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

A Procedure for Secure Personal Health Records Sharing over cloud

Nimma Vishali, studentmember,M.Tech (CSE) ,Project guide: G.Chenna Kesava Reddy, M.Tech, Assistant Professor, Srinivasa Institute of Technology and Science, Kadapa.

ABSTRACT

As a result of the broad use of cloud-based services in the healthcare industry, personal health records (PHRs) can now be exchanged between numerous participating entities of e-Health systems in a way that is both affordable and practical. The development of approaches that guarantee the privacy of PHRs is necessary since keeping private health information on cloud servers leaves it open to theft or disclosure. In order to share PHRs securely in the cloud, we suggest a solution we've named SeSPHR. The SeSPHR system offers patient-centered control over PHRs and protects their confidentiality. Patients selectively allow access to various user types on different portions of the PHRs and store the encrypted PHRs on untrusted cloud servers. Setup and Re-encryption Server (SRS), a semi-trusted proxy, is used to create the re-encryption keys and to set up the public/private key pairs. Additionally, the system imposes forward and backward access control and is secure against insider attacks. Additionally, using High-Level Petri Nets, we formally assess and confirm the effectiveness of the SeSPHR methodology (HLPN). A performance study of time usage shows that the SeSPHR methodology has the potential to be used for safely sharing PHRs in the cloud. Additionally, cloud computing integrates a number of significant healthcare domains, including patients, hospital staff including doctors, nurses, and employees at pharmacies and clinical laboratories, as well as service providers, insurance companies, and other healthcare-related organizations.

As a result, a collaborative and cost-effective health ecosystem develops as a result of the integration of the aforementioned entities, allowing patients to easily build and manage their Personal Health Records (PHRs). PHRs typically include information like the following: (a) demographic data; (b) medical history, including allergies, surgeries, and treatments; (c) laboratory results; (d) information regarding health insurance claims; and (e) patient-only notes about specific significant observed health issues.

INTRODUCTION

The widespread and on-demand availability of different resources in the form of hardware, software, storage and infrastructure has made cloud computing a significant computing paradigm. 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, cloud computing also integrates various important entities of healthcare domains namely patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers. Therefore, the combination of the aforenamed entities leads to the development of a collaborative, cost-effective health ecosystem where patients can simply maintain and construct their Personal Health Records. PHRs typically include data on the following topics: (a) demographics; (b) medical history, including diagnosis, allergies, previous surgeries, and treatments; laboratory results; (d) information regarding health insurance claims; and (e) private notes of the patients about specific significant observed health conditions.

More formally, PHRs are controlled by Internet-based tools that allow patients to generate and control lifelong records of their health information that can be made accessible to anyone who requires it. As a result, PHRs give patients the ability to successfully interact with medical practitioners to discuss symptoms, seek guidance, and maintain current health records for proper diagnosis and treatment. Despite the benefits of the scalable, adaptable, affordable, and widespread services provided by the cloud, a number of issues linked to the privacy of health data also come up. Patients' concerns about the secrecy of PHRs are mostly a result of the way that PHRs are shared and stored on the cloud. Private health information stored on cloud servers run by third parties is vulnerable to intrusion.

The privacy of PHRs stored in public clouds run by commercial service providers is extremely risky. Theft, loss, and leakage are just a few of the ways that the PHRs' privacy may be at risk. Because of the harmful actions of outside parties, PHRs that are in cloud storage, being transferred from the patient to the cloud, or being accessed by any other user could be subject to unauthorized access. Additionally, some legitimate insiders have made threats against the data. For instance, because of the nefarious actions of external entities, PHRs that are stored in cloud storage, transferred from the patient to the cloud, or transferred from the cloud to another user may be vulnerable to unauthorized access. Additionally, there are occasional threats made against the data by valid insiders. The individuals working at the cloud service provider have the potential to behave maliciously. One well-known instance of that is the event in which a U.S. Department of Veterans Affairs employee took home the personal sensitive health information of almost 26.5 million veterans without authority. The Health Insurance Portability and Accountability Act (HIPAA) requires that the confidentiality and integrity of electronic health information kept on file by healthcare providers be secured by the terms and conditions of use and disclosure, as well as with the consent of the patients. The PHRs should be accessible only to those organizations or people who have the "right-to-know" privilege. To further prevent any unauthorized changes or misuse of data when it is transferred to the other stakeholders in the health cloud environment, the PHR access mechanism should be managed by the patients themselves. The privacy of PHRs stored on cloud servers has been ensured using a variety of techniques. The privacy-preserving techniques ensure audit trial, accountability, integrity, and confidentiality.While integrity focuses on preserving the originality of the data, whether in transit or cloud storage, confidentiality ensures that the health information is completely hidden from unauthorized parties. Accountability refers to the requirement that data access regulations follow the established protocols, whereas authenticity ensures that the health data is only accessed by authorized parties. The term "audit trial" refers to the process of keeping tabs on how health data is being used even after access has been given. We offer a way for managing 1the PHR access control system that is controlled by patients themselves, called Secure Sharing of PHRs (SeSPHR) in the Cloud.

