ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

A Securable and Sharing Health Records in A Cloud Using Cryptographic Technique.

Jesila Mol J*.

Faculty of Computing, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

Technology development provide personal health record (PHR) as a patient-centric model where information about health is been exchanged. Through cloud all personalized records are given to the third parties. But that is not sure to tell that our records are kept in a safe area, because they are not fully protected. In cloud storage secured PHR access, are the most important risk to achieving, cryptographically implement data access control. In this paper, propose a unique patient-centric frame work and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. This paper propose ABE-based framework for patient-centric which is highly securable and sharable of PHRs in cloud computing environments, under the multi owner settings. This divide the users in the system into two types of domains, public and personal domains (PSDs) to address the key management.

Keywords: Cloud Computing, Personal Health Record, Multi-Authority, Secret key and Attribute based Encryption.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

As cloud computing becomes prevalent, and more sensitive information are been centralized into the cloud, such as personal mails,patients health details, government documents, etc. it is been often used in our day to day happenings. Recently, personal health record (PHR) has arisen as a patient-centric model where information about health is exchanged. It allows a patient to create, manage, and control their own personal health data in one place through the web, which has made the retrieval, sharing, and storage of the medical information more efficient. Each patient has promised to control their own medical records and can share their health data among their users, including family members, friends, or healthcare providers. Many PHR services are outsourced to or provided by third party service provider to building and maintaining specialized data centers. Many security and privacy risks are available in PHR services wide adoption. Third party storage server are often targeted by various malicious behaviors since third party service providers of personal health information (PHI) obstruct main concern to the patient as they may not fully trusted so that this may lead to exposure of PHI. Encrypting the data before outsourcing would be the most feasible and promising approach. Encryption of files and access security to users both are decided by the PHR owners. User with corresponding decryption key can access PHR file can be accessed only to the user, while rest of users remains confidential. Patient can grant and revoke access privileges when it is required. The authorized users may either need to access the PHR for personal use of professional purpose. Example of the former is family members and friends while the later can be doctors, and researchers, etc. This paper may conclude to two categories personal and professional users' respectively. In order to protect personal heath data stored on semi trusted servers, this adopts attribute based encryption (ABE) as the main encryption technique. Using this method, patient can choose the person to share their PHR among set of users by encrypting files under a set of attributes without knowing complete list of users. To implement the ABE into large scale PHR system had issues such as scalability of key generation, dynamic updates of patient details and efficient revocation are nontrivial to solve and remains largely up-to-date. Data's been stored are saved in encrypted format using public key encryption. It provides less security to the data's.

PROPOSED SYSTEM

In this paper expressed a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing system, under the multi- owner processing. To address the key management threat, ABE conceptually divide the users in the system into two types of domains, namely public and personal domains. In the public domain, it use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Proposed a multiple-authority ABE (CC MAABE) solution in which multiple TAs, MA-ABE scheme is used, where each authority governs a disjoint set of attributes distributive. In particular, an authority can revoke a user or user's attributes immediately by re-encrypt cipher textsand updating users' secret keys. The main advantage of our ABE system is re-keying message. Each user can accesses the secret keys from any subset of the TAs in the system.

RELATED WORK

[1] Dong et al Provide the Attribute based Encryption system that define the access control in PHR over the cloud network. ABE system also assure the fine grained , scalable and efficient access control over PHRs. ABEs still have the risk in key management and user revocation.[2-4]Saravanan et al describe the biomedical text search and video image search in cloud using clustering method. [4] Imposed to search the records in cloud based on the ranked keyword RSE technique that provide efficient security to access the data based on ranked keyword.[5]Goyal et al Proposed to protect the personal health data stored on a semi-trusted server, ABE adopt attribute-based encryption as the main encryption attribute. Using ABE, access policies are shared based on the attributes of patient or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file This methods can be used to improve the scalability of the key management. There has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). [6-7]Li et al enforced the private keyword search in patient centric health record in cloud network. It also proposes the multi-way, multiple query searches for access the encrypted PHR in cloud. This paper proposes the Encrypting the data before outsourcing would be the most feasible and promising approach. Encryption of files and access security to users both are decided by the PHR owners. User with corresponding decryption key can access PHR file can be accessed only to the user, while rest of users remains confidential. Patient can grant and revoke access privileges when it is required. The authorized users may either need to

access the PHR for personal use of professional purpose. Example of the former is family members and friends while the later can be doctors, and researchers, etc.[7] established the Key escrow (also known as a “fair” cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in this cryptosystem so that, under certain point, an authorized third party may have the control to access those keys. These third parties may include businesses, who may want access to employees' personal information, or governments, who may want to be able to complete list of users Key escrow (also known as a “fair” cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in this cryptosystem so that, under certain point, an authorized third party may have the control to access those keys. These third parties may include businesses, who may want access to employees' personal information, or governments, who may want to be able to complete list of users. [8]Boldyreva et aldemanded the Identity based security for PHR in cloud System. That provides enough security to access patient centric system. [9-10]Ibraimi et al prevalent the Attribute based cipher text for accessing PHR in cloud. Encryption and decryption is done by using threshold value. It is a combination of decryption attributes and access structure. [10] Present the new way to provide the security of PHR system that is multi-authority of CP-ABE technique. This allows encrypting the data based on the attributes of authorized person. [11]Bethencourt et al designed the schema as double encryption to provide the efficient privacy and security to PHR.

