A REVIEW ON SECURE PERSONAL HEALTH RECORDS SHARING OVER CLOUD STORAGE

ANANDA RAO M
Research Scholar, OPJS University,
Rajasthan.

DR. VIJAYPAL REDDY
Associate Professor, Department of CSE
OPJS University, Rajasthan

.

ABSTRACT

Personal Health Record (PHR) service is an emerging design for health knowledge interchange. It enables subjects to create, update and manage personal and medical data. Additionally, they can manage and share their pharmaceutical information with other users as well as healthcare providers. PHR data entertained to the third party cloud service providers in order to improve its interoperability. Nonetheless, there have been severe protection and privacy concerns in outsourcing these data to the cloud server. For protection, encrypt the PHRs before outsourcing. Several issues such as risks of privacy disclosure, scalability in key administration, flexible access and effective user repeal, have remained the most critical difficulties toward producing fine-grained, cryptographically imposed data access controller. Complete fine-grained and scalable data passage control for the client's data, a novel patient-centric framework is used. This framework essentially concentrated on the various data owner scenario. A significant degree of subject privacy is confirmed concurrently by utilizing multi-authority ABE. This design also enables effective modification of path policies or file properties, support efficient on-demand user/attribute revocation.

Nevertheless, some functional obstructions are in building the PHR system. Consider the workflow based entrance control situations; the data entrance right could granted depends upon users identities willingly than their attributes, while ABE does not handle that efficiently. For solving this puzzle in this thesis purposed PHR system, based on Attribute Based Broadcast Encryption (ABBE).

1. INTRODUCTION

Cloud computing means storing and accessing data and programs over the internet instead of using computer's hardware and software. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. Advance technology of cloud computing PHR has undergone substantial changes. Most health care providers and different vendors related to healthcare information technology started their PHR services as a simple storage service. Then turn them into complicated social networks like service for patient to sharing health information to others with the emergence of cloud computing. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client's data, a novel patient centric framework is used.

2. LITERATURE REVIEW

[2] A personal health record () is a patient-made, understanding kept up record that patients can influence accessible to their wellbeing to mind suppliers. This paper examines an online framework, the patient-focused wellbeing record (PcHR), that was made by an exploration amass at the University of Washington.

[1] This paper portrays another approach for gathering and sharing individual wellbeing and health data. The approach depends on an personal health record () including both clinical and non-clinical information. The situated on a system server alluded as basic server. The general administration design for giving mysterious and private access to the portrayed.

[3] Exact and dependable data sharing is basic in the human services area. Right now, nonetheless, data about individual patients is held in segregated medicinal records kept up by various separate human services suppliers. Precisely connecting this data is vital for arranged across the country Electronic Health Record frameworks, yet this must be done in a way that fulfills customary information secrecy prerequisites, as well as meets patients' close to home security needs.

[8] Patient-controlled Personal Health Record () frameworks may encourage a patient not exclusively to share her wellbeing records with medicinal services experts yet additionally to control her wellbeing protection, in an advantageous and simple way. Administered by security assurance laws, express assent/authorization of the particular patient is an essential for sharing individual wellbeing records.

[7] Wellbeing buyers have grasped the web to get access to wellbeing data and to mingle and share information with peers. Furthermore, the web has turned into a more intuitive and rich stage with the joining of wellbeing applications and administrations, for example, Personal Health Records. Some of these applications give customized cooperation's in view of client particular attributes.

[9] Distributed computing is a rising innovation that is relied upon to help Internet scale basic applications which could be fundamental to the human services part. Its versatility, flexibility, flexibility, network, cost diminishment, and superior highlights can possibly lift the productivity and nature of human services.

[10] Tolerant self-administration is fundamental for care and administration of ceaseless sicknesses. It can help patients to have their very own superior comprehension way of life and wellbeing conduct and consequently enhance the infection condition and wellbeing status. Generally, in self-administration, patients and doctors physically note down fundamental signs, medicine record, social insurance visits, and movement sign on paper or onto a PC.