By preventing unauthorized users from accessing PHRs, the approach protects their confidentiality. In the suggested approach, there are typically two main categories of PHR users: (a) PHR owners or patients (b) users of PHRs other than owners, such as patients' family members or friends, physicians, health insurance company representatives, pharmacists, and researchers. By selectively providing people access to various PHR sections, patients who are the PHRs' owners are allowed to upload encrypted PHRs to the cloud. Depending on their role, each member of the group of users of the later type is granted access to the PHRs to a particular level by the PHR owners. Similarly, insurance company representatives would only be able to see the PHR sections that contain information concerning health insurance claims, with access to other personal medical information, such the patient's medical history, being blocked for these users.By giving the SRS the responsibility of creating the public/private key pairs and issuing the decryption keys to only the authorized users, the SeSPHR methodology avoids the overhead. This strategy saves overhead by proposing that PHR owners produce the decryption keys, in contrast to the technique suggested in [10], which advises that they manage numerous keys. In the end, the PHR owner will incur overhead. Since the cloud servers are seen by the approach as an untrusted entity, the Setup and Re-Encryption Server (SRS), a semi-trusted server, is employed as the proxy. An approach based on proxy re-encryption is used by the SRS to produce the re-encryption keys for the safe exchange of PHRs across users. Only authorized users with keys supplied by the SRS can decode PHRs that have been encrypted by patients or PHR owners. Additionally, the users are given access to the PHRs' specific sections that the PHR owner deems to be crucial. The proposed method is secure compared to other constructs since the PHR data is never sent from the SRS in the proposed framework. The proposed approach also enforces forward and reverse access control. Newly added members of a particular user group receive a key from SRS. Shared data is encrypted with only the owner's key. Access to the data of new members will be granted after the consent of the PHR owner. Similarly, the resigning user is removed from her ACL and the key corresponding to that user is deleted. Deleting the user keys and removing them from the ACL will deny access to the PHR for unauthorized access attempts after the user leaves.We also performed a formal analysis of the proposed schema using High Level Petri Nets (HLPN) and his Z language. HLPNs are not only used to mimic systems, but also provide mathematical properties that are used to study system behavior. Validation is done using the Satisfiability Modulo Theories Library (SMT-Lib) and the Z3 Solver. Validation tasks using SMT are accomplished by first converting the Petri net model to SMT with specific properties and then using her Z3 solver to determine if the properties hold. The main contributions of the proposed research are listed below.

• Presents a method called Her SeSPHR that allows patients to manage their sharing of her PHR in the cloud. • PHR secrecy is guaranteed through the SeSPHR methodology's usage of proxy re-encryption and El Gamal encryption. • Using user groups listed in her ACL that have varying access levels, the PHR owner can utilize this strategy to provide users access to specific PHR sections only. The suggested methodology additionally incorporates forward and reverse access control and deploys a semi-trusted proxy named SRS to offer access control and create re-encryption keys for different user groups, removing the PHR owner's burden of key maintenance. • To ensure that the suggested approach is operating in accordance with specification, a formal analysis and validation is carried out. This essay is structured as follows. El-Gamal encryption and proxy re-foundational encryption's ideas are introduced in this section. SeSPHR is a proposed methodology that is discussed in section along with a presentation of the proposed methodology itself. In section, the proposed technique is given a formal study and evaluation. The section that follows summarizes the work's findings from the experiment.

