International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 4, No. 3
August 2015

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 4, No. 3, August 2015

Research Paper

PRIVACY HEALTH DATA ACCESS IN CLOUD USING ABE CRYPTO-SYSTEM

K Karthika[1]* and C Sumitradevi[1]

Corresponding Author: **K Karthika ✉ karthikamca91@gmail.com*

Attribute Based Encryption (ABE) determines encryption facility based on a user attributes. Within a multi-authority Attribute Based Encryption system, multiple user-authorities monitor different sets of attributes and subject corresponding decryption keys to user and encryptors can need that a user obtain keys for proper attributes from each authority before decrypting a message. PHR is maintaining in the centralized secure server to manage the patient's details. The patient data's should be managed with high security and privacy. These systems are used to continue the personal data from public access. Every authority is allocated with access permission for a limited set of attributes. In this thesis work, propose a novel patient-centric framework and a suite of data access mechanisms to control PHRs stored trusted servers. These mechanisms realize fine-grained and scalable data access control for PHRs, leverage ABE techniques to encrypt each patient's PHR file. Proposed mechanism could be extended to Multi-Authority ABE (MA-ABE) for multiple authority based access control mechanism.

Keywords: Cloud computing, Attribute Based Encryption (ABE), Searchable Symmetric Encryption (SSE), Personal Health Records (PHR).

INTRODUCTION

PHR is emerged as a patient centric model of health records exchange. Enables the patient to control their medical information which may be located in a single place such as data server. Building and maintaining dedicated data centers is high cost, many PHR services are outsourced to third-party service providers, example, Google Health, Health Vault. It is exciting to have convenient PHR data services for everybody, there are more privacy and security risks which could impede its wide approval. The main concern is about whether the patients could control the sharing of their susceptible Personal Health Information (PHI), mainly when they are upgraded on a third-party location which people may not trust fully. There exist health care policy is recently amended to incorporate business associates, cloud providers are usually not covered entities.

The high value of the sensitive PHI, the third-party storage servers are often the targets of

[1] Department of MCA, V.S.B Engineering College, Karur, Tamil Nadu, India.

various malicious behaviors which may lead to exposure of the PHI (Bethencourt, 2007). "As a well-known incident, a Department of Affairs database containing Personal Health Information, including their social security values and health problems was stolen by data home. To ensure security control over their own PHIs, it is essential to have fine data access control processes that work with trusted data home. Hence move to a new encryption mechanism namely ABE. This ABE, it is the attributes of the consumers or the data that selects the access policies, which enables a patient to selectively share their PHI among a set of consumers by encrypting the file under a set of attributes, without the need to know a complete list of consumers. The number of attributes involved calculates the complexities in encryption, key generation and decryption. The Multi Authority ABE (MA-ABE) system is used to present multiple authority based access control schemes. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHI owner them self should decide how to encrypt their information's and to allow which set of consumers to obtain access to each data. A PHI file should only be presented to the consumers who are given the corresponding data retrieval key, while remain confidential to the rest of consumers.

RELATED WORK

The paper is mostly related for cryptography enforced access control for outsourced information and ABE. To recover upon the scalability of the data's, one-to-many encryption methods such as ABE can be used. A fundamental property of ABE is preventing against user knowledge. In addition, the encryptors are not required to know the attributes and Personal Health Records.

Trusted Authority

A number of works used ABE to recognize fine-grained access control for outsourced data's (Narayan, 2010). The proposed an ABE infrastructure for PHR systems, where each patient's PHR files are encrypted using a broadcast variant of Ciphertext Policy ABE (Yu, 2010) that allows direct revocation. There are several common disadvantages of the works. First, they usually assume the use of a single Trusted Authority in the system. This not only may create a load, but also suffers from the key escrow (distribution) problem. In addition, it is not practical to hand over all attribute management task to one Trusted Authority, including certifying all consumers attributes or roles and generating secret keys (Sahai, 2005).

Attribute Based Encryption

It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE. Traditionally this is often done by the authority broadcasting periodic key updates to unrevoked users frequently (Sahai, 2005; Nishide, 2008), which does not achieve complete backward/ forward security and is less efficient. This paper bridges the above gaps by proposing a unified security framework for patient-centric sharing of PHR in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHR and distributes users' trust to multiple authorities that better reflects reality.