[5] With the improvement of data innovation and restorative innovation, created nations have been build up association to set standard for electronic medicinal records in light of new age and data on the application, they slowly create developing therapeutic data trade mode, Personal Health Records () can incorporate diverse sort of individual wellbeing records.

[4] As a developing patient-driven model of wellbeing data trade, cloud-based personal Health record () framework holds awesome guarantee for enabling patients and guaranteeing more powerful conveyance of social insurance. In this paper, we propose a novel patient-driven cloud-based secure framework, which enables patients to safely store their information on the semi-trusted cloud specialist organizations, and specifically share their information.

[6] To date, the development of electronic individual information prompts a pattern that information proprietors want to remotely outsource their information to mists for the happiness regarding the top notch recovery and capacity benefit without stressing the weight of nearby information administration and support.

3. DIFFERENT ENCRYPTION SCHEMES

3.1 Public key Encryption (PKE)

In this scheme, the plain text is converted to cipher text using the public key. Thus, the sender provides the encrypted text for you and by using your private key you can decrypt it. It's simple but the main drawback of this schema is the use of multiple computer resources, if an attacker determines a person's private key, his entire messages can be read and the loss of a private key means that all received messages cannot be decrypted. The main steps used for this cryptography are illustrated in Figure 1. The main problems in this scheme are the management of keys and the absence of key revocation.

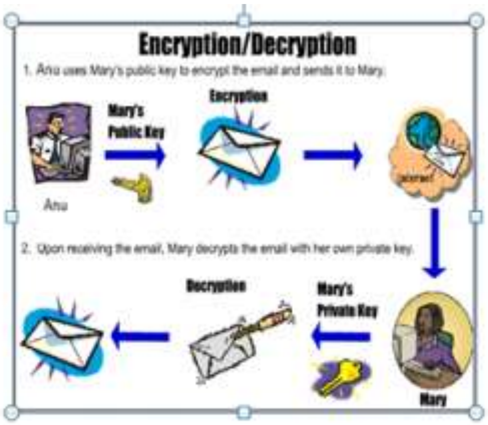
Encryption/Decryption
1. Anu uses Mary's public key to encrypt the email and sends it to Mary.
Mary's Public Key
Encryption
Anu
Internet
2. Upon receiving the email, Mary decrypts the email with her own private key.
Decryption
Mary's Private Key
Mary

Fig 1. Public Key Encryption/Decryption

3.2 Identity Based Encryption (IDE)

The BIE sender can encrypt a message using only the identity without the need for a public key certificate. The common feature of IBE is that they consider identities as a string of characters. In IBE, a public identity (for example, an email address) is used as a public key while the corresponding private key is generated by the known identity. The IBE encryption scheme is a four algorithms / steps scheme in which the algorithms are

(1) Setup Algorithm.

(2) Key (private key) Generation Algorithm.

(3) Encryption Algorithm.

(4) Decryption Algorithm.

In cryptographic identity identities based on fuzzy identities as a set of descriptive attributes. Thus, in this scheme, identity error problems in IBE are resolved. These are two interesting Fuzzy IBE apps

(1) Identity based encryption system that uses biometric identities.eg: iris scan.

(2) It is used in Attribute based encryption.

3.3 Attribute Based Encryption (ABE)

Sahai and Waters have introduced attribute-based encryption (ABE) for the first time to control forced access through public-key cryptography. The main aspects are flexibility, scalability and accurate access control. In the ABE scheme, the secret user key and cipher text are associated with a set of attributes. Suppose that the sets of attributes are those of the computer, of the man and of the age of 40 years.

