A Novel Approach towards Secure Sharing of Electronic Health Records

A.Sendhooran, D.Subosan, S.Satheesh Kumar, G.Vijay, M.Nanthini
Department of CSE
K.Ramakrishnan College of Technology

Abstract:
In recent trends, Healthcare providers are willing to shift their Electronic Health Records (EHR) to the cloud that has several advantages including lower operational cost and better interoperability with the other health care providers. However, the adaptation of cloud technologies raises issues related to security and associated challenges including authentication, identity management and so on. Hence in this study, We propose a novel scheme that ensures the confidentiality of the health records. The encrypted EHR's are stored on cloud servers and are given selective access to varied users based on the applicability. The scheme proposes a semi-trusted proxy and Re-encryption server is introduced. Further, the analysis and the verification of the methodology is done using High-Level Petri Nets that adds to the novelty of the proposed method.

Keywords: *Cloud Computing, Personal Health Records, Data Security, Secure Storage.*

I. INTRODUCTION

Cloud Computing is one of the advanced technology used for storage purpose. In order to increase the mobility in storage, we use a cloud. In cloud storage, we can access the data from any place in and around the world. It also provides security and privacy for the data stored in the cloud. It reduces the storage in a particular device and it makes the data stored on the internet. It reduces the storage cost of data and securing the data. It also plays a vital role in a lot of fields such as medical, military, education, etc. In the medical field, it is necessary to share the patient details from the doctors' side as the patients from the far distance can also continue their existing treatment in any country. But when a user shares the patient's history, the data can be accessed from the cloud side or while user upload data to the cloud by the anonymous user. In order to secure this data, we use encryption and decryption by using web services for a particular hospital as the other users and even other doctors cannot access these data without the permission of the particular organization. The data are encrypted in the web service and the encrypted data are uploaded to the cloud. When the doctor needs the data uploaded by another doctor, a request is sent to the uploaded doctor and when the request is accepted, the encrypted data is downloaded and then decrypted in the web service. The request is accepted with two permissions such as Read-only and Read-write permission. With Read-only permission, the person can only view the data and with reading write permission, the person can view and modify the data. Without the web service, the data cannot be decrypted. To encrypt and decrypt the data, we use RSA (Rivest Shamir Adleman) algorithm as it makes public key encryption and it is broadly used to secure sensitive data while the data is sent over internet. The web services differ from organization to organization in order to provide privacy to the particular organization. So, this provides confidentiality of the data to the patients and the doctors.

II. PROBLEM IDENTIFICATION

The sensitive Personal Health Information(PHI) is a candidate for attacks by hackers, especially when the records are stored on a third-party server.These third-party servers are not trusted by people as they fear hacking. On the one hand, there exist Healthcare regulations such as HIPAA (Health Insurance Portability and Accountability Act of 1996) which is recently amended to incorporate business associates. Sensitive PHI data are of high value in the market, and hence the third-party storage servers are often used as the targets of various malicious activities which may lead to exposure of PHI. To ensure the Patient-oriented privacy control over their own PHRs, it is importantthe access control mechanisms are tweaked such that they work with the semi-trusted servers. The authorized users may never have to access the PHR for personal use or professional purposes. If the owner has to manage the access of PHR for professional purpose themselves, they will easily be overwhelmed by the key management overhead as the possibility of the usage scale is very high.

III. LITERATURE SURVEY

In this paper, the outsourced data can be made secure by using a novel approach of Re-encryption method. To get detailed access control, the traditional public key encryption-based schemes can be used. In order to improve scalability one-to-many encryption and re-encryption methods are used. This approach has the potential to make encryption and key management more efficient. A fundamental

property of ABE (Attribute-based Encryption) is preventing against user collusion.

This methodology preserves the confidentiality of the PHRs and enforces patient-oriented access control to different portions of the PHRs based on the access provided by the patients [1]. We implemented a detailed access control method in such a way that even the valid system users cannot access the part of the PHR for which they are not authorized [1]. The PHR owners store the encrypted data on the cloud.The authorized users who possess a valid re-encryption keys issued by a semi-trusted proxy only are able to decrypt the PHRs [1]. The semi-trusted proxy is responsible for generating and storing the public/private key pairs for the users in the system [1].

Based on the time consumed to generate keys, encryption and decryption operations, and turnaround time, the performance evaluation was done. [1]. The experimental results prove that the SeSPHR methodology is viable to securely share the PHRs in the cloud environment [1]. In cloud storage, users can store their data in remote servers rather than their local computers [2]. Secure storage is used to make ensure the data is safe in clouds. Encryption based approaches are commonly used in secure storage systems [2].