Searchable Symmetric Encryption

SSE allows owners to store encrypted documents on server, which is modeled as honest but curious party, and simultaneously provides away to search the encrypted documents. The operation of neither

outsourcing nor keyword searching would result in any information leakage to any party other than the data owners, achieving a sound guarantee of privacy.

KeyGen: This function is used to the users generate keys to initialize the system. It takes the security parameters and outputs a secret key K.

Build Index (D, K): The user runs security system to build the indexes, denoted by Idx, for a collection of document D. It takes secret key K and D and outputs Index, which document can be searchable remaining encrypted.

Search (Index): This function is processed by the server to search for documents containing the user assigned keyword. Due to the use of the user data, the server is able to carry out the exact query without knowing the genuine keyword. The function takes the built secure data index *I* and the trapdoor, and outputs the identifiers of files which contains keyword.

PROBLEM DEFINITION

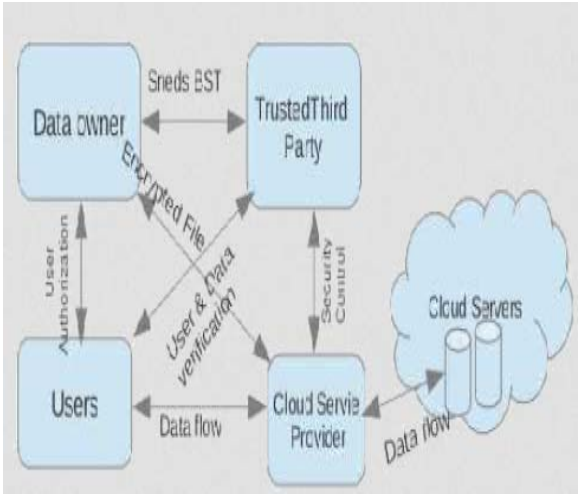
E-healthcare systems are increasingly popular, a large amount of personal health data for medical purpose is involved, the people initiate to realize that they would completely drop control over their personal data's once it enters the cyber-space. The government website, around million's of patients' health data's was leaked in the past years. There are good reasons for keeping medical data's private and limiting the access. Users may choose not to hire someone with certain diseases. An insurance company may refuse to sponsor life insurance knowing the disease history of a patient like users.

The encrypted PHR disallow the centralized facility from obtaining the secret information, it still looks the difficulty of data verifiability. Multiple users address the problem of secure Private Set Intersection (PSI), which is related to the highest privacy level in our proposed system. Users are facing the problem of verified the validity of corresponding credentials issue by without exposing. Loss without generality, hereby list the following steps are implemented in all of our security levels.

SOLUTION FRAMEWORK

Outsourcing the computation to the cloud saves from buying and maintaining servers, and allows taking advantage of Cloud to process and analyzing data faster and more efficiently. The proposed cloud-assisted health networking is inspired by the convenience, flexibility, power, and cost efficiency of the cloud based data computation outsourcing pattern. Introduce the private cloud can be consider as a service offered to cloud users. PHR users outsource data tasks to the private cloud which stores the processed results on the cloud. Advantages of Proposed System, High Security, No potential leakage of Personal Health Records (PHR), Provides privacy to users. The below Figure 1 mentioned these short forms.

Figure 1: Architecture Diagram



The similarity achieve between two patients is the size of identical attributes of their intersection sets. Based on the cipher texts of certificates, patients complete encryption on each single data and return to each other for deriving the results. Our proposed mechanism relies on the encryption results of encryption which has the following properties.

METHODOLOGY

A Multi Authority Attribute Based Encryption system is comprised of n attribute authorities and one central authority. Each and every data's managed on attribute authority is also assigned a value, key. The system uses the following algorithms:

Set up: A random algorithm that is run by the inner authority or some other trusted authority. It takes as input the security parameter and outputs a public, secret key pair for all of the attribute authorities, and also output public and master key which will be used by the inner authority.

Attribute Key Generation: A random generation runs by an attribute authority. This is takes as input the authority's secret key, the authority's value data key, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.

Central Key Generation: A randomized algorithm that is run by the central authority. It takes as input the master secret key and a user's GID and outputs secret key for the user.

