International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A Cloud-Based Methodology for Safely Sharing Personal Health Records

Ms.M.ANITHA[1], Mr. E.NAGARAJU [2], Ms.T.CHANDANA PRIYA [3]

#1 Assistant professor in the Master of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#2 Assistant professor in the Master of Computer Applications SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#3 MCA student in the Master of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

Abstract: In the health care industry, this has led to the efficient and cost-effective exchange of personal health records (PHRs) among numerous e-Health system participants. In any case, putting away the classified wellbeing information to cloud servers is inclined to disclosure or burglary and request the occasion of philosophies that ensure the protection of the PHRs. As a result, we typically suggest a method known as SeSPHR for the secure cloud sharing of PHRs. The SeSPHR theme ensures that PHR management is patient-centred and protects PHR confidentiality. The encrypted PHRs are stored by the patients on cloud servers that aren't trusted, and the patients choose who can access which parts of the PHRs. A semi-believed intermediary alluded to as Arrangement and Re-encryption Server (SRS) is acquainted with line up the general population/confidential key matches and to supply the re-encryption keys.

Additionally, the approach enforces both forward and reverse access management, making it resistant to threats from business executives. High Level Petri Nets (HLPN) are also used to formalize our analysis and verification of SeSPHR methodology's operation. Execution investigation concerning time utilization shows that the SeSPHR approach has potential to need for solidly sharing the PHRs inside the cloud. conjointly we will generally Execute as a commitment during this paper deadbeat, Secure Reviewing Stockpiling, in Deadbeat PHR Proprietor add the beginning and Finishing time join to transferred Scrambled documents, and conjointly carry out the TPA Module for check the PHR Record its hack or defiled for the other programmer and miscreant in the event that data hack from programmer feature find all framework subtleties of transgressor like Mac Address and data science Address its our commitment in our task.

Keywords: Access control, cloud computing, Personal Health Records, privacy

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 form the protected job of infrastructure development and has encouraged them to trust on the third party information technology services additionally the cloud computing model has demonstrated significant potential to

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

increase coordination among several healthcare stakeholder and also to ensure continuous availability of health information and scalability. Despite the advantages of scalable agile cost effective and ubiquitous services offered by the cloud various concerns correlated to the privacy of health data also arise a major reason for patients apprehensions regarding the confidentiality of PHRs is the nature of the cloud to share and store the PHRs. Storing the private health information to servers managed by third parties is susceptible to unauthorized access. In particular privacy of the PHRs stored in public clouds that are managed by commercial service providers is extremely at risk the privacy of the PHRs can be at risk in several ways, for example theft, loss, and leakage the PHR either in cloud storage or in transit form the patient to the cloud or from cloud to any other user may be susceptible to unauthorized access because of the malicious behaviour of external entities. The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users. 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 defined in the Access Control List (ACL) by the PHR owner. For example, the family members or friends of the patients may be given full access over the PHRs by the owner. Similarly, the representatives of the insurance company may only be able to access the portions of PHRs containing information about the health insurance claims while the other confidential medical information, such as medical history of the patient is restricted for such users.[1] The key contributions of the proposed work are given below: ➢ 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 methodology allows the PHR owners to selectively grant access to users over the portions of PHRs based on the access level specified in the ACL for different groups of users. ➢ A semi-trusted proxy called SRS(Setup and Reencryption Server) is deployed to ensure the access control and to generate the re- encryption keys for different groups of users by eliminating the key management overhead at the PHR owner's end. ➢ 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.

2.LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company Traffic Redundancy Elimination, once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

external support. This support can be obtained from senior programmers, from book or from websites. Before building the system we have to known the below concepts for developing the proposed system

A new general framework for secure public key encryption with keyword search

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt'04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual- Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted

2)Searchable symmetric encryption: Improved definitions and efficient constructions

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

3.PROPOSED SYSTEM

In order to ensure the security of information while it is stored in the cloud, the attribute based encryption algorithm is used. Two variations of ABE exist, distinguished by their respective placement attributes and access attribute policies. In this study, we create a model and mechanism to regulate access to PHRs kept in the cloud. We offer an ABE encryption method for encrypting each PHR file to achieve effective and modular data access control for PHRs. Here, we make an effort to simplify key management for both data owners and users by dividing them into separate security domains. The use of multiple authorities in this system ensures that patient privacy is protected.

