International Journal of Computer Techniques -– Volume 2 Issue 2, 2015

RESEARCH ARTICLE OPEN ACCESS

PRIVACY ENHANCING AND PROTECTED DISTRIBUTED OF PERSONAL HEALTH RECORD USING ABE

Vijayakumar K, (M.Tech) ,S.Sivamohan,(Assistant Professor)
Department of CSE, Department of IT,
SRM University, Ramapuram Campus
Chennai-600089

----------------------------*********************************------------------

Abstract:

In recent years clients generally outsource the sensitive information in any storage providers in order to access everywhere. There are so many intermediaries such as cloud providers to provide this. Personal health record is a promising approach for patient - centric model in which all the sensitive information including personal details will be outsourced to those third party providers. However there have been serious security issues will arise when any illegal parties tries to access those details. In order to ensure the privacy over the personal health information it is suggested to encrypt the data before outsourcing. Most significant challenges such as modularity issues in administrating the keys, disclosure of details, extensible in approaching the data and nullifying the data consumer details are turned to be a showstopper to achieve fine grained data mechanisms. In this paper we propose an innovative approach which makes sure of individual patient preferences and ensuring that patient values when PHRs stored in semi trusted servers. To overcome those significant challenges mentioned above we extended the attribute based encryption techniques to encrypt each patient's PHR file. By exploiting key policy and multi authority ABE data consumers are classified into various domains which will significantly reduces the key administrations. Also an efficient algorithm is used along with ABE which will Ensure the encryption of personal health details and provides high degree of privacy.

Keywords: - Attribute Based Encryption, Key-policy, Multi-Authority, Central Authority

----------------------------*********************************------------------

1. Introduction:

Consider a PHR system which contains multiple owners. Each owner is responsible for managing their own records. Also they need to provide the keys whenever the user required. Users here are referring to the people who are ready to access the file and modify. In such case if the user is managing the key it will lead to hug e burden for the owner also the owner must be in online whenever the user requests key. It leads to tedious job for the owner to be always stayed tuned.

As an alternative approach we can give the key management control to central authority that can provide the keys when the user request. It doesn’t require the user to be in online. Such single authority can manage the entire system. However it overcomes the drawback of the single owner management it suffers from the following issues. i.e. when the central authority got crashed or if unauthorized users understand the work flow of that system it leads to serious issue in key management. An unauthorized user can act as an actual user and gains the access and take the control.

It proposes another approach called cipher text ABE[3]. In which each user will get the secret key by having set of attributes. Message will be encrypted by having the proper access policy or access tree structure. Cipher text will be framed based on the nodes. Only the users who satisfy the access structure can decrypt the text. When such cipher text is produced it will increase the length of the text especially for unrevoked users it grows linearly.

Cloud computing plays a dominant role in the IT industry. Cloud computing cannot fulfill the promises such as security and privacy even though it provides enthusiasm to data owners. In this new model main idea is divide the users into multiple domains namely public and personal.

2. Related works:

To compute the similarity and identify the issues related to existing system, some of the proposed measure has been analyzed against the existing system. It leverages the existing system in order to make sure the performance achieved by proposed measure is superior than the available system. Here we addressed few issues and related works to overcome those factors.

- Access structure :

  An access structure is the one which can be represented in the form a tree. It also contains threshold gates of AND, OR. Let us consider an example for an access structure.
  ((“Research Industry” AND (“Maryland” OR “NewYork”)) OR (Scienties-grade > 5) OR “Name: John Charles”)

- Cipher Text Attribute based encryption:

In a cipher text ABE[3], user’s private key is created by using set of attributes. Such Attributes can be any of the roles (e.g.: Department or dates or executive level). Cipher text will be prepared based on the access structure which is framed based on attributes of the user. Only the users whose private key falls into the access structure can decrypt the data. The main drawback of the Cipher text ABE[8] is length of the key size will be increased by the number of attributes. Also when the user is not revoked that particular key cannot be reused. Cipher text ABE[8] algorithm consists of four steps. Setup, key-Generation, Encryption and Decryption.

