International Journal Of Engineering Research & Management Technology ISSN: 2348-4039

IJERMT

July- 2014 Volume 1, Issue-4

Email: editor@ijermt.org www.ijermt.org

SECURE DISTRIBUTION OF PERSONAL HEALTH RECORDS IN CLOUD COMPUTING BY APPLYING ATTRIBUTE-BASED ENCRYPTION

A.Srikanth
M.Tech:
Department of CSE
SIETK, Puttur, INDIA

A.Dhasaradhi
Associate Professor
Department of CSE
SIETK, Puttur, INDIA

P.Nirupama
Head of the department
Department of CSE
SIETK, Puttur, INDIA

Abstract—

Health record is internet base appliance that enable individuals to accessed and organize their permanent health data .The patient central protected distribution of PHR is succeed by store them in an exceedingly third party server, like cloud server. Cloud server gives a capable platform for storage of information. every patient is secure the total management of his/her medical records and may share his/her health knowledge with a good vary of users, as well as aid suppliers, members of the family or friends. The Patient's solely decide that set of users will access that set of files .To achieve fine-grained date access management for private health records, use attribute based mostly coding to encipher the information before outsourcing. This paper focuses on the multiple knowledge owner situations, and divides the users within the PHR system into multiple security domain that greatly reduces the key management quality for homeowners and users. For multiple authority based mostly access management mechanism, use Multi Authority based mostly coding (MA-ABE).

Keywords:

Personal health records, cloud computing, knowledge privacy, fine-grained access management, attribute-based coding.

INTRODUCTION

A personal health record (PHR) may be a assortment of knowledge pertinent to a patient's health. It permits a patient to form, handle, and organize his/her personal health knowledge in one place through the online. Patients will management the health data in PHR and may compass anyplace at any time with net access. Every patient has assured the total management of his/her personal health records. It's shared with wide selection of users, like aid suppliers, relatives or friends attributable to the high value of building and maintaining specialized

knowledge centers, several PHR services area unit outsourced to or provided by third-party service suppliers, for instance, Microsoft Health Vault .Recently , architectures of storing PHR's in cloud computing are projected , however whereas exploitation third party service suppliers there area unit several security and privacy risks for PHR. The most concern is whether or not the PHR owner really gets full management of his knowledge or not, particularly once it's keep at third party servers that isn't absolutely trust worthy . To confirm patient-centric privacy management over their own PHRs, it's essential to produce knowledge access management mechanisms. Our approach is to encode the information before outsourcing. PHR owner can decide that users can get access to that knowledge in his PHR record. A PHR file ought to out there to solely those users United Nations agency square measure given corresponding decipherment key.

What is more, the patient shall forever retain the proper to not solely grant, however conjointly revoke access privileges once they feel it's necessary. The approved users might either have to be compelled to access the PHR for private use or skilled functions. We have a tendency to divide forms of users into 2 domains, personal domain and property right. The latter has probably giant scale; ought to every owner herself be directly to blame for managing all the skilled users, she is going to simply be flooded by the key management overhead. additionally, since those users 'access requests square measure usually unpredicted-able; it's troublesome for associate degree owner to see an inventory of them .On the opposite hand, completely different from the only knowledge owner situation thought-about in most of the prevailing work in an exceedingly PHR system, there square measure multiple homeowners United Nations agency might encode in line with their own ways that, probably victimization completely different sets of crypto-graphic keys .To protect personal health knowledge keep on semi-trusted servers, we have a tendency to adopt attribute-based coding as main coding primitive. Using ABE, access policies square measure expressed supported attributes of users or knowledge.

Scalability: 'N' variety of users will be more into this application.
Security: We have a tendency to square measure victimization Attribute based mostly coding for security purpose. The information is encrypted victimization RSA.

CONNECTED WORK

A. Symmetric Key Cryptography (SKC) Based Mostly Solutions

Vimercati ET.AL.Projected an answer for securing outsourced knowledge on semi-trusted servers supported trigonal key derivation ways, which may bring home the bacon fine-grained access management. Sadly, the complexities of file creation and user grant/revocation operations square measure linear to the quantity of approved a user that is a smaller amount ascendable. In [4], files in an exceedingly PHR square measure organized by graded classes so as to create key distribution additional economical. However, user revocation isn't supported.

The SKC-based solutions have many key limitations. First, the key management overhead is high once there square measure an outsized variety of users and homeowners, that is that the case in an exceedingly PHR system. The key distribution will be terribly inconvenient once there square measure multiple homeowners, since it needs every owner to forever be on-line. Second, user revocation is inefficient, since upon revocation of 1 user, all the remaining users are going to be affected and therefore the knowledge have to be compelled to be re-encrypted. What are the more, users write and browse rights aren't severable.

B. Public Key Cryptography (PKC) Based Mostly Solutions :

PKC based mostly solutions were projected attributable to its ability to separate write and browse privileges. Benalohet. Al projected a theme supported graded identity based mostly coding (HIBE), wherever every class label is thought to be associate degree identity. However, it still has probably high key management overhead. so as to influence the multi-user situations in encrypted search, Dong et.al. Projected an answer supported proxy coding . Access management will be enforced if each write and browse operation involves a proxy server. However, it doesn't support fine-grained access management, and is additionally not collusion-safe Attribute-based coding (ABE). The SKC and ancient PKC based mostly solutions all suffer from low measurability in an exceedingly giant PHR system, since file coding is completed in associate degree matched manner, whereas every PHR might have random sizable amount of users. To avoid such inconveniences, novel one-to-many coding ways like attribute-based coding will be used. Within the seminal paper on ABE, knowledge is encrypted to a bunch of uses characterized by a group of attributes that probably makes the key management a lot of economical. Since then, many works used ABE to appreciate fine-grained access management for outsourced knowledge. However, they need not addressed the multiple knowledge owner settings, and there lacks a framework for patient-centric access management in multi-owner PHR systems. Note that, in one authority for all users and patients is adopted. However, this suffers from the key written agreement drawback, and patients' privacy still can't be secure since the authority has keys for all house owners. CP-ABE could be a policy to amass complicated management on encrypted knowledge. This system is employed to stay encrypted knowledge confidential. However, they still assume one public authority, whereas the difficult key-management problems stay mostly unresolved. However, there are many common drawbacks of the higher than works. First, they typically assume the utilization of one sure authority (TA) within the system. This not solely might produce a load bottleneck, however additionally suffers from the key written agreement drawback since the metal will access all the encrypted files, gap the door for potential privacy exposure. Additionally, it's not sensible to delegate all attribute management tasks to 1 metal, together with certifying all users' attributes or roles and generating secret keys.

C. Cipher Text Policy Attribute Primarily Based Secret Writing (CP-ABE) :

CP-ABE could be a policy to amass complicated management on encrypted knowledge. this system is employed to stay encrypted knowledge confidential . First, they typically assume the utilization of one sure authority (TA) within the system. This not solely might produce a load bottleneck, however additionally suffers from the key written agreement drawback since the metal will access all the encrypted files, gap the door for potential privacy exposure. Additionally, it's not sensible to delegate all attribute management tasks to 1 metal, together with certifying all users' attributes or roles and generating secret keys.

D. Key-Policy Attribute-Based Secret Writing (KP-ABE) :

KP-ABE could be a crypto system for fine grained sharing of encrypted knowledge. The key-policy ABE outsourced knowledge in to the cloud wherever one knowledge owner will inscribe her knowledge and share with multiple licensed users, by distributing keys to them that contain attribute-based access privileges. They additionally propose a technique for the information owner to revoke a user with efficiency by relegating the updates of affected cipher texts and user secret keys to the cloud server. Since the key update operations are aggregative over time, their theme achieves low amortized overhead.

FRAMEWORK FOR SECURE AND ASCENDIBLE PHR SHARING:

A. Necessities:

To achieve patient-centric PHR sharing, a core demand is that every patient wills management WHO are licensed to access to her own PHR documents. Particularly revocation is that the core security objectives for any electronic health record system, detected by Mandela in as early as 2001. The safety and performance necessities are summarized as follows:

B. Knowledge Confidentiality :

Unauthorized users (including the server) WHO don't possess enough attributes satisfying the access policy or don't have correct key access privileges ought to be prevented from decrypting a PHR document, even below user collusion. Fine-grained access management ought to be implemented, which means totally {different\|completely different} users are licensed to scan different sets of documents.

C. On-Demand Revocation:

Whenever a user's attribute is not any longer valid, the user shouldn't be able to access future PHR files victimization that attribute. this can be typically known as attribute revocation, and also the corresponding security property is forward secrecy . There's additionally user revocation, wherever all of a user's access privileges are revoked.

D. Knowledge Access Policies:

The data access policies ought to be versatile, i.e., dynamic changes to the predefined policies shall be allowed , particularly the PHRs ought to be accessible below emergency situations.

E. Measurability Potency And Value

The PHR system ought to support users from each the non-public domain and public domains. Since the set of users from the general public domain is also giant in size and unpredictable, the system ought to be extremely ascendible, in terms of complexness in key management, communication, computation and storage. In addition, the owners' efforts in managing users and keys ought to be reduced to get pleasure from usability.

F. Architecture:

Fig.1 Depicts the projected system design for secure sharing of non-public health record. During this projected system, the system is split into 2 security domains, like personal domain (PSDs) and property right (PUDs). The division is disbursed in step with the user's knowledge access necessities .The PUDs includes users WHO create access supported their skilled roles, like doctors, nurses and insurance agents. Users within the personal domain area unit in person related to the patient like relations or friends. Here, {the knowledge\ the info \ the information} owner WHO possess the PHR and data reader WHO will access the encrypted PHR.

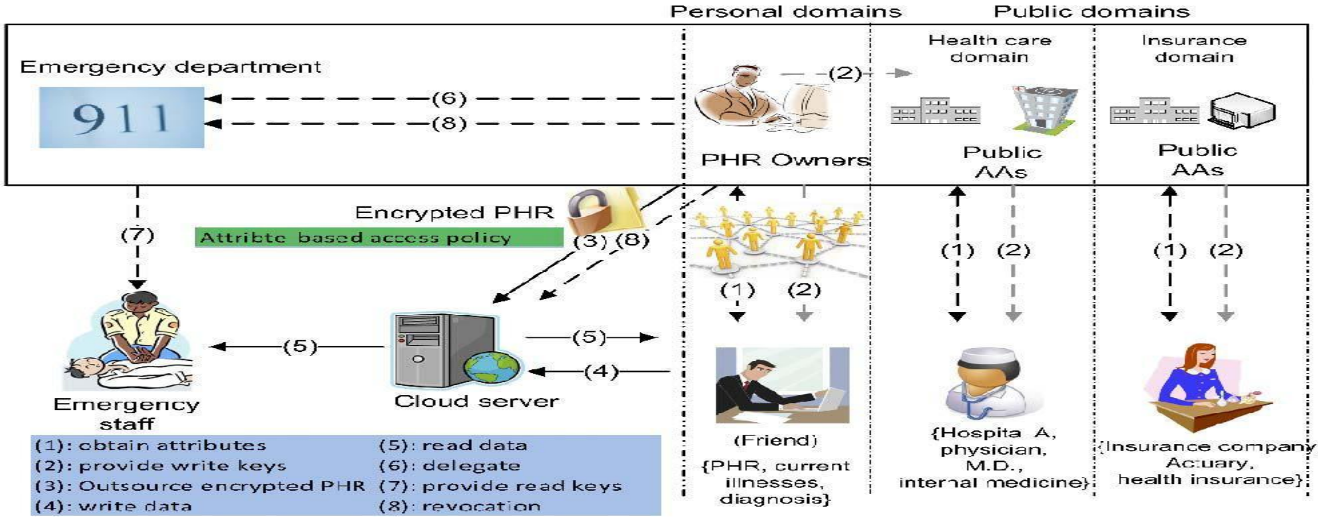

Fig : 1 The projected framework for patient-centric, secure and ascendible PHR sharing on semi trusty storage beneath multi owner settings .

In the PSD, the owner makes use of key-policy attribute based mostly secret writing. The owner generates the key keys for PSD users. The multi-authority attribute based mostly secret writing is employed within the pudding. Secret keys for pudding users area unit generated by the attribute authorities reckoning on their profession.

G. Details Of The Planned Frame Work

In our frame there is a unit multiple SD's, multiple homeowners, multiple AA's, and multiple users. Additionally, 2 ABE systems area unit involved for every PSD the YWRL revocable KP-ABE theme is adopted for every pudding, our planned rescindable MA-ABE theme is employed.

- **System Setup And Key Distribution**

The system 1st defines a typical universe of information attributes shared by each PSD, like "basic profile" , "medical history", "allergies" and "prescriptions". Associate emergency attribute is additionally outlined for break-glass access. Every PHR owner's consumer application generates its corresponding public / master keys. The general public keys may be printed via user's profile in an internet attention social-network (HSN).

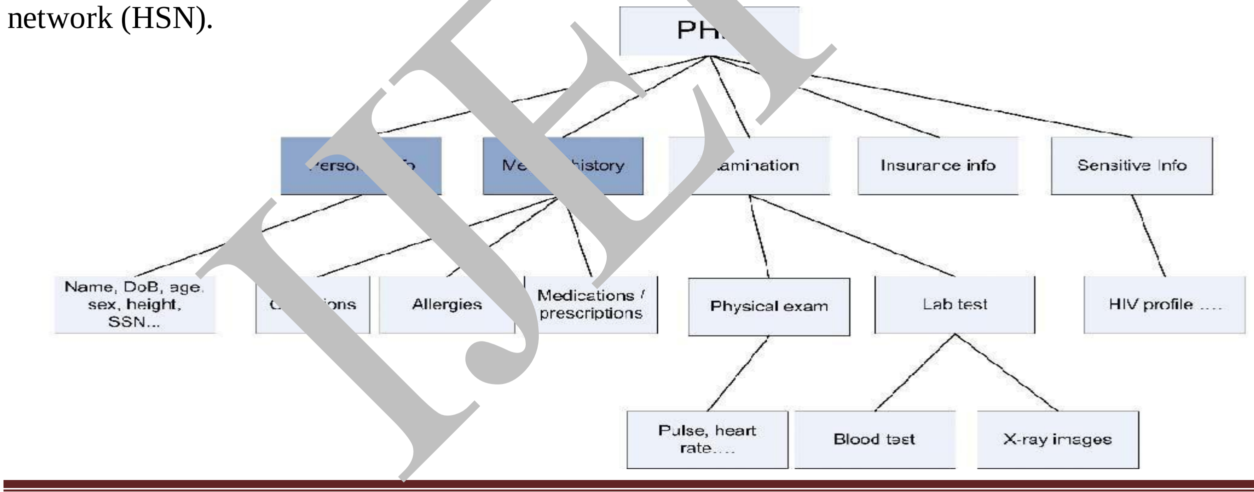

Fig : 2 The attribute hierarchy of files—leaf nodes are atomic file classes whereas internal nodes are compound classes. Dark boxes are the classes that a PSD's knowledge reader has access to.

There square measure 2 ways in which for distributing secret keys. First, once 1st mistreatment the PHR service, a PHR owner will specify the access privilege of an information reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a very method resembling invites in Google Doc. Second, a reader in PSD might acquire the key by causation missive of invitation (indicating that sorts of files she desires to access) to the PHR owner via HSN, and also the owner can grant her a set of requested knowledge sorts .Based on that, the policy engine of the applying mechanically derives AN access structure, and runs key gen of KP-ABE to get the user secret key that embeds her access structure. Additionally, the info attributes is organized in a very hierarchic manner for economical policy generation see Fig. 2. Once the user is granted all the file sorts below a class, her access privilege are painted by that class instead.

- **PHR Secret Writing And Access :**

The homeowners transfer ABE encrypted PHR files to the server. Every owner's PHR file is encrypted each below a precise fine-grained and role primarily based access policy for users from the pudding to access, and below a particular set of knowledge attributes that enables access from users within the PSD. Solely licensed users will rewrite the PHR files, excluding the server.

- **Break-Glass:**

When AN emergency happens, the regular access policies could not be applicable. To handle this case, break-glass access is required to access the victim's PHR. In our framework, every owner's PHR's access right is additionally delegated to AN emergency department (