3.1 IMPLEMENTATION

Cloud Server

In this module, the Server login by using valid user name and password. After login

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

successful he can do some operations such as Authorize PHR User, Authorize PHR Data Owner, Clinical Report, View Patient Details, Access Control Request, Encryption Key Requests, View Key Transactions, and View Result in Chart

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

PHR Owner

In this module, there are n numbers of Owners are present. Owner should register before doing any operations. Once Owner registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful Owner will do some operations like View Profile, Add Patient Details, View Patient Details, View Key Requests, and View Clinical Reports

PHR User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Request Key, View Access Control, View Clinical Reports, and View Patient Details

4.RESULTS AND DISCUSSION

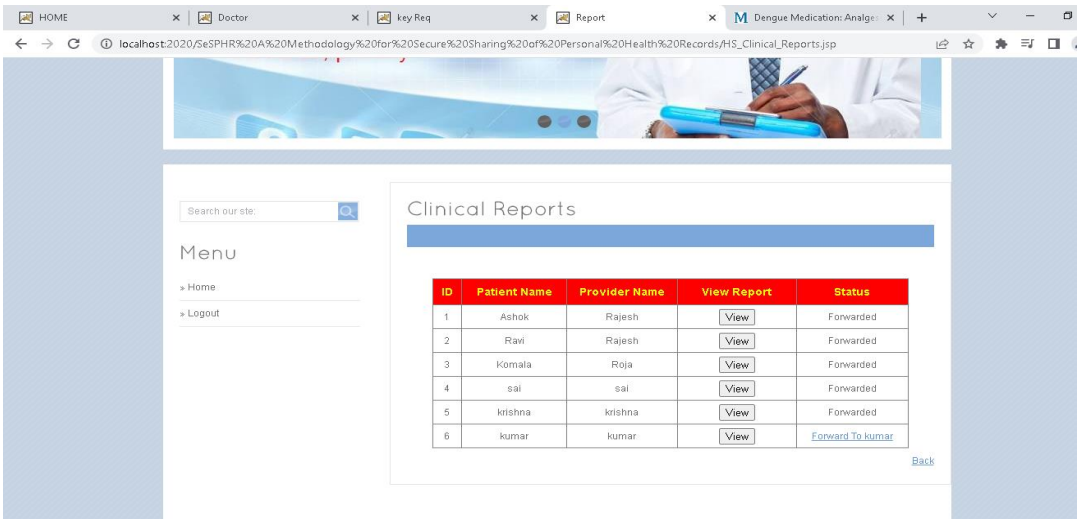

Fig 1:Clinical Report

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

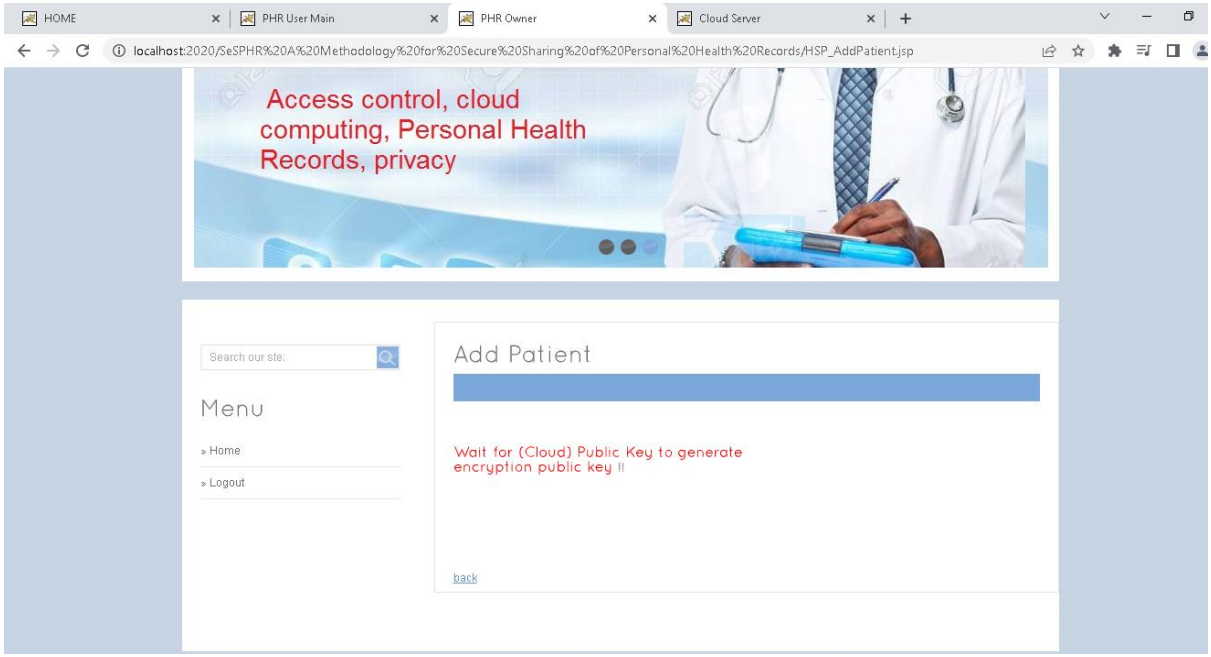

Fig 2:Request for encryption key

5.CONCLUSION

We proposed a method to safely keep PHRs in the cloud and send them to the appropriate parties. This approach ensures that protected health information (PHI) remains private by restricting access to specific sections of PHI based on the permissions granted by individual patients. With the help of a granular method of access control, we made it so that not even legitimate users of the system can view the protected health information (PHI) for which they do not have permission. If a PHR is encrypted and stored in the cloud, only authorised users in possession of valid re- encryption keys issued by a semi trusted proxy will be able to access the data.

