ENFORCED ENCRYPTION OF PERSONAL HEALTH RECORDS STORED IN SEMI-TRUSED CLOUD

[1]Dr. R. Bullibabu, [2]G.V. Siva Krishna, [3]P. Jeshwanth, [4]M.Pravallika, [5]M.Harishma Roy

[1]Assoc Prof, Dept of ECM, KL University

[2, 3, 4, 5]Student, Dept of ECM, KL University

ABSTRACT

In this paper we provide enforced encryption for health information stored in semi-trusted servers in cloud. This health information is known as personal health records and as it said personal it is in patient perspective and access control authority will be patient of all. As cloud servers are not trusted we need to provide encryption for the records before outsourcing. In the existing systems key distribution and encryption is have been provided though key management and dynamic access policy has always been challenging. So in our proposed system we provide different mechanism to provide flexible access to all PHR owners and minimized key overhead and efficient emergency system with extended security and providing greater amount of privacy with multi authority for public access. As this is attribute based encryption, users cannot access whole information at a time granting security for PHR owner and achieving our purpose.

INTRODUCTION

PHR is created by patient through registration in cloud service provided by hospitals using third party providers like Microsoft Health Vault. It is managed systematically and controlled by PHR owner i.e. patient itself. And patient share this information with other users like family, friends, hospitals, Insurance companies, relatives etc .Hence this is a personal information and sometimes confidential and there is lot of possibilities of security risks and privacy violations. The PHR users can be of many business personalities, celebrities or military persons, so there is utmost need of blocking the access to people other than PHR owner has given access to with proper authorization. This is where we need to achieve fine grained access control, Patient decided to which set of users should access which part of the file and PHR must be accessed by that person only of that part and remaining must stay confidential and also patient must be able to modify or revoke the access policy whenever he wants to.

As we discussed there are lot of users involving the PHR, they are segmented into two domains public and private domain. Private domain is controlled by the user and this includes owner's friends, families and other relatives. This contains small set of users and hence there will be no problem for PHR owner in maintaining this. Whereas when it comes to public domain there will be lot of users and this will create key management overhead and it will be a lot of trouble for patients. And there can be lot of requests coming from their users and PHR owner i.e. patient will not be able to manage by his own as he doesn't know many of them. And that is where attribute authorities come into picture and they will be managing and

controlling the public domain. And since there are lot of PHR owners each may encrypt in their own way and this may lead to discrepancies and hence we need to employ a single attribute authority.

Another disadvantage that we need to look is patient is not online always and there may be requests from each user to access PHR and even this is solved by using multiple attribute authorities and he will manage the key distribution. The access policy for each user is specified in the form of attributes and hence the name attribute based encryption. The encryption is done based one those attributes and to specific user list. Key generation is directly proportional to the number of attributes involved.

RELATED WORK

As data is outsourced, in this scheme we provide enforced encryption to data stored in cloud. In previous works, the encryption schemes used create large overheads in key generation and there exists lot of copies of same file because of encrypting with different user's keys. Due to scalability issues, Attribute based Encryption is introduced where data gets encrypted with the help of attributes and users having proper keys can only decrypt which prevents any user collusion and key management is made more efficient. Narayan proposed EHR systems where each patients 's files are encrypted using CP-ABE that gives direct revocation authority to the owners and cipher text length is directly proportional to unrevoked users. In other paper access policies are also described to share the records which are mentioned in Ibraimi's paper. And also the availability of these EHRs even when patient or health provider is offline is proposed in Akinyele'scontribution.

The drawbacks in the above discussed systems is with that there is only single authority and key escrow problem may arise due to this violating privacy concerns. This is no encouraged by the HER owner because he doesn't want anyone else having the equal authority of his and also it is very difficult to have one single authority to manage all the users requests from the public domain which will be too much for him. As there are many subdomains in this system, having a authority for each domain makes more sense and this is proposed in Ming Li's paper. In his paper they also contributed about dynamic policy changes where patient can change or revoke any access policy.Recently in Yu e al's paper, he proposed KP-Abe to secure data where PHR owner can encrypt data to share with multiple authorized users by distributing keys to those who have proper access and authorization and revocation system is more efficient due to updating of cipher texts but even this system has a drawback where multiple owners governing same attribute sets and users receive keys from different owners. In other system proposed by Chase and chow, they said about multiple AA systems where each AA governs different subset of attributes and key generation is scalable and hence prevents user collusion. In the Ming Li's and Shucheng Yu's paper ,it is said about file access policies where owner can edit his access policy instead of cipher texts and owner can chose which part of his record must be seen by users. Rujetlal proposed alternative solution for revocation policies as data owner must send updated cipher text component to every non

revoked user which in turnincrease communication overhead as there can be lot users in public domain.

