An Efficient Multi Authority Attribute Based Encryption for Securing Personal Health Recording in Cloud

Tulasi Ram.T and S.V.V.D Sharma

Abstract: **This project presents a design and implementation of a Personal Health Records (PHR) and providing security and stored such as cloud data. This web based application allows user to access and coordinate their lifetime health information, it maintained in centralized server to maintain the patents personal and diagnosis information. The person records should maintain with high privacy and security. These security techniques are used to protect the patient data from the public access. Any authority can assigned access permission for a particular set of attributes. We can control the access data and complex privacy management task in the patient record process management. Multi cloud computing is a colloquial expression can be used to find different types of computing concepts are interface more number of computers are connected in real time communication networks. Host person updates his data into third party cloud data centers. In this project we are propose to a novel patient centric Architecture and access mechanism to control PHRs in multi-trusted servers. We get fine grained and scalable control of data access for patient records stored in multiple trusted servers, and attributes based encryption (ABE) technique to encrypt the each patient's medical record into a file. In this project we are extend Multi Authority Attribute Based Encryption (MA-ABE) for access control mechanism.**

Keywords: Personal Health Records, Cloud Computing, Data Privacy, Fine-grained access control, Multi Authority Attribute Based Encryption.

1. Introduction

Recent years this personal health record is emerged a patient centric design of health message exchange. It activates the patient to create and control their medical data it may be placed in a single place such as data center. High cost of building and managing stream of data centers many of PHR services are outsourced to third party service providers, for example Microsoft Health Vault, Google Health. When it is exciting to have convenient PHR data passing for each one, there are number of security and privacy risks it's a wide adoption. The third party service provides there is no security and privacy risk for PHR. The maximum value of sensitive Personal Health Information (PHI) the unauthorized person storage service are often to target the various malicious behaviors it may lead to exposure to the PHI.

Tulasi Ram.T is a M.Tech (CSE) Student Department of CSE, EVMCET, Narasaraopet, Guntur(Dist), Ap, India and , S.V.V.D Sharma is working as Assistant Professor, Department of CSE, EVMCET, Narasaraopet, Guntur(Dist), Ap, India, Emails: Tulasiram.tech@rediffmail.com, sharama.nic@gmail.com

The main concern is about privacy of patients, personal health data and find which user could gain access to the medical records, stored in a cloud server. The famous incident, deportment of Veterans Affairs containing sensitive database PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who require the data from home without authorization. We ensure the privacy of the control over their own PHRs, it is essential to have fine grained data access control mechanisms that work with may trusted servers. Then we can move to a new encryption pattern namely Attribute Based Encryption (ABE). In this ABE it attributes the users or the data to selects the access policies. It enables a patient to selectively share their own PHR among a group of users by encrypting the file under a set of attributes, need to know complete content of users. The scope of result the number of attributes are involved determines the complexities in the encryption technique, security key generation, and decryption. Bu suing Multi Authority Attribute Based Encryption scheme is used to provide the multiple authority based access mechanism. The aim of this Patient Centric Privacy is often in conflict with the scalability and reliability in PHR system. Only the authorized users need to access the PHR system for personal use of professional purpose. We are refer two categories as a personal and professional users respectively.

2. Related Work

This article is mainly related to operation in cryptographically enforced control access for outsourced and attribute based on encryption data. So we can improve the scalability of the above answer, one to many encryption methods such as ABE can be utilized. The fundamental property of ABE is preventing agenest the user collusion.

a. Trusted Authority

Multiple works can be used ABE to realize fine grained access outsourced data control. Each patient files are encrypted by using broadcast variant of CP-ABE allows directly. Here several communication drawbacks of the above mentioned work. Mainly they are usually assuming the use of single trusted authority in the system. Not only may create to bottleneck but also it suffers from the security key problems. This management also includes certification of all users to attributes and generating secret keys.

b. Attributed based Encryption

This scheme is a well known challenging problem to invoke users efficiently and on-demand in ABE. Mainly this technique is done by the authority of periodic key updates to unrevoked users frequently, and which does not get complete forward/backward security efficiency is less.

For that uniform security, we are proposing frame work of patients centric sharing of PHR in semi-domain, semi-authority PHR

system with multi users. It captured framework application requirements level of both public and personal use of patients PHR and it distributed users trust on multiple authorities are better reflects reality.

3. Proposed system Requirements and Design goals

The most important task is efficient PHR access is to enable patient centric sharing. It means that the patient should contain the ultimate control over their own health record. And also it determines which users shall have access to their medical data. Human control write/read access and revocation are two main security objectives for any type of electronic health record system. The person controlled write access control in PHR context entitles prevents the unauthorized users to get access to the record and to modifying it. The aim of o ur framework is to provide authority of patient's centric PHR access and efficient key management at the same time. When a user attribute is no valid, the user should not be able to access future PHR files using that attribute. This PHR system should support users from the personal domain as well as public domain. Since the many number of users from the public domain may be large size and unpredictable, system should be highly scalable in terms of complexity in key management system communication, computation and storage. Additionally the owners effort in managing users and keys should be minimized to enjoy usability.