METHODS AND EXPERIMENT

A PHR service allows a patient to create, manage, and control personal health data’s in a place through web, which has made the retrieval, storage, and sharing of the medical information more efficient and ease. All personalized records are given to the third parties through cloud. Nobody can surely tell that our records are kept in a safe area, because they are not fully protected. In order to protect these records before outsourcing, an encryption and decryption mechanism is provided for securing the records. It is the best way to secure all data’s in a cloud. It is the best way to secure all data’s in a cloud. To assure the patients control over access to the personal data's, it is rise to encrypt the PHRs before outsourcing. still issues of risks in privacy policies, key management, flexible access, and efficient user access control, have remained the most important problem toward achieving fine-grained, encrypted data access control.This ABE system avoid all the risks to achieve the secured data access in cloud.

Hospital Registration

It is used to store all information about the patient, doctor and patient relations details and also hospital details. This framework is common for all the hospitals each hospitals should register their hospital id and necessary details then they will get the username and password. The admin from the particular hospital will collect all the mandatory information about the patient .i.e. name, age, phone no, mail id, address..etc. The admin will register the data (one time entry) in the hospital database then he will provide a user name and password to the patient mail id and also to mobile.Here the sub modules are patient, doctor, patient relation details.It helps the management to store the detail about patient history from the beginningwith personal details. with personal details.

Figure 1: Registration

ISSN: 0975-8585

Authentication and Verification

After receiving the user name and password from the registration section then the user will be logged in by enter the login details. Here in this it will perform the authentication and verification process in the database, if the id is belongs to new user he will be getting the new registration from else the user will get their home page screen. Else he will get the error message like check your user and password.

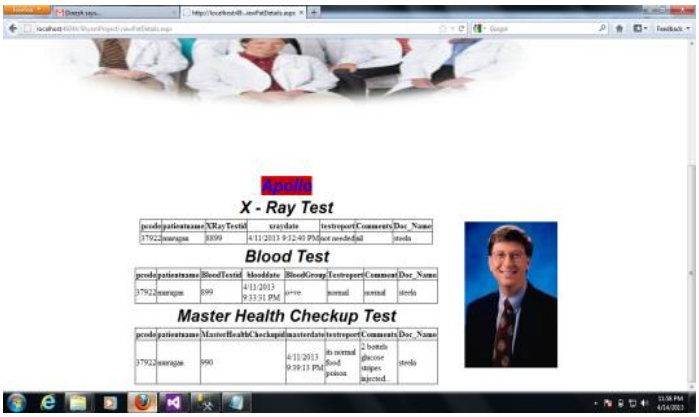

Figure 2: Authorized PHR Report

Transaction

Here the regular updating of the test reports and the patient status will be maintained in this section. The sub modules are x-ray test, blood test, master health check up, doctor's comments and the patient relative's comments. This section will give brief idea about the patient status like allergic medicines, prescription details, in case the patient is admitted into other hospital they will be easily identified the patient status in the transaction section details.

Figure 3: Transaction

Encryption

In this encryption section, the PHR .i.e. patient id is encrypted by using HMACMD-5 algorithm and it is posted to the cloud database. So the other third person cannot easily find the patient id in the database. If other hospitals want to access the particular patient database they need to select the view other hospital details in this module by submitting their mail id, name of the patient id and also the hospital name, then they will get one time password to their mail id. By using that they can view the PHR file for the particular instance only. To improve the security I have added the three features in this section: OTP, image is added in the DB, assigning the patient ids in random manner (unique id) then that Id will be encrypted.

ISSN: 0975-8585

Figure 4: Encrypted Report

CONCLUSION

This paper Proposed a novel framework of secure sharing of personal health records in cloud computing. Instead of partially trusted cloud servers, this paper argue that to fully secure patient-centric concept, and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers using MA-ABE and CC-MAABE method that provides effective solution to some of the issues related to on-demand user revocation and its security. Though implementation and simulation, this paper show that the solution is both scalable and efficient. The results suggested that the proposed design would provide reasonable performance and also reduce the Complexity of key management while enhance the privacy guarantees compared with previous works.

REFERENCES

[1] Dong C, Russello G, and Dulay N. J Computer Security 2010;19: 367-397.
[2] Saravanan D, Srinivasan S. "Data Mining Framework for Video Data", In the Proc.of International Conference on Recent Advances in Space Technology Services & Climate Change (RSTS&CC-2010), held at Sathyabama University, Chennai, 2010; p196-198.
[3] Saravanan D, Srinivasan S. International journal of Computer Science 2013;9 (5): 534-542.
[4] Saravanan D, Srinivasan S. Journal of Computer Applications 2012;5(1)39-42.
[5] Goyal V, Pandey O, Sahai A, and Waters B. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006;pp. 89-98.
[6] Li M, Yu S, Ren K, and Lou W. Authorized private keyword search over encrypted personal health records in cloud computing, in ICDCS ' 2011.
[7] Li M, Yu S, Ren K, and Lou W. "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings, in Secure Comm 10, Sept. 2010;pp. 89–106.
[8] Boldyreva A, Goyal V, and Kumar V. Identity-Based Encryption with Efficient Revocation, Proc. 15th ACM Conf. Computer and Comm. Security (CCS), 2008;pp. 417-426.
[9] Ibraimi L, Petkovic M, Nikova S, Hartel P, and Jonker W. Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes, 2009.
[10] Ibraimi L, Asim M, and Petkovic M. Secure Management of Personal Health Records by Applying Attribute-Based Encryption, technical report, Univ. of Twente, 2009.
[11] Bethencourt J, Sahai A, and Waters B. Ciphertext-Policy Attribute-Based Encryption, Proc. IEEE Symp. Security and Privacy