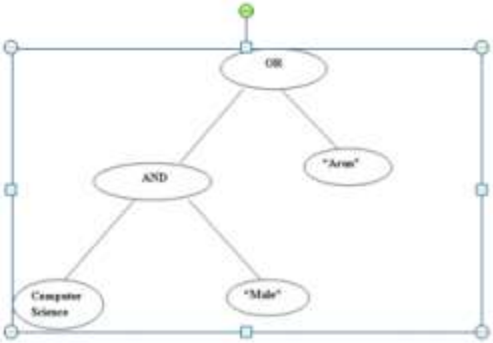

Fig. 2. Access Structure for ABE

The internal node consists of AND, OR doors and leaves are made up of different attributes. The sets of attributes that satisfy the tree structure can reconstruct and access the secret message. In a typical model, this can only be done when the user and server are in a trusted domain. Thus, various alternatives of ABE are introduced.

3.4 Key Policy Attribute Based Encryption (KP-ABE)

To allow for more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters proposed a cryptographic scheme based on key-key attributes (KP-ABE). This is the modified form of the classic ABE model. In the KP-ABE schema, attribute policies are associated with keys and data is associated with attributes. In KP-ABE, a set of attributes is associated with the cipher text and the decryption key of the user is associated with a monotone access tree. When the attributes associated with the cipher text satisfy the access tree, the user can decrypt the cipher text. The limitations of KP-ABE are not able to decide who can decrypt the encrypted data, is not suitable for some applications such as sophisticated broadcast encryption and offers accurate access, but does not have more flexibility and extensibility.

3.5 Cipher text Policy Attribute Based Encryption (CP-ABE)

Sahai et al. introduces the concept of another modified form of ABE called CP-ABE which is attribute-based cryptography of the text cryptography policy. In the CP-ABE schema, attribute policies are associated with data and attributes are associated with keys. Only the keys that the associated attributes meet the data-bound policy can decrypt the data. In a CP-ABE scheme, an encrypted text is associated with a monotone tree structure and a user decryption key is associated with a set of attributes. The limits of this system are that it cannot meet the access control requirements of the company, which requires considerable flexibility and efficiency.

3.6 Hierarchical Attribute-Base Encryption (HABE)

This scheme (HABE) proposed by Wang et al. It is a combination of Basic Hierarchy Identity (HIBE) and CP-ABE encryption. Provides fine access control, full delegation, and high performance. The HABE schema is composed of many attribute authorities and many users. ABE uses a disjunctive normal form policy. The same attribute can be administered by multiple domain masters based on specific strategies, which is more complicated to implement in practice. The HABE model consists of a root master (RM) and several domains. A domain includes the number of domain masters and the number of end-user related users. The HABE model is shown in Figure 3.

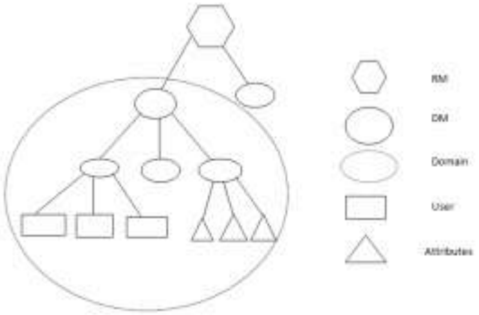

Fig 3. HABE model

It is mainly applicable to the environment of companies that share data in the cloud. This schema presents problems with multiple value assignments and the practical implementation is very difficult because the same attribute can be administered by several domain masters.

3.7 Hierarchical Attribute Set Based Encryption (HASBE)

The HASBE scheme is proposed and implemented by Zhiguo Wang et al. This scheme extended the ASBE scheme to manage the hierarchical structure of the system. The HASBE model is shown in Figure 4. In this model, the trusted authority is responsible for managing top-level domain authorities. Each user of this system is assigned a key structure. This system offers scalable, flexible and accurate access control in cloud computing. The actual revocation of the user can be performed in this scheme due to the assignment of multiple values to the attributes.

3.8 Multi-Authority Attribute Base Encryption (MA-ABE)

This scheme includes many attribute authorities and many users. The attribute key generation algorithm will perform the authorization and the result will be sent to the user. In an ABE schema with multiple authorizations, different attribute authorities monitor different sets of attributes and issuing corresponding decryption keys for users and numbers may require a user to obtain keys for the appropriate attributes of each authority before decrypting a message. Chase has given a multi-authority ABE system that supports many different authorities operating simultaneously, each handling secret keys for a different set of attributes.

