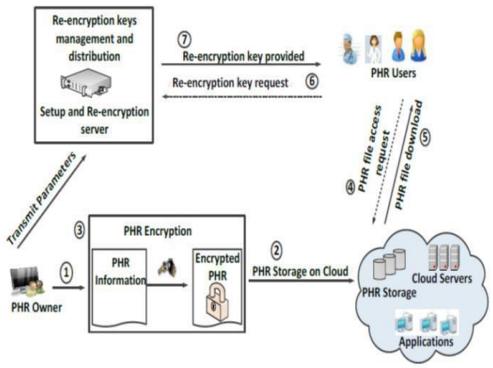


**Figure 3.1system Architecture**

### Modules

### Register & Login

In this Module whether the User or Patient could register and then login .Based On the Usage, they can view their Details and to improve their performance. Individual login activities are modified.

### Admin

In this Admin Module, Admin Could Add the Patient details, to modify the Patient Details with allocation. Hospital records are also updated by the admin. Admin provide authentication of requested Records

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

**Patients**

Patient Visit the Hospital and created a record on the Individual id .They get access through any hospital with the identification.

Hospitals

Hospital update the patient record on cloud, they can access through permission of the data owner such as (patients) Even hospital cannot view the records without the responsibilities of the data owners.

**Cloud Records**

Hospital Updated Patient records are stored in cloud with the Encrypted Format, The Requested access are send to the data owners. This module controlled by the Admin.

## IV RESULT

The results for each of the screenshots shown below.