EXISTING SYSTEM

- A variety of techniques have been used to guarantee the privacy of PHRs kept on cloud servers. The privacy-preserving strategies ensure accountability, authenticity, and audit trials as well as confidentiality and integrity. Integrity deals with preserving the originality of the data, whether in transit or in cloud storage, whereas confidentiality ensures that the health information is completely hidden from the unapproved parties.
- Accountability means that the data access policies must adhere to the established protocols, while authenticity ensures that the health data is only accessed by authorised parties. Audit trials are used to

keep track of how health data is being used even after access has been given.

Disadvantages

- The system doesn't implement El-Gamal encryption which is effective to secure data.
- There is no dynamic data integrity proof instead manual.

PROPOSED SYSTEM

In order to handle the PHR access control mechanism that patients themselves manage, the proposed system proposes a methodology termed Secure Sharing of PHRs in the Cloud (SeSPHR). By limiting unauthorized users, the technique protects the confidentiality of the PHRs.

According to the proposed methodology, PHR users can be divided into two groups: (a) patients or PHR owners; and (b) users of PHRs who are not the owners, such as patients' family or friends, medical professionals, representatives of health insurance companies, pharmacists, and researchers.

Patients who are the PHR owners are allowed to upload encrypted PHRs to the cloud by giving users just limited access to certain PHR sections. The levels of access granted to various categories of users are defined in the Access Control List (ACL) by the PHR owner.

Benefits

- Using a method provided by the system known as SeSPHR, patients can manage how their personal PHRs are shared in the cloud.
- The SeSPHR approach enables PHR owners to deliberately grant users access to the sections of PHRs by using the access level described in ACL for distinct user groups.
- Depending on the access level established in the ACL for various user groups, the PHR owners can use the SeSPHR method to selectively provide users access to PHR regions. The SeSPHR technique uses both proxy re-encryption and El-Gamal encryption to safeguard PHR secrecy.

LITERATURE SURVEY

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.

Edge computing, cloud computing, and Internet of Things are just a few of the techniques that are being combined in a connected world (IoT). Throughout the data transmission process, privacy issues have surfaced, some of which are brought on by the communication protocols' lax security. Due to increased compute workloads and communication manipulations, high security protection systems in practice typically call for a more powerful computing resource. When data sizes get huge, it becomes harder to implement high security communications.

This study focuses on the topic of the tension between privacy protection and effectiveness and suggests a novel method for delivering higher-level security transmission via multi-channel communications. To assess the efficacy of the suggested strategy, we use experiment evaluations.

2) K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," Journal of Network and Computer Applications, 2017, pp. 1-12.

FinTech, a relatively new phrase in the financial sector, has gained popularity as a way to define cutting-edge technologies used by financial service providers. This phrase encompasses a broad range of methods, including data security and the provision of financial services. Both academics and professionals have an urgent need for an accurate and current understanding of fintech. A theoretical, data-driven FinTech framework is provided in this article, which aims to generate a survey of the field by compiling and reviewing recent accomplishments. These five technical areas—security and privacy, data approaches, hardware and infrastructure, applications and management, and service models—are summarized and involved. The principles of creating active FinTech solutions are the study's primary conclusions.

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.

The recently developed idea of a "Health Insurance Marketplace" that makes it easier to purchase health insurance by comparing various insurance plans' costs, benefits, and quality gives health insurance providers a significant role. The web-based tools for finding health insurance policies currently do not provide adequate suggestions based on the costs and benefits of the coverage. In order to provide individualized suggestions about health insurance plans, we provide a cloud-based framework in advance of the consumers' needs. Using coverage and cost factors like (a) premium, (b) co-pay, (c) deductibles, (d) co-insurance, and (e) maximum benefit provided by a plan, we employ the Multi-attribute Utility Theory (MAUT) to assist users in comparing various health insurance plans. We provide a consistent representation for the health insurance plans to address the problems that may result from the heterogeneous data formats and various plan representations used by the providers. Using the Data as a Service, the plan details for each of the providers are retrieved (DaaS). By employing a rating technique for the detected plans in accordance with the user-specified criteria, the framework is implemented as Software as a Service (SaaS) to provide tailored recommendations.

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.