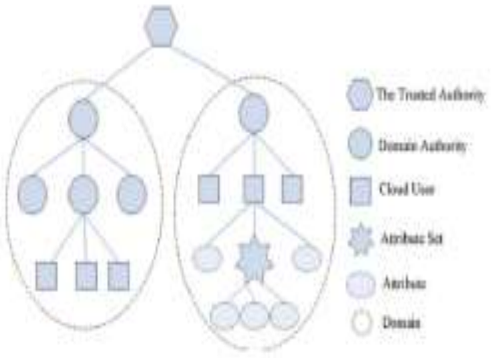

Fig. 4. HASBE model

4. CONCLUSION

Data security is the main problem of cloud storage. Before outsourcing the PHR to a third-party server, encryption schemes based on different attributes are used for secure storage. ABE is used to encrypt PHR data, so that patients can access not only individual users, but also various public domain users with different roles, qualifications, and professional affiliations. By using the Enhance MA ABE scheme, better query revocation is possible. In the practical case, other problems will arise. The main problem in this case is to try to implement conditions based on the workflow. To resolve these issues, you must have attribute-based broadcast (ABBE) encryption. Workflow The basic situation is implemented using ABBE and analyzes the security and calculation costs. The analysis shows that this workflow-based schema is both scalable and efficient. It also offers better user revocation on demand. In the future, it would be interesting to consider the attribute-based broadcast coding system with different types of impressions. If you consider that different identifiers are identical, the distributed ABE schema is required.

References:

1. Anna Sachinopoulou; et.al, 2007, "Ontology-Based Approach for Managing Personal Health and Wellness Information", ISSN: 1094-687X, Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, PP: 569-571.

2. A. Stolyar; et.al, 2006, "A Patient-Centered Health Record in a Demonstration Regional Health Information Network", Distributed Diagnosis and Home Healthcare, 2006. D2H2. 1st Transdisciplinary Conference on, PP: 160-163.

3. Bandar Alhaqbani & Colin Fidge, 2008, "Privacy-aware access to Patient-controlled Personal Health Records in emergency situations", ISSN: 2153-1633, Pervasive Computing Technologies for Healthcare, 2009. PervasiveHealth 2009. 3rd International Conference on, PP: 108-117.

4. Chang-Ji Wang; et.al, 2014, "An Efficient Cloud-Based Personal Health Records System Using Attribute-Based Encryption and Anonymous Multi-receiver Identity-Based Encryption", P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on, PP: 74-81.

5. Chia-Hui Liu; et.al, 2013, "Secure Access Control Scheme for Healthcare Application Clouds", ISSN: 0190-3918, Parallel Processing (ICPP), 2013 42nd International Conference on, PP: 1067-1076.

6. Kaitai Liang & Willy Susilo, 2015, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage", ISSN: 1556-6013, Volume: 10, Issue: 9, PP: 1981-1992.

7. Luis Fernandez-Luque; et.al, 2010, "Personalized health applications in the Web 2.0: The emergence of a new approach", ISSN: 1094-687X, Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE, PP: 1053-1056.

8. Md. Nurul Huda; et.al, 2009, "Privacy-aware access to Patient-controlled Personal Health Records in emergency situations", ISSN: 2153-1633, Pervasive Computing Technologies for Healthcare, *2009. PervasiveHealth 2009. 3rd International Conference on, PP: 1-6.*

9. Mina Deng; et.al, 2011, "A Home Healthcare System in the Cloud--Addressing Security and Privacy Challenges", ISSN: 2159-6182, Cloud Computing (CLOUD), 2011 IEEE International Conference on, PP: 549-556.

10. Yan-Yu Lam Andy; et.al, 2012, "Continuous, personalized healthcare integrated platform", ISSN: 2159-3442, TENCON 2012 - 2012 IEEE Region 10 Conference, PP: 1-6.