ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
I2OR PIF 2.125

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 10, OCTOBER 2015, PP 679-682

Attribute-Based Encryption for Reliable and Secure Sharing of PHR in Cloud Computing

[1]R.Srinivas, [2]Ajay Kumar
[1]M.Tech (CS), Department of Computer Science & Engineering, Sri Indu Institute of Engineering & Technology, Sheriguda (v) Ibrahimpatnam (M), RR District, 501510
[2]Asst-professor,Department of Computer Science & Engineering , Sri Indu Institute of Engineering & Technology, Sheriguda (v)Ibrahimpatnam(M), RR District,501510
Email: srinu90v@gmail.com, mavunuri.ajaykumar503@gmail.com

Abstract— In this paper we investigating on Personal health record (PHR),which is a patient-centric model of health information exchange, and is stored at a third party i.e., cloud providers. But there are concerns such as personal health information can be exposed to third party servers and to unauthorized parties. In order to assure the patients' authority over approach to their personal PHRs, it is an assuring method to encrypt the PHRs before outsourcing. These are issues like elastic access, reliability in key management; privacy exposure and efficient user revocation have continued to be the most significant dispute towards accomplishing fine-grained, cryptographically imposed data access control. Sequentially to have control for data access to PHRs stored in semi trusted severs, a novel patient-centric structure and a suite of methods is proposed in this paper. We leverage attribute-based encryption (ABE) practices to attain scalable and fine grained data access control for personal health records to encrypt each patient's PHR file. In this paper, we concentrate on the several data owner situation, which is different from earlier works in secure data outsourcing. It divides the users in the PHR system into several security domains which decreases the key management complexity for owners and users. Simultaneously, patient confidentiality is maintained and guaranteed by exploiting multiauthority ABE.

Index Terms— Personal health records; cloud computing; data privacy; fine-grained access control; attribute-based encryption, secure sharing.

I.INTRODUCTION

Personal Health Record (PHR) idea has risen as of late. We can say that it is a patient driven model as general control of patient's data is with the patient. He can make, delete, modify and impart his PHR through the web. Because of the high cost of building and keeping up data focuses, outsider administration suppliers give PHR administration. Yet while utilizing outsider administration suppliers there are numerous security and protection dangers for the PHR. The principle concern is whether the PHR holder really gets full control of his data or not, particularly when it is put away at outsider servers which is not completely trusted. To guarantee persistent, driven protection control over their own particular PHRs, it is fundamental to give data access control components. Our methodology is to encode the data before outsourcing. PHR holder will choose which clients will get access to which data in his PHR record. A PHR document ought to accessible to just those clients who are given relating unscrambling key. Furthermore the patient should hold the right to disavow the right to gain entrance benefits at whatever point they feel it is essential. The sanctioned clients might either need to get to the PHR for Personal utilization or export purposes. We separation sorts of clients into two domains, personal space and open area. To ensure Personal wellbeing data put away on semi-trusted servers, we receive property based encryption as fundamental encryption primitive. Utilizing ABE, access arrangements are communicated focused around attributes of clients or data

In this paper, we have investigate the secure sharing, patient-centric of PHRs stored on trusted servers, and focus on addressing the challenging and complicated key management problems. In order to secure the personal health information stored on trusted servers, we use the attribute based encryption (ABE) as the key encryption primitive. Using the ABE, access policies are based on attributes of data or users which enable patient to selectively share her or his PHR among the set of users by scrambling the file under set of attributes, without need to know the complete list of users. The complexities for each encryption, key generation and decryption are linear with the number of attributes involved. But, to integrate the ABE into the PHR system, important issues such as

ISSN (ONLINE): 2349-7084
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 10, OCTOBER 2015, PP 679-682

Adaptability: "N" number of client can include into this application.

Security: For security reason we are utilizing Attribute Based Encryption Standards (AES) and Message Digest5 (MD5) calculation. We are scrambled information utilizing AES algorithm and we are encoded secret password word utilizing MD5 algorithm

Dynamic policy updates, key management scalability and efficient on-demand revocation are nontrivial to solve, and remain open up to date. To this end, we make the following contributions: i) we propose an ABE-based framework for patientcentric secure and scalable sharing of Personal Health information in cloud computing, under the multi owner settings. The users in the system are divided into two types of domains, namely Public and Personal Domains (PSDs), in order to address the key management challenges. ii) In the public domain, we use the Multi Authority ABE (MA-ABE) to increase the security and to avert key escrow problem. Every Attribute Authority (AA) in it supervises a disjoint separation of user attributes, while none of them is able to control the safety of the whole system. The mechanisms are proposed for encryption and key distribution so that PHR owners can enumerate personalized fine-grained role-based access policies during file encryption. iii) We provide an analysis of the scalability and complexity of our proposed safe PHR sharing solution, in terms of multiple metrics in calculation, storage, communication, and key management.