A semi-trusted proxy's job is to create and store users' public and private key pairs. Furthermore, the methodology manages forward and backward access control for leaving and joining users, respectively, protecting patient privacy and ensuring PHRs are only accessed by those who need them. Using the HLPN, SMT-Lib, and the Z3 solver, we also formally analysed and verified the operation of the SeSPHR methodology. Time to generate keys, time to perform encryption and decryption operations, and turnaround time were all used to assess performance. The experimental findings prove that the SeSPHR methodology is effective for securing cloud-based PHR sharing.

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

[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. 4344, 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," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work

IEEE Transactions on Cloud Computing, Issue date:10.July.2018 14
sharing (Collaborate Com), 2012, pp. 711-718.

[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.

[7] 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," Journal of Computer and System Sciences, vol. 90, pp, 46-62,2017.

[8] J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI:10.1109/MC.2013.225.

AUTHOR PROFILES

Ms.M.ANITHA completed her Master of Computer Applications and Masters of Technology. Currently working as an Assistant professor in the Department of Masters of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr. EJJIVARAPU NAGARAJU completed his Masters of Computer Applications. He has published A Paper Published on ICT Tools for Hybrid Inquisitive Experiential Learning in Online Teaching-a case study- Journal of Engineering Education Transformations, Month 2021, ISSN 2349-2473, eISSN 2394-1707. Currently working has an Assistant professor in the department of MCA at SRK Institute of Technology, Enikepadu, NTR (DT). His areas of interest include Artificial Intelligence and Machine Learning.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Ms.T.Chandana Priya, as MCA student in the department of MCA at SRK INSTITUTE OF TECHNOLOGY, Enikepadu, NTR(DT). She had completed BSC in SRI DURGA MALLESWARA SIDDHARTHA MAHILA KALASALA. Her areas of interests are Networks, Data Mining, Machine Learning.