Cloud computing aims to provide reliable, customized, and quality of service (QoS) guaranteed dynamic computing environments for end-users. However, other applications, like e-health and monitoring emergency response, require low latency and quick response. Delays caused by transferring data over the cloud can seriously affect the performance and reliability of real-time applications. Before outsourcing e-health care data to the cloud, the user needs to perform encryption on these sensitive data to ensure its confidentiality. Traditionally, any change to the user data necessitates encrypting the entire data set and creating a new hash value for the data. The cost of communication and computation over the cloud is increased by this data modification process. Fog computing uses a distributed environment to get around some of the drawbacks of cloud computing. For the purpose of sharing e-health data in fog computing, this study presented the certificate-based incremental proxy re-encryption system (CB-PReS). The updated, deleted, and inserted file actions are all improved by the suggested technique. The iFogSim simulator is used to test the proposed method. The iFogSim simulator makes it easier to create models for fog and IoT environments and evaluates how resource management strategies affect network latency and congestion. Experiments depict that the proposed scheme is better than the existing schemes based on expensive bilinear pairing and elliptic curve techniques. The proposed scheme shows significant improvement in key generation and file modification time.

5) 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.

A potential system called the Personal Health Record (PHR) has been created to enable very efficient interactions between patients and clinicians. Although cloud computing has been considered a leading contender to store PHR's sensitive medical records, the security measures are still insufficient without negatively affecting the system's usability. In this study, we offer a broad architecture for the secure sharing of PHRs as a solution to this issue. Our system enables patients to safely store and share their PHR in the cloud server (for example, with their caregivers). In addition, the treating physicians can, as needed, refer the patient's medical record to specialists for research while maintaining the confidentiality of the patient's information. Additionally, our technology facilitates cross-domain operations (e.g., with different countries' regulations).

MODULES OF PROJECT

Cloud Server

The server login in this module requires a valid user name and password. After successfully logging in, the user can do a number of actions, including authorizing PHR users and data owners, viewing clinical reports, viewing patient details, access control requests, requesting encryption keys, viewing key transactions, and viewing results in charts.

View and Authorize Users

The list of people who have registered can be seen by the administrator in this module. The admin can examine the user's information in this, including user name, email address, and address, and admin can also authorize users.

PHR Owner

There are 'n' numbers of Owners present in this module. Before beginning any operations, the owner needs to register. Once an Owner registers, the database will record their information.After successfully registering, he must log in using an authorized username and password. Once logged in, the owner can perform a number of actions, including seeing their profile, requesting a key, viewing access controls, viewing patient details, and clinical reports.

PHR User

There are 'n' numbers of users present in this module. Before doing any operations, the user should register. Once a user registers, the database will record their information. After successfully registering, he must log in using an authorized user name and password. Once logged in, the user can perform a number of actions, including seeing their profile, requesting a key, viewing access controls, viewing clinical reports, and viewing patient information.

CONCLUSION

We proposed a mechanism for transmitting and storing PHRs in the cloud securely to authorized parties. This technique preserves a patient-centric access control to various PHR subsystems based on the access granted by the patients, maintaining the confidentiality of the PHRs. We put in place a form of fine-grained access restriction so that not even authorized users of the system could access restricted areas of the PHR. Only authorized users with legitimate re-encryption keys supplied by a semi trusted proxy are able to decrypt PHRs, which are stored encrypted by PHR owners in the cloud.The semi-trusted proxy's task is to generate and preserve the public/private key pairs for the system's users.

The technique also manages forward and backward access control for leaving and incoming users, respectively, in addition to maintaining confidentiality and ensuring patient-centric access control across PHRs. Additionally, we formally assessed and validated the SeSPHR methodology's operation using the HLPN, SMT-Lib, and Z3 solver. The time it took to generate keys, the activities involved in encryption and decryption, and turnaround time were all taken into account when evaluating performance. The outcomes of the experiment show that the SeSPHR methodology may be used to safely exchange PHRs in a cloud context.

BIBLIOGRAPHY

[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. 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] 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,” 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.Kamara and K.Lauter, “Cryptographic cloud storage,” Financial Cryptography and Data Security, vol. 6054, pp. 136–149, 2010.

[10] 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.

[11] 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.

[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.

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.