II.RELATED WORK

Key-Policy Attribute-based Encryption (KP-ABE): In KP-ABE outline contents are mark with individuality and private key are connected with access structures that control which figure message a client can unscramble. It is utilized for securing delicate data put away by outsiders on the web.

Key Policy Attribute Based Encryption V. Goyal, O. Pandey, A. Sahai, and B. Waters [5] proposed a key-policy attribute-based encryption (KP-ABE) scheme. KP-ABE plan, quality strategies are connected with keys and information is connected with characteristics. The keys just connected with the approach that is to be fulfilled by the qualities that are partner the information can unscramble the information. Key-policy attribute-based encryption (KP-ABE) plan is an open key encryption system that is intended for one-to-numerous interchanges. This plan empowers an information manager to lessen a large portion of the computational overhead to cloud servers. Each one document or message is encoded with a symmetric information encryption key (AEK), which is again scrambled by an open key comparing to a set of properties in KPABE, which is produced relating to a right to gain entrance structure. The information document that is scrambled is put away with the comparing characteristics and the encoded DEK. Just if the relating qualities of a document or message put away in the cloud fulfill the right to gain entrance structure of a user's key, then the client can unscramble the encoded DEK, which is utilized to decode the record or message. Constraints of KP- ABE: The principle inconvenience in the plan is that the information manager is likewise a Trusted Power (TP) in the meantime. On the off chance that this plan is connected to a PHR framework with different information holders and clients, it would be wasteful in light of the fact that then every client would accept numerous keys from various managers, regardless of the possibility that the keys hold the same set of properties

Cipher text Policy Attribute based Encryption (CP-ABE):

This strategy is utilized to keep scrambled information private [9].

Multi-Authority Attribute-Based Encryption (MA-ABE):

MA- ABE strategy permits any polynomial number of free powers to screen characteristics and convey mystery keys. An encryption can pick, for every power, a number and a set of characteristics; he can then encode a message such that a client can just unscramble in the event that he has at any rate of the given properties from every power [10].

III.ENCRYPTION MECHANISUM

Attribute-Based Encryption Attribute-Based Encryption (ABE), Information is scrambled utilizing a situated of qualities so that numerous clients who have fitting can decode. Attribute-Based Encryption (ABE) offers fine-grained access control as well as anticipates against intrigue. J. Yet it is a solitary information holder situation and subsequently it is not simple to include classes. C. Dong [5] has investigated that the information encryption plan does not oblige a trusted information server. At the same time in this plan the server knows the right to gain entrance example of the clients which permits it to construe some data about the questions. To acknowledge fine grained access control, the customary open key encryption based plans and either bring about high key administration overhead, or oblige encoding various duplicates of a record utilizing distinctive client's keys. To enhance the adaptability of the above results, one-to-numerous encryption strategies, for example, Attribute-Based Encryption

ISSN (ONLINE): 2349-7084
INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 10, OCTOBER 2015, PP 679-682

(ABE)might be utilized. The primary perspectives are to give adaptability, versatility and fine grained access control. In established model, this framework could be accomplished just when client and server are in a trusted area. In this way, the new get to control conspire that is „attribute Based Encryption (Abe)" plan was presented which comprise of key approach Attribute-Based Encryption (ABE). Notwithstanding it fizzles as for adaptability and versatility when powers at numerous levels are considered. In ABE plan both the client mystery key and the ciphertext are connected with a situated of traits. Limits of ABE: The utilization of a solitary trusted power (TA) in the framework. Single trusted power (TA makes a heap bottleneck, as well as have key escrow issue since the TA can get to all the scrambled documents. This opens the entryway for potential security presented

We use attribute-based encryption (ABE) techniques to attain scalable and fine grained data access control for personal health records to encrypt each patient's PHR file. In this paper we concentrate on the multiple data owner situation, which is distinct from previous works in secure data outsourcing. It divides the users in the PHR system into several security domains which decreases the key management complexity for owners and users. Simultaneously, patient confidentiality is maintained and guaranteed by exploiting multiauthority ABE. In emergency scenario, proposed scheme provides dynamic change of access policies or file attributes supports breakglass access and well-organized on-demand user/attribute revocation. Extensive analytical and experimental results are given which shows the security, scalability, and efficiency of our scheme.

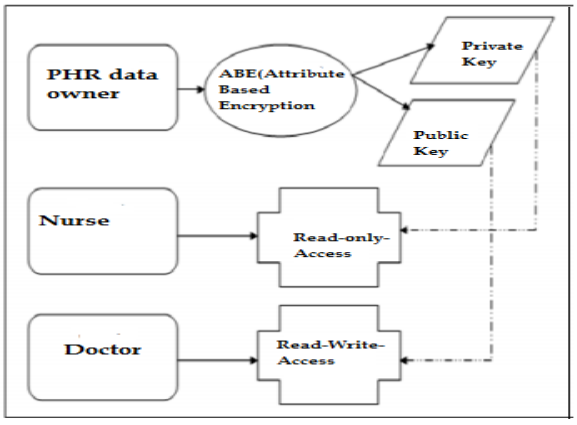

Fig 1.PHR Using ABE

IV.SYSTEM OVER VIEW

A.PHR Data Owner :The main aim of our agenda is to provide efficient key management and secure patient-centric PHR access at the same time. According to the various users' data access requirements we split the system into multiple security domains (i.e., personal domains (PSDs) and public domains (PUDs)). The PUDs consist of users who build access based on their skilled roles, such as nurses, doctors and medical researchers. The public domains can be mapped to a separate sector in the society, for instance the government, health care or insurance sector. For every PSD, PSD users are associated with a data owner (such as close friends or family members), and they build accesses to personal health records based on the access rights assigned by the owner. Every data owner (example, patient) is the trusted authority of his/her own personal domains, which uses a KPABE system to administer the access rights and secret keys of users in his/her PSD. However the PHR owner knows the users personally, to recognize patient-centric access, on a case-by-case basis the owner is at the top position to grant user access privileges. For personal domains, data attributes are defined which are referred to the essential properties of the personal health record data, for instance the type of a PHR file. For the function of PSD access, each PHR file is named with its data attributes, as the key size is known with the number of file categories a user can access.

However the number of users in a personal domain is small, it reduces the load for the owner. While encrypting the data for PSD, the owner needs to know is the essential data properties.

B. Cloud Server: In this section, we consider the server to be the semi trusted, i.e., honest but curious. The server will attempt to detect as much secret information in the stored Personal Health Record files as possible, but they will directly follow the protocol in general. Alternatively, some users will try to access the files beyond their rights. For example, the pharmacy wants to obtain the prescriptions of patients for boosting and marketing its profits. To do so, they may join together with the server or even either the other users. Additionally, we assume every user in our system is preloaded with a private/ public key pair, and entity authentication can be prepared by traditional challenge response protocols.

C. Characteristic based Access Policy: In our system, there are multiple owners, multiple nurses, multiple users and multiple Doctors. Additionally, two ABE systems are involved. We name the users having write and read access as data readers and contributors respectively. We use Attribute based encryption algorithm for it.

D. Data confidentiality: Attribute Based Encryption-encrypted PHR files are upload to the server by the

owners. Every owner's PHR file is ciphered both under a certain role-based and fine grained access policy for users from the public domain to access and under a chosen group of data attributes that allows access from users in the personal domain. The PHR files can be decrypt by the authoritative users, excluding the server

Crypto System

Touchy information is imparted and put away on cloud server; there will be a need to encode information put away at outsider. In Quality based encryption figure content named with set of characteristic. Private key connected with access structure that control which figure message a client can unscramble. Utilizing ABE, access arrangements are communicated focused around the qualities of clients or information, which empowers a patient to specifically impart her PHR among a set of clients by scrambling the document under a set of characteristics, without the need to know a complete arrangement of the clients. The complexities for every encryption, key era and unscrambling are just direct with the amount of traits included. Nonetheless, to incorporate ABE into a vast scale PHR framework, essential issues, for example, key administration versatility, dynamic arrangement overhauls, and effective on-interest disavowal are non-recovery to settle, and remain to a great extent open breakthrough

V. CONCLUSION

In this paper we made a review on the Enhancing the Security on Personal health Record Framework in cloud computing. Furthermore likewise Attribute Based Encryption is the great method to securing the Health records. We use Attribute Based Encryption to encipher the Personal Health Record data, hence that patients can permit access not only by personal users, but also many users from public domains with different professional roles, affiliations and qualifications. In addition, we enhance an existing Multi Authority Attribute Based Encryption scheme to manage on-demand user revocation, efficient, and prove its security.

REFERENCES

[1] 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.

[2] Ming LiShucheng Yu, Yao Zheng,Kui Ren, 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, vol. 24, no. 1, january 2013.

[3] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption", master" s thesis, Worcester Polytechnic Inst., 2011.

[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. 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.

[6] 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.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proc. IEEE Symp. Security and Privacy (SP " 07), pp. 321-334, 2007.

[8] Q.Wang et al.,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS „09, Sept. 2009, pp. 355–70.

[9] 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.

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

[11] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010

[12] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.

[13] Melissa Chase "Multi-authority Attribute based Encryption," Computer Science Department Brown University Providence, RI 02912