- Algorithm:

✓ *Setup: Only implicit security parameter will be taken as an input. It produces the public parameters PP and a master key MK.*

✓ *Encrypt(PP,M,S): Three parameters are passed as an input to produce the cipher text. public parameters PP, a plain text message M , and an access structure S over the collection of attributes. The algorithm produce a ciphertext CT. User’s private key that contains a set of attributes which satisfies the access structure can only decrypt the message.*

✓ *Key Generation(MK,A): Here private key will be generated PR_k for a specified attributes of the user along with the master key.*

✓ *Decrypt(PP,CT, PR_k): Plain text message will be produced only for the user’s private key matches with the access structure present in the cipher text*

- Single Vs Multiple Authority:

In order to provide the keys to the users, respective data owners will validate those and provide the keys. This will limit the accessibility since it is not practical to expect the users always in online. An alternative approach called Central Authority which can control the key management. But it leads to a dependency of single authority also opens key escrow[2] problem. To overcome this Multi authority can be used thereby dependency issues will be resolved. Each attribute authority governs subset of attributes and the complete system will be controlled by collection of all authorities.

3. Implementation:

3.1Proposed Methodology:

In the proposed framework users are broadly classified into two type's namely public and personal domain. Key policy Attribute based encryption[5] and Multi Authority attribute based encryption[4] techniques are used. Personal data verification will be done by separate authorities called Admin. Once it is validated user can upload the PHR. Before the data getting settled down in cloud server all the data will be encrypted using ABE techniques and encryption algorithm called Triple DES. Personal domain users are the owners of the data and the level of accessibility is based on each individual owners. They can extend the access to friends and relatives. Remaining users such as doctors, nurses, pharmacists and insurance sectors are associated to Public domain. In other words they are referred as individual sector in the society. Let's take an example once the user (owner) uploads his/her details, central authority will be validating those details. Once it is validated CA will generate public and private keys for the users which are used to decrypt. All the details will be encrypted using ABE and triple DES encryption algorithm in the cloud server as shown in the architecture. Each user can read and write their respective PHR[6] based on the keys which are provided. Thereby fine grained data[1] will be obtained. Access structure of the key must match with the attributes present in the cipher text.

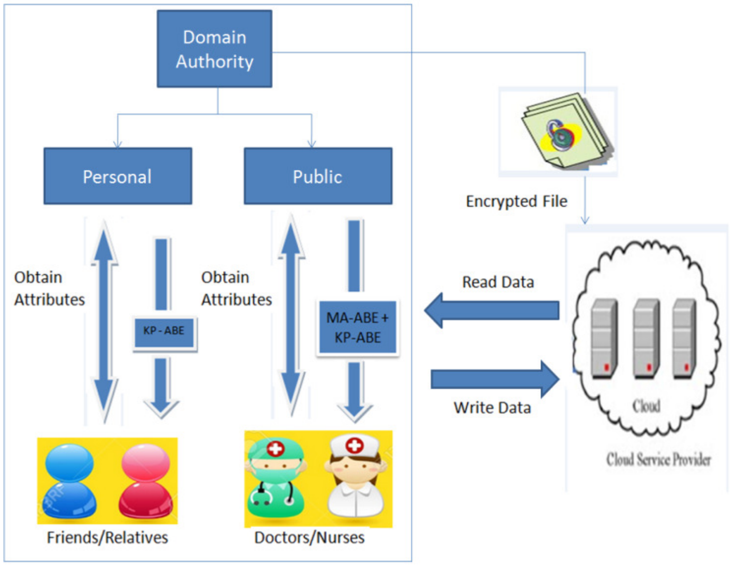

Fig 3.1 System Architecture

3.2Encryption techniques:

3.2.1 KP-ABE

Key policy attribute based encryption[5] is reverse of Cipher text attribute based encryption. In these technique users private key is based on access policy. If any revocation processed, updating the policy alone will resolve the issue. Also key length issue will not occur. Key policy algorithm contains four steps similar to cipher text.

- Algorithm:

✓ Setup: This algorithm takes as input a security parameter P and returns the public key Pu_K as well as a system master secret key MK. Pu_K is used by message senders for encryption. MK is used to produce user private keys.

- ✓ *Encryption: This algorithm takes a plain text message M , the public key Pu_K , and a set of attributes. It will be part of universal authorities and produces the ciphertext C.*

- ✓ *Key Generation: This algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key called as private key $PR_{K.}$ that enables the user to decrypt a encrypted message only when PR_K satisfies (access structure T) set of attributes present in the cipher text.*

- ✓ *Decryption: It takes as input the user's secret key PR_K for access structure T and the ciphertext C, which was encrypted under the universal attributes. It produces the actual message M only if the attribute set satisfies the user's private key PR_K created by using access structure T.*

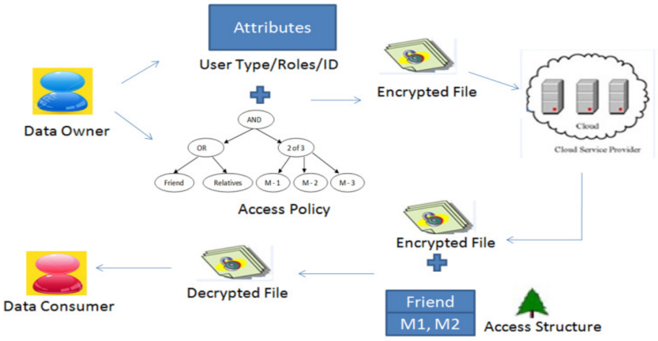

Fig 3.2 KP-ABE Architecture

3.2.2 MultiAuthority ABE:

- ✓ Setup: An anticipated multinomial time algorithm a that given the security parame-er 1^l, a list of pair wise disjoint sets of attributes $[X_k]k$ ∈K and thresholds $[T_k]k$∈K generates – a (public key, secret key)-pair for each attribute authority k∈K public system parameters

- ✓ *Attribute key generation: An* anticipated multinomial time algorithm *time algorithm^a that given an attribute authority k's secret key, the corresponding threshold T_k , a (unique identifier of a) user u and a subset $X_u \subseteq X_k$ outputs decryption keys for user u.*

- ✓ *Encryption: An* anticipated multinomial *time algorithm that given a plaintext, attributes XC⊆X and the public system parameters, outputs a ciphertext E.*

- ✓ Decryption: A deterministic multinomial time algorithm that given a set of decryption keys for a set of attributes X_u and a ciphertext E encrypted with attribute set XE, outputs the corresponding plaintext M if $|X_u \cap X_k \cap X_E| \geq d_k$ for al attribute authorities k∈K; otherwise it outputs an error symbol ⊥.

3.2.3 Triple DES

Triple DES is so called Triple Data Encryption algorithm which is Symmetric key cipher. It is a three stage encryption process with three different keys. Availability of increasing computational power made brute-force attacks feasible. It requires input 56 bit key (i.e. 56 * 3)

- Algorithm:

Triple DES consists of three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits).

$$CT = EK_3(DK_2(EK_1(PT)))$$

I.e., As mentioned it is a three stage process of DES

a. Encryption with K_1,
b. Decryption with K_2,
c. Finally Encrypt with K_3.

Decryption is the reverse:

$$PT = DK_1(EK_2(DK_3(CT)))$$

I.e., decryption with K_3, encryption with K_2, then decryption with K_1.

Strength of the algorithm depends on key option preferences. They are:

- All three keys are independent.
- K_1 and K_2 are independent, and $K_3 = K_1$.
- All three keys are identical, i.e. $K_1 = K_2 = K_3$.

4. Revocation and Policy updates:

There might be a situation where the user will leave the organization. In such case all the particulars of the respective users must be revoked such that he/she cannot access PHR outside of the world. Revoking the access privileges will be taken care by each attribute authority owners. Since MA-ABE is used it needs to be revoked in all AAs. In another situation a policy needs to be updated when a new user is getting added. Here the data owner will be responsible since access privileges of personal domain are fully controlled by the owner. By adding the required attributes a policy can be updated.

5. Experimental Results:

To test the accuracy of user creation, uploading and fetching the data and to determine an exact measure of the similarity between users, wide – ranging of users creation are conducted.

In this graph X-axis represents the number of users and Y-axis represents time taken in seconds. The experimental setup shows two set of users. The first user transactions like uploading personal details, followed by uploading the PHR, submitting the query and viewing the results. It takes almost 100s. Second user also tried to upload the similar approach. It takes less than the first user.

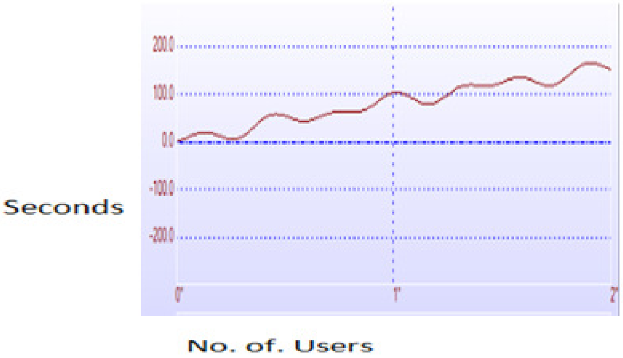

Fig 5.1 Performance Diagram

It shows that when number of users are getting increased the complete transaction time is less and proves that it does not leads to time complexity issues. The below graph shows only for two set of users. We can achieve this graph by having move number of users.

6. Conclusion and Future work:

In this paper we adopted a new approach which considerably reduces the key administration issues. Efficient algorithm leads to encrypt the data in a secure manner and avoids unauthorized parties access. The new framework focuses on security level and it is achieved even in minimal attributes. By keeping the complex access policy unauthorized parties need more trial works to break the encryption. There are so many possibilities to extend this paper. One of the approach is having the user image is one of the attribute in the personal details which makes unauthorized parties more complex to break the encryption. Another approach is by increasing the number of attributes which in turn strengthen the encryption. Also we can maintain the logging mechanism to trace all the transaction details to trace if any issues occurred.

7. Reference:

[1] V. Goyal, O. Pandey, A. Sahai, B.Waters, "Attribute - based encryption for fine – grained access control of encrypted data". In: ACMCCS 2006 , pp. 89 - 98 (2006)

[2] S. Al - Riyami, J. Malone - Lee, and N. Smart. "Escrow - free encryption supporting cryptographic work
flow". In Int. J. Inf. Sec ., volume 5, pages217 - 229, 2006.

[3] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext policy attribute - based encryption. In ICALP, pages 579
-591, 2008.

[4] Sascha Müller, Stefan Katzenbeisser, and Claudia Eckert, "On Multi - authority ciphertext - policy attribute - based encryption In: Bulletin of the Korean Mathematical Society 46,no.4 pages803 - 819, 2009

[5] Li, Qi, Jianfeng Ma, Rui Li, Jinbo Xiong, and Ximeng Liu,"Large universe decentralized key-policy attribute-based encryption." In: Security and Communication Networks, 2014

[6] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou "Scalable and Secure Sharing of Personal Health Records in Cloud
Computing Using Attribute-Based Encryption",Vol.24, No 1, January 2013

[7] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of
Personal Health Records by Applying Attribute-Based Encryption,
"technical report, Univ. of Twente, 2009.

[8] 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.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,
and Fine-Grained Data Access Control in Cloud Computing,"
Proc. IEEE INFOCOM '10, 2010.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data
Sharing with Attribute Revocation," Proc. Fifth ACM Symp.
Information, Computer and Comm. Security (ASIACCS '10), 2010.