YIDDISHVol 4 Issue 01,JAN 2016
ISSN NO: 0364-4308

A Cloud-Based Methodology for Safely Sharing Personal Health Records

Ms. B.Trivenai,Ms. P.Sahithish

#1Assistant professor in the department of AI & IT at DVR & DR.HS MIC College of Technology (Autonomous), Kanchikacherla, NTR (DT)..

#2 MCA student in the department of IT at DVR&Dr.HS MIC College of Technology, Kanchikacherla, NTR(District

Abstract_ Value-effective and simple exchange of private health records (PHRs) across several e-Health system participants is the consequence. However, there is still a need for the development of techniques that guarantee the privacy of PHRs while keeping them on cloud servers, since such data is vulnerable to disclosure or theft. As a result, we propose a method called SeSPHR for safe cloud-based PHR sharing. The SeSPHR concept safeguards PHR privacy and promotes patient-centered PHR management. Patients keep their encrypted PHRs on third-party cloud storage and decide who has access to what elements of the file. To align the public/private key pairs and to give the re-encryption keys, a semi-trusted proxy known as Setup and Re-encryption Server (SRS) is implemented. In addition, the technique enforces both forward and backward access control and is safe against dangers posed by corporate executives. In addition, we use High Level Petri Nets (HLPN) to formally examine and validate the functioning of the SeSPHR technique. Analyses of SeSPHR's performance in terms of time spent show promise for using the approach for secure cloud-based PHR sharing. In addition to the TPA Module for verifying the PHR, we also develop time server, secure auditing storage, in this article as a contribution. in time server PHR Owner add the start and ending time attach to uploaded encrypted files. Our contribution to the initiative is to keep track of any instances of information being hacked or corrupted, so that other hackers and wrongdoers might benefit from the knowledge we provide.Keywords: Access control, cloud computing, Personal Health Records, privacy

1.INTRODUCTION

2. Distributed computing has emerged as a prominent computing paradigm due to its ability to provide constant and on-demand access to a variety of hardware, software, infrastructure, and capacity. The distributed computing model has prompted the use of external information technology (IT) support by encouraging foundations by relieving them of the burden of the prolonged activity of framework upgrading. In addition, the distributed mathematical prototype guarantees the constant availability of health information and its adaptability, and it has shown significantly increased cooperation among a few human services partners. Patients, emergency room doctors and nurses, pharmacists, researchers at academic medical centers, and medical nonprofits are just some of the groups who may benefit from the coordination provided by distributed computing in the healthcare industry. Therefore, patients may easily arrange and manage their Health Records thanks to the development of a financially smart and shared biological system that incorporates newly cited drugs.Similarly, PHRs allow individuals to effectively communicate with their doctors and other care providers to share information about symptoms, seek advice, and maintain up-to-date medical records that may be used for targeted diagnosis and care. Despite the cloud's adaptability, dynamism, efficiency, and comprehensiveness, there are still certain effects to consider in regards to sensitive health data. Concerns about the privacy of patients' health information (PHI) serve an important role. Some legitimate insiders may also pose a threat to the confidentiality of the data. The PHRs stored in the third-party distributed storage should be encrypted to ensure that neither the cloud server providers nor any unauthorised substances may access them. Instead, only those who have earned the 'right-to-know' privilege should be able to see PHRs. In addition, patients should be in charge of the system for granting access to their PHRs, so that no unauthorized changes or misuse of data occur while it is sent to various partners in the health cloud environment. Agents, medication experts, and analysts with medical insurance companies.

3.LITERATURE SURVEY

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

2)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 servers, as long as they do not collude. We then present a generic construction of DS- PEKS using a new variant of the Smooth Projective Hash Functions (SPHFs), whichis of independentinterest.

3) 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 severalsecuritydefinitionsandconstructions havebeenproposed.Inthispaperwe begin byreviewing 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.

4.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.

IMPLEMENTATIONCloudServer

In this module, the Server login by using

valid user name and password. After login 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 adminauthorizes 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 ClinicalReports

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

5.RESULTS AND DISCUSSION

Fig 1:Clinical Report

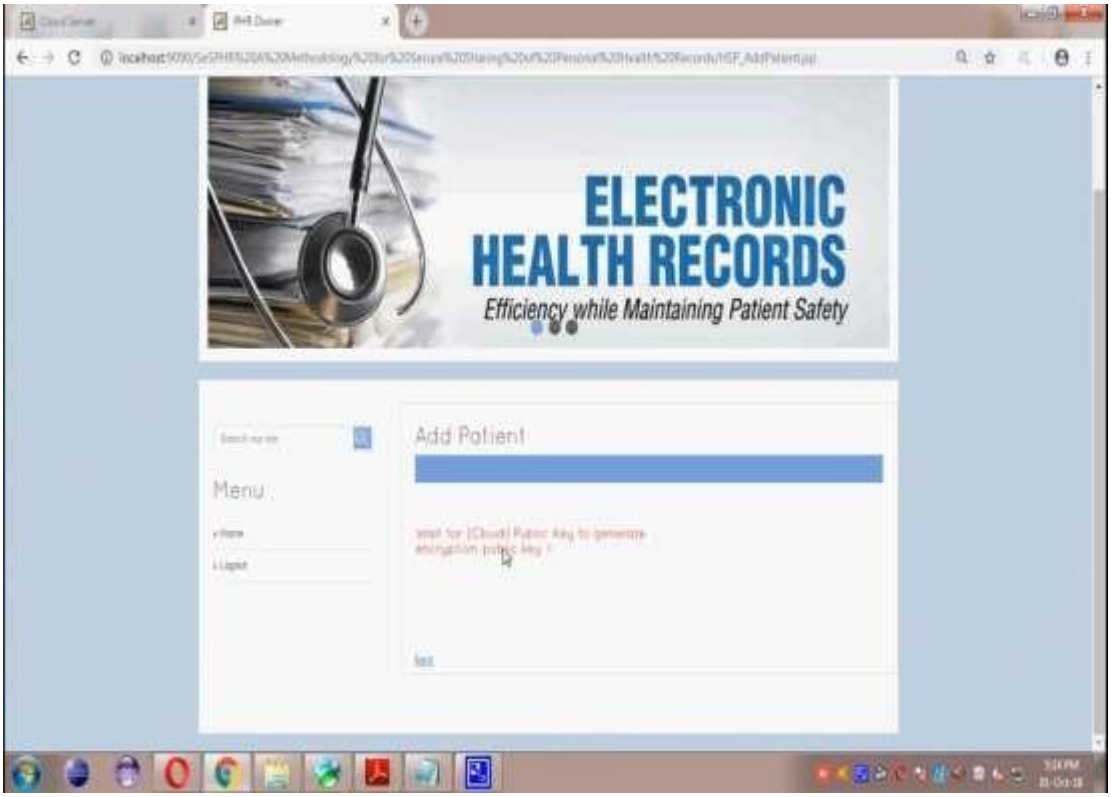

Fig 2:Request for encryption key

6.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 semitrusted 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 forsecuring 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 and

[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 andWork

IEEE Transactions on Cloud

Computing,Issue date:10.July.2018 14

sharing (CollaborateCom), 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.