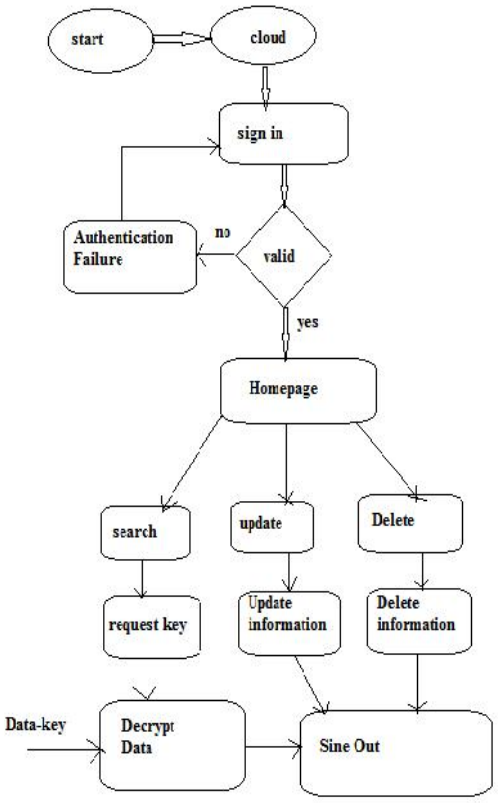

Fig.4.1. system flow diagram.

4. Attribute Based Encryption

By using Attribute Based Encryption techniques we are providing database security. In that the sensitive data is shared and stored in the cloud server, it will be need to encryption cipher text labeled with set of attributes. The private key is associated with access structure to control with cipher text a user is able to decrypt. We are using Attribute Based Encryption (ABE) as the main encryption primitive. By using this ABE access policies are expressed based on the attributes of user data, which enable to selectively share his/her PHR among a set of users to encrypting the file under a set of attributes, without a need of complete users. The complexity per encryption, security key generation, and decryption are only linear with multiple number of attributes are involved. When we integrate ABE into a large scale of PHR system, the important issues such as key management and scalability, dynamic policy updates, and an efficient on demand revocation are non-retrieval to solve.

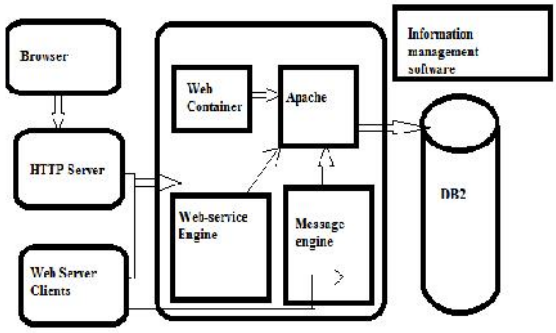

Fig.4.2 system architecture

a. Multi-Authority ABE

A Multi-Authority ABE system is comprised of k attribute authorities and one central authority. Each attribute authority is also assigned a value dk. This proposed system can be uses the following algorithms:

The random algorithm is run by the central authority or some other trusted security. It takes as input the security parameter and outputs public key secret key pair for each of the attribute authorities and also outputs a system public key and master secret key, which will be used for central authority.

Attribute Key Generation: a random algorithm run an attribute authority. The secret key as to take for security authority input and the authority's value dk, a users GID, and authority's domain and output secret key for the user.

Central Key Generation: central authority can be used random algorithm. It takes input as a master key and a user's GID and outputs secret key for user.

Encryption: This technique can be done by a sender. As input a set of attributes for each authority, a data, and the public key the outputs gives the cipher text.

Decryption: This technique can be done by a receiver. It takes input as a cipher text, which was encrypted under set of decryption keys for that attribute set.

Using this ABE and MA-ABE which enhances the system scalability, there are some limitations in practicality of using then building PHR system. While this ABE does not handle that efficiently. In those scenarios one may consider the help of attributes based broadcast encryption.

5. Security Analysis of the Proposed System

i. Data confidentiality: This research scheme disclosed the information about each user to access on the PHR among one another. For example the data revealed to a research scholar unknown to a lab technician.

ii. User Access Privilege Confidentiality: The system does not reveal the privileges of one person to another. This ensures a user can access strong confidentiality. And also it maintain for public domain as well as private domain.

A. Secure Sharing of Personal Health Records

System designer manage Personal Health Records with various user access environment. Those data values are maintained under a third party cloud provider system. The cloud data and privacy provide a privacy and security is ensured by the system. Finally this system is enhanced to support Distributed ABE model. The system can provide multiple modules.

- ✓ Owner of the module data is designed to maintain the patient details. The PHR is maintained with multiple attribute collections. Data header can assigns access permission to different authorities.
- ✓ The second one is cloud provider module is help to store the PHR values. The PHR values are stored in database. Data header uploads the encrypted PHR to the cloud provider. Human can access data are also maintained under the cloud provider.
- ✓ Key management is one of the main tasks to design and manage key values for various authorities. The key values are updated by the owner of the data. These dynamic policy is based on key management scheme is used in this system.
- ✓ The client module is used to access the patients. The personal and professional access models are used in this system. Access category is used to provide multiple attributes. Clients are access log maintains to the user request information for auditing process.

6. Conclusion

This PHR system needs against the security attackers and hackers. The secure data sharing combined basic securities to protect the data from unauthorized access. We are proposed new approach for existing PHR system providing high security using Attribute Based Encryption which plays main role, because these are the unique, and it's not a simple to hack-able. This ABE model is enhanced and operates with MAABE.

References

[1] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.

[2] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded,"2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26.

[3] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 417–426.

[4] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[5] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded,"http://articles.latimes.com/2006/jun/26/health/heprivacy26, 2006.

[7] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[9] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," Pairing-Based Cryptography–Pairing 2009, pp. 248–265, 2009.

[10] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[11] "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

[12] S. M¨ uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption,"Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

[13] Priyanka Korde, Vijay Panwar and Sneha Kalse, "Securing Personal Health Records in Cloud using Attribute Based Encryption,"International Journal of Engineering and Advanced Technology (IJEAT), Issue-4, April 2013.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[15] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010

.