Data are encrypted and stored in persistent storage like disks and flash memories [2]. When the data are needed by users, they are decrypted and accessed by the users [2]. Meanwhile, the cloud systems mustapply a fault tolerance strategy on the data, which also brings the performance deduction [2]. All these factorscause a high price for data security in the cloud systems [2]. So, we propose methods to reduce the overhead of secure storage while guaranteeing the safety of data [2]. To address these concerns, we have to propose an approach to provide scalable security for the data on storage systems [2].

We design a nominal encryption scheme to minimize the overhead of the encryption [2]. In this paper, we present the CamFlow (Cambridge Flow Control Architecture) [3]. CamFlow's IFC model comprises a new operating system level implementation of IFC.It is a Linux Security Module (LSM), which supports application management, together with an IFC enabled middleware [3]. IFC has proposed to guarantee safe usage of the data by the social network applications [3]. The aim is to give a purpose-based disclosure through IFC between secluded components.This guarantees that shared data can only be used for a well-defined and agreed upon purpose [3].

We presented a new kernel implementation of IFC as an LSM. It demonstrated the low overhead for worst-case scenarios where processes continuously make read/write system calls.This makes cloud adoption feasible [3]. In this paper, we investigated a new primitive called identity based remote data integrity checking for the secure cloud storage [7]. Cloud computing brings a number of benefits for cloud users [7]. This new computation model represents the new vision of providing computing services as public utilities like water and electricity [7].

We structured the security model of the two important properties, namely, soundness and the perfect data privacy [7]. We provided a new construction of this method and showed that it achieves soundness and perfect data privacy [7]. Both theoretical numerical analysis and implementation demonstrated that the proposed protocol is efficient and practical [7]. Cloud computing is a new phenomenon which is used in all areas in today's life [4]. It is cost-effective, fast and easily available tool in the market [4]. The security is very important in it [4]. Many of the government and private agencies are working on the security aspect of the cloud [4]. More and more security needs to be achieved and one day cloud will the preferred area to store, retrieve, use and process the data securely [4]. In this paper, all the models of cloud, various security issues, and aspects to provide the security have been discussed [4]. As the development and research in the cloud is in early stage, it is not possible to achieve the complete security now. by finding the new ways for security and by sharpening the older techniques in the cloud, it can be achieved sooner. [4]. In this paper, we propose a lightweight data sharing scheme (LDSS) for the mobile cloud computing [12].

It adopts CP-ABE, an access control technology used in the normal cloud environment.The structure of the access control tree is changed slightly to make it suitable in mobile cloud environments [12]. First, when people upload their data files into cloud, they are leaving the data in a place where it is not in their control. CSP may spy on the data to make money or for other reasons [12]. However, doing this require a fine-grained access control [12].

To solve the above problems, personal sensitive data should be encrypted before it is uploaded into the cloud so that the data is secure against the CSP [12]. This mechanism needs a centralized Key Distribution Centre also known as KDC.It is responsible for distributing and maintaining attributes and secret keys to its users [5].

The security in these security systems suffers a vulnerability when one user requests for the sharing

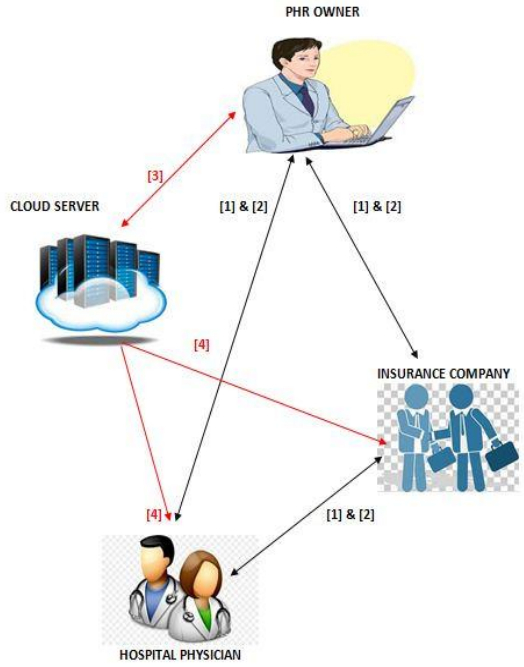
of data of some user [5]. The aim of recognizing the risks involved in data sharing in the cloud environment enables improvements in data security, data integrity, data anonymity and user privacy [5]. We have also proposed a system improvement for the same [5]. The proposed system is expected to improve security levels further in cloud computing and storage [5]. In this paper, we propose a novel server less message-locked integrity auditing scheme for encrypted reduplication storage [14].