Encryption: A randomized algorithm runs by a sender. This takes as input a set of attributes for each authority, a message, and the system public key and outputs the cipher text.

Decryption: A deterministic algorithm runs by a user. This takes input a cipher-text was encrypted under attribute set and decryption key pair for that attribute set. This algorithm outputs a decrypted like message m.

IMPLEMENTATION

ABE is a well-known challenging problem to revoke attributes /users efficiently and on-demand in service. Usually this is often done by the authority broadcasting periodic key updates to unrevoked users commonly, which does not achieve complete backward/forward security and is fewer efficient.

A PHR examine allows a patient to create, manage, and control their personal health information in one place via the web, which has made the retrieval, sharing, and storage of the medical data's more efficient.

This approach would be to encrypt the data's before outsourcing. Normally, the PHR owner herself should choose how to encrypt their ales and to allow which set of user to achieve access to each file. PHR file should only be accessible to the users who are agreed the corresponding decryption key, while remain classified to the rest of users.

Encryption

Attribute Values (Attr).

Get Byte [] (B1) of that Attr.

Generate Public Key (Pk).

Perform Encryption on Byte B1.

Convert Byte B1 into string (EAttr).

Decryption

Encrypted attribute's value (EncAttr)

Convert EAttr into byte [] (B2).

Generate Private Key.

Perform Decryption on B2.

Convert B2 into string (DAttr).

Secret Key

Input: PK (see Decryption 3) and No. of Authority (nAuth) =10.

Get Length of PK: Length = PK. Length.

To become private key multiple of NAuth (10) pad it by zero (0).

M = Length / NAuth

Each authority having 'M' no. of bytes.

For Each Byte value from 'M'.

For (int I = 0 ; I < M.Length ; i++)

{

Square = M[i] * M[i] ;

Hex value = Hex (Square);

Hex value = Hex value +"&"

Full hex value = Full hex value + Hex value;

}

Add this Hex value into database as a secret key.

Attribute Key Generation

List = List of Attribute assign to the user (Authorities).

For each (string Attribute in List) {

For each (char ch in Attribute)

{

Value = Value + ch;

} }

In the Value we get ASCII value of that character.

ASCII values save into database.

CONCLUSION AND FUTURE WORK

The Personal Health Records (PHR) is maintained in a data server under the multi-cloud environment. Novel framework of privacy sharing of PHRs has been proposed in this development. Personal and public access models are designed with privacy and security enabled mechanism. The framework concentrates on the unique challenges provided by multiple PHR users and owners, in that the complication of key organization is greatly reduced. The ABE model is enhanced to support operations with MA-ABE.

The Developed MA-ABE could be further enhanced in future to proactive Multi authority attribute based encryption. Also, combine other privacy-enhancing techniques with cryptographic techniques. Cryptographic techniques are an essential, but not the only one, method to protect private data against partially trustworthy cloud server. Therefore, we are trying to find more efficient way to address the security and privacy issue of PHR systems.

REFERENCES

1. Bethencourt J, Sahai A and Waters B (2007), "Ciphertext policy attribute based encryption", *IEEE Symposium on Security and privacy*, pp. 321-334.
2. Boneh D and Waters B (2007), "Conjunctive, Subset, and Range Queries on Encrypted Data", TCC'07.LNCS 4392, pp. 535-554, Springer.
3. Emura K, Miyaji A and Omote K (2009), "A ciphertext policy Attribute –Based Encryption scheme with strong Recipient Anonymity",The 4th International workshop on Security (IWSEC), pp. 49-63.

4. Li J, Ren K, Zhu B and Wan Z (2009), "Privacy aware Attribute based Encryption with user Accountability", eprint.iacr.org/ 2009/284.

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

6. Nishide T, Yoneyama K and Ohta K (2008), "ABE with partially hidden encryptor specified access structure", ACNS'08, LNCS 5037, pp. 111-129, Springer.

7. "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, worcester polytechnic institute, 2011.

8. Sahai A and Waters B (2005), "Fuzzy Identity-based encryption", *LNCS,* Vol. 3494, pp. 457-473, Springer, Heidelberg.

9. Waters B (2008), "Ciphertext policy attribute based encryption: An expressive, efficient, and provably secure realization", Cryptology ePrint report 2008/290 .

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

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com