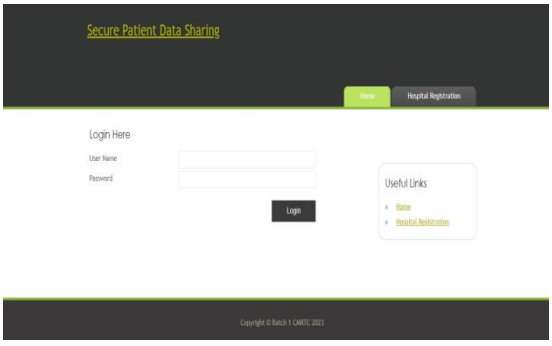


Fig- 4.1: Home page

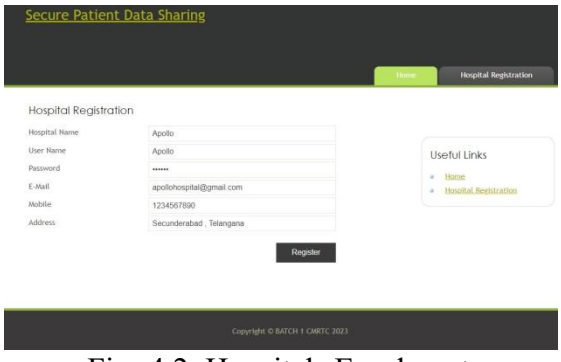


Fig- 4.2: Hospitals Enrolment

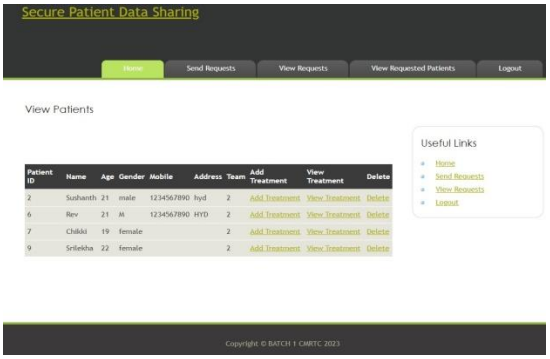


Fig- 4.3:Hospital Dashboard 1

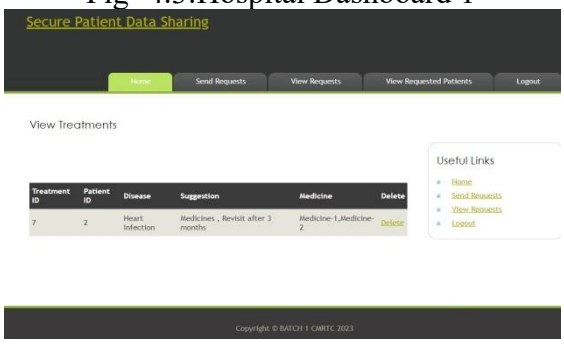


Fig- 4.4: Hospital Dashboard 2


Fig- 4.5: Hospital Data Request

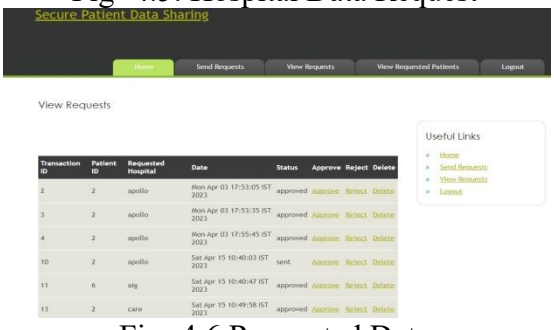


Fig- 4.6 Requested Data

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

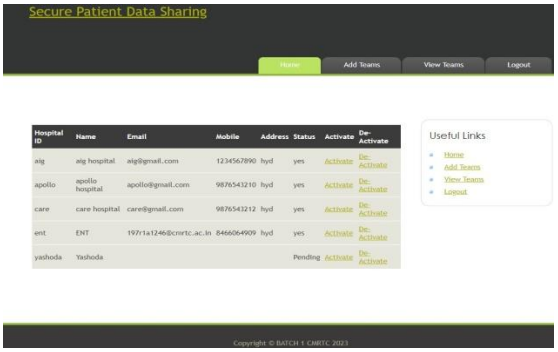


Fig- 4.7: Admin Dashboard 1

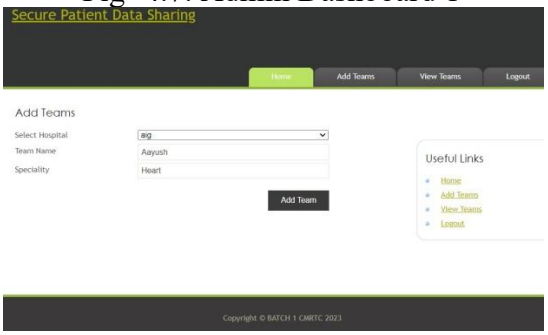


Fig- 4.8: Admin Dashboard 2

## V.CONCLUSION

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access pro-vided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized us-ers 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 pub-lic/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. Moreover, we formally analyzed and verified the working of Se SPHR methodology through the HLPN, SMT-Lib, and the Z3 solver. The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability of the Se SPHR methodology to securely share the PHRs in the cloud environment.

## REFERENCES

1. K. Gai, M. Qiu, Z. Xiong, and M. Liu, “Privacy-preserving multi-channel communication in Edge-of-Things,” Future Generation Computer Systems, 85, 2018, pp. 190-200.
2. K. Gai, M. Qiu, and X. Sun, “A survey on FinTech,” Journal of Network and Computer Applications, 2017, pp. 1-12.
3. A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, “A cloud based health insurance plan recommendation system: A user centered approach, “Future Generation Computer Systems, vols. 43- 44, pp. 99-109, 2015.
4. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, “Incremental proxy re-encryption scheme for mobile cloud computing environment,” The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.
5. R. Wu, G.-J. Ahn, and H. Hu, “Secure sharing of electronic health records in clouds, ] [6] A. Abbas and S. U. Khan, “A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds,” IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.
6. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, “A general framework for secure sharing of personal health records in cloud system,”

ISSN: 2057-5688

Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.
7. J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.
8. D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.
9. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.
10. S. Kamara and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security, vol. 6054, pp. 136–149, 2010.
11. T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.
12. K. Gai, M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers," IEEE Transactions on Industrial Informatics, 2017, DOI: 10.1109/TII.2017.2780885.