Our design is very suitable for the outsourcing model.From this model each participant can reap the benefit [14]. For cloud users, this model offers the data confidentiality and integrity guarantees andincurs minimal computation overhead [14]. On the other hand, the cloud can still utilize the reduplication technique to reduce its operating cost [14]. The security analysis shows that our scheme is definitely secure under the CDH assumption in the random oracle model [14]. Experimental results demonstrate its efficiency, effectiveness, and practicality [14].

IV. PROPOSED SYSTEM

The outsourced data can be made secure by using a new approach of Re-encryption method.In this a web service is usedto provide privacy for the user. To getmaximum access control, the traditional public key encryption-based schemes can be used as the cryptographic method. The third-party storage servers are often used as the targets of various malicious activitiesthat may lead to exposure of PHI due to the high value of the sensitive PHI. To make sure the Patient-oriented privacy control over their own PHRs, it is important to have the maximum data access control mechanisms that work with the same trusted servers. In order to improve upon scalability one-to-many encryption and re-encryption methods are used to provide security. The scheme proposes the storage of the PHRs on the cloud by the PHR owners.The owner can subsequently share with other users in a secure manner. The cloud is assumed as the interested entity and the users can upload or download PHRs to or from the cloud servers. As per the proposal, the cloud resources are utilized only to upload and download the PHRs, therefore, no changes are required to be made to the cloud. The authorized users are not required to access the PHR for personal use or professional purposes. This possibly makes the encryption and key management more efficient for the user. A fundamental property of ABE (Attribute-based Encryption) is preventing against user collusion.

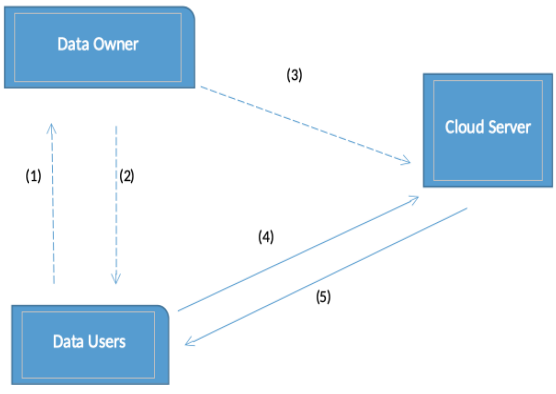
V. ARCHITECTURE



[1]. Obtain attributes
[2]. Provide write keys
[3]. Outsourced encrypted PHR
[4]. Access Data

VI. USER DIAGRAM

(1)Obtain attributes
(2)Provide write keys
(3)Outsourced encrypted PHR
(4)Write Data
(5)Read Data



VII.METHODOLOGY

Here we try to study a PHR system where there are multiple PHR owners and PHR users. The owners might be patients who have complete access control over their own PHR data. Here they can generate, maintain and delete the PHR data. There is

a server that belongs to the PHR service provider.They store all the owners' PHRs data. The usersdata may come from various fields; for example it may come from a friend, a researcher or anyone. Here users try to access the PHR records through the server. They try to read or write to someone's PHR. Also, users have the right to access multiple owners' data. Following are the 3 phases:

A. Preventing Unauthorized Access: It is an important requirement.Efficient PHR access is to enable "patient-oriented" sharing. It implies that the patient should have all the control over their personal health record. They mustcontrol which users shall have access to their medical record. User controlled read-write access and reversal is the two main security objectives or concerns for any electronic health record model. User controlled write access control in a PHR system specifies the prevention of unauthorized users to access the records and modifying it.

B. Fine-Grained Access Control: Fine-grained access control should be used in a way that different users are allowed to read different sets of documents. The main objective of our model is to provide secure patient-oriented PHR access and efficient key management at the same time. Whenever a user's attribute is no longer appropriate, the user need not be able to access further PHR files using that same attribute.

C. Attribute Revocation: The PHR system should let users from both the personal domain and public domain. Since the groups of end users from the public domain may be huge in size and indeterminate, the system should be scalable.It should be able to manage the complexity in key management, communication, computation, and storage too. Also, the owners' difficulty in governing users and keys should be reduced to improve usability.