PROBLEM DEFINITION

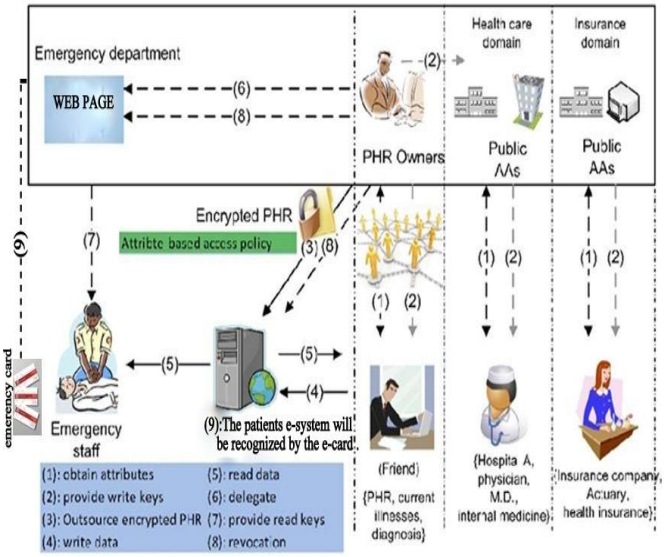
PHR users should be accessible at emergency incidents without much effort or time. The key distribution and overhead must be less. The scalability must be very high as there are lot of users in public domain. The access to PHR always must be dynamically controlled by PHR owner. Encryption and key generation must not be visible to the user or owner .User can have access to data of multiple owners. Security is really an important issue as there are many users who try to access the file beyond their privileges leading to user collusion. That is why each user in the system is preloaded with a public/private key pair and entity authentication which can be done by different challenge-response protocols.

Different users are authorized to read disjoint sets old records and those who doesn't have proper attributes satisfying the access policy should not be allowed to decrypt the PHR. When owner changed the access policy, the user's policy will be no longer valid and must not be able to access any documents in future with that old attribute. This is known as user revocation. And no user or contributor must gain control over the PHR owner. Changes to predefined policies must be allowed and flexible for the user. Scalability must be always maintained so the user and owner will feel very comfortable in using this system. Large number of users in public domain will create a possibility of overhead and it should be minimized.

PROPOSED SYSTEM

In this paper we propose a multi domain multi authority PHR system with improved emergency access module where patient distributes keys to his personal domain and he entrusts attribute authorities who distributes keys for public domain. Also patient can edit their own access policy for each PHR and revoke user whenever owner feels like. The emergency access module has more efficient approach with combination of emergency domain and finger print access without any secret key requests at the time of emergencies and it will save lot of time in accessing owner PHR's

The set of attributes managed by each attribute authority will be disjoint and no AA (attribute authority) will have control over complete set .In this way we increase the efficiency of the security and encryption we provide to the PHR owner. In the personal domain, PHR owner directly assign access privileges for personal users and encryption is done using those data attributes. We also have user revocation scheme where PHR owner can revoke access policy of any user any time. This places the patient in control of everything and protecting his privacy. In conclusion we use Multiple Authority ABE (MA-ABE) for public domain and Key Policy ABE (KP-ABE) for personal domain thus making an efficient framework for patient centric model of PHR storage in cloud.



Users obtain secret keys from AAs without interacting with owners and it binds users to their roles. They are free to specify role based access policies for PHR files.KP-ABE system manages secret keys and access rights of users in their PSD. Key size of file is linear with number of file categories accessible. Data readers download PHRs and able to decrypt them only if they have suitable attribute based keys. The write access is given by AAs if they present proper write keys. He attributes are edited in cipher text for updating sharing policy PUD collaboratively generate secret key for user which reduces workload per AA. User's role verification is easier because of many sub domains and different AAs. Thus our framework is efficient and effective for sharing the records with high scalability and security.

We also employed emergency access in our system where we can access the PHR details at that time and this comes under emergency domain and the request is handled by that particular authority. This request will be handled by him after genuine authentication of the person requested. This domain is integrated with finger print database and whenever system run his prints, his PHR can be accessed immediately which saves the time of key generation and accessing. If there are patients who cannot give fingerprints then they are redirected to emergency domain as usual and key sent to them after proper ID verification. After emergency is over, patient can revoke the access via ED .In real time scenarios the doctor/medical personnel who is going to operate on the patient will know the system in which the patient is registered by a emergency card(e-card) the patient carries with him , on which some non-confidential data is provided.

CONCLUSION

In this paper we have proposed an efficient way of sharing and storing records in semi trusted cloud using enforced encryption techniques. Here patients will have total control over their

privacy and allowing fine grained access to the users. The key management overhead is also greatly reduced. We used ABE to encrypt the data to enable role based access and for effective user revocation we used MA-ABE which also helps enabling dynamic policy changes. In this paper we even proposed new efficient system in emergency access with finger print access enhancing security and ease of access.

REFERENCES

1) M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained
Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10),pp. 89-106, Sept. 2010

2)Ming Li, Shucheng Yu, Yao Zheng, KuiRen " Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" IEEE Transactions on Parallel and Distributed Systems pp. 131- 143 Jan 2013

3) M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

4) 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.

5) V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"
Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),
pp. 89-98, 2006.

6) 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

7) 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.

8) S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM
Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010

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

10) X. Liang, R. Lu, X. Lin, and X.S. Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation," technical report,
Univ. of Waterloo, 2010.