VIII. ENCRYPTION METHOD

In cloud computing, there are different current techniques that provide security, data confidentiality, and access control. Here users need to provide their sensitive information with other users based on the receiver's ability to achieve policy in distributed systems. One of the encryption schemes is Attribute-Based Encryption (ABE).This is a new technique where policies are labelled and cryptographically enforced in the encryption algorithm itself. Hence, the existing ABE schemes are two types. They are Key- Policy ABE (KP-ABE) scheme and the Ciphertext-Policy ABE (CP-ABE) scheme. Encryption techniques for personal health records in cloud computing literature review as follows:

IX. ATTRIBUTE-BASED ENCRYPTION

Attribute-Based Encryption (ABE), is a simplification of identity-based encryption that includes attributes as inputs to its cryptographic primitives. Data is encrypted with a set of attributes so that other users who gain proper keys can decrypt. Attribute-Based Encryption (ABE) not only offers fine-grained access control but it also averts against the collision. Here to implement fine-grained access control, the traditional public key encryption based methods encounter high key management overhead, or need encrypting copies of a file with a different set of users keys. To progress upon the compliance of the above solutions, encryption methods such as attribute-based encryption (ABE) can be used. The main objective of these models is to provide security and access control. The main feature is to provide flexibility, scalability and fine-grained access control. In the classical model, this system can be attained only when user and server are in a trusted domain. So, the new access control scheme that is "Attribute-Based Encryption (ABE) " scheme is introduced.This consist of the key policy attribute-based encryption (KP-ABE). As compared with the classical model, KP-ABE provided fine-grained access control. However, it fails with respect to the flexibility and scalability when the authorities at multiple levels are considered. In ABE scheme both the user secret key and the ciphertext are associated with a set of attributes. ABE is implemented for one-to-many encryption.In this case the cipher-texts are not essentially encrypted to one particular user, it may be for more than one number of the users.

X. AES & SHA ALGORITHM:

A lot of extensive and widely adopted trigonal encoding formula possible to be encountered today is that the Advanced encoding normal (AES). It's found to be a minimum of six time quicker than triple DES.

A replacement for DES was required as its key size was too tiny. With growing computing power, it undeniably was thought-about susceptible against thorough key search attack. Triple DES was planned to beat this downside.But it surely was found to be slow.

Till date, no sensible cryptographic attacks against AES has been discovered to boot. AES has basically flexibility of key length, that permits a degree of 'future-proofing' against progress within the capability to perform thoroughgoing key searches.

However, even as for DES, the AES security is guaranteed given that it's properly imposed and smart key management is used.

SHA-1 or Secure Hash formula one could be a science hash perform that takes AN input and

produces a 160-bit (20-byte) hash price. This hash price is thought as a message digest. This message digest is sometimes then rendered as a positional representation system range that is forty digits long. It is a U.S. Federal informatics normal and was designed by the U.S. National Security Agency.

XI. EXPERIMENTAL GRAPH:

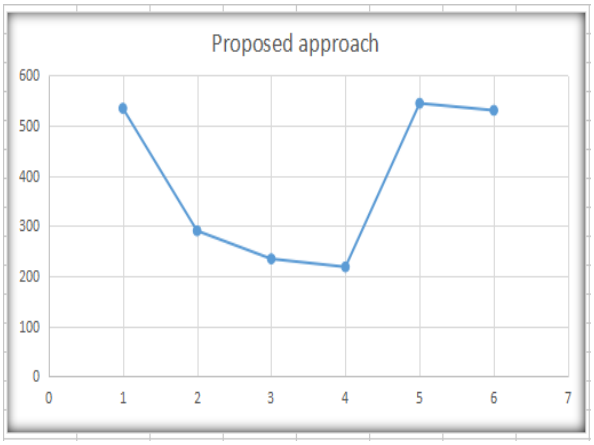
In experimental work, we incline to check the theory and live visible quantities. Often, we tend to add plot graphs to prove anassociation between the results and our theory.

A graph plots the link of 1 amount compared to another on 2 axes at right-angles to every alternative. Usually, we've succeeded over one in all the quantities and this is often called the variable quantity, the opposite amount is set by the result of the experiment or some mathematical relationship. we tend to decide this the variable quantity because of it depends on the variable quantity. we tend to typically plot the variable quantity on the coordinate axis and therefore the dependent variable on the coordinate axis.

XII.ENCRYPTION PROCESS

To show the performance of proposed approach, encryption execution time is reported in figure 1 and table 1. In this diagram the X axis shows the different experiments on which we run different files as an input and the Y axis shows the amount of time consumed for encrypting the input text file.

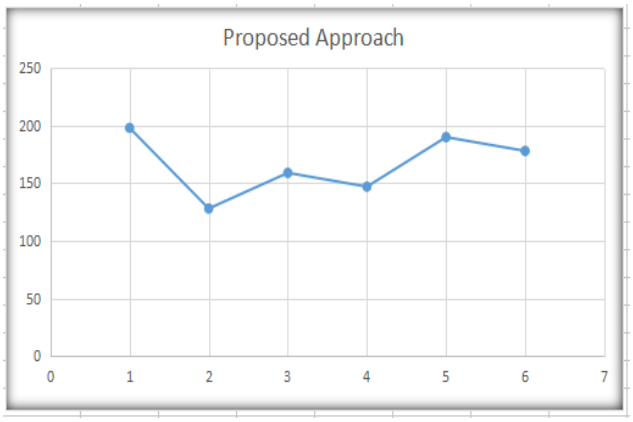
Number of Experiments	posed approach
1	534
2	290
3	234
4	218
5	544
6	530



XIII. DECRYPTION PROCESS

X-axis shows the different numbers of experiments are performed and the Y-axis shows the amount of time consumed for decryption process. According to the generated results the encryption time is higher than the decryption time in the system, but the decryption time of the proposed algorithm is much adaptable and after secure sharing user can be downloaded in their system.

Number of Experiments	Proposed Approach
1	198
2	128
3	159
4	147
5	190
6	178



XIV. CONCLUSION

A structure of securely sharing of personal health records has been proposed in this paper. Bearing in mind partially trustworthy cloud servers, we know that to fully deploy the patient-status concept, the patient's need complete control over their own privacy. Attribute-Based Encryption is a decent technique for securing Health records. It is efficient in the Conjunctive Property. We utilize Attribute-Based Encryption to encrypt the Health record data so that patients can allow access not only by personal users but also various users from public domains with different professional roles, qualifications, and affiliations. The system is improved to support dynamic policy management model. Thus, Personal Health Records is maintained with security and privacy.

REFERENCES

[1] Mazhar Ali, Assad Abbas, Muhammad smanUShahidKhanandSameeU.SeniorKhan, "SeSPHR:A Methodology for Sec of Personal Health Records", IEEE Transactions on Cloud Computing 2018.

[2] Longbin Chen, Wenyun Dai, MeikangQiu, Ning Jiang, "A Design for Scalable and Secure Key-value Stores" IEEE International Conference on Smart Cloud 2017.

[3] Thomas F. J.M. Pasquier, Jatinder Singh, Member, IEEE, David Eyers, and Jean Bacon Fellow, "CamFlow: Managed Data-sharing for Cloud Services" 2017 IEEE Transactions on Cloud Computing.

[4] Mrs. VarshaAnupJujare, "Cloud computing: Approach, Structure and Security", Proceedings of the Second International Conference on Computing Methodologies and Communication 2018.

[5] Prof. N. C. Thoutam, Kadam Prasad, JadhavPoonam, KhupaseGauri, "Data Sharing Security and Privacy Preservation in Cloud Computing", 2016 International Conference on Green Computing and Internet of Things.

[6] Songyang Wu, Yong Zhang, "EFFICIENT VERIFICATION OF DATA POSSESSION IN CLOUD COMPUTING", Proceedings of CCIS 2016.

[7] Yong Yu, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 12, NO. 4, APRIL 2017.

[8] ChetanGudisagar, BibhuRanjanSahoo, Sushma M, Jaidhar CD, "Secure Data Migration between Cloud Storage Systems", IEEE2017.

[9] WenqingTian, HengXu, MessanKomi, and Junxing Zhang, "Secure and Flexible Data Sharing via Ciphertext Retrieval for Cloud Computing", IEEE 2016.

[10] RuixuanLi,ChenglinShen, Heng He, ZhiyongXu, and Cheng-ZhongXu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing" IEEE Transactions on Cloud Computing 2016.

[11] RajatSoni, SmruteeAmbalkar, Dr.PratoshBansal, "Security and Privacy in Cloud Computing", Symposium on Colossal Data Analysis and Networking (CDAN) 2016.

[12] Ruixuan Li, Member, IEEE, ChenglinShen, Heng He, ZhiyongXu, and Cheng-Zhong Xu, Member, IEEE, *"A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing",*IEEE TRANSACTIONS ON CLOUD COMPUTING, 2016.

[13] Rizwana A.R. Shaikh, Masooda M. Modak, "Measuring Data Security for a Cloud Computing Service", IEEE2017.

[14] Xuefeng Liu, Wenhai Sun, Wenjing Lou, Qingqi Pei, Yuqing Zhang, "One-tag Checker: Message-locked Integrity Auditing on Encrypted Cloud Deduplication Storage", IEEE Conference on Computer Communications IEEE INFOCOM 2017.

[15] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, "Study on Data Security Policy Based On Cloud Storage", 3rd International Conference on Big Data Security on Cloud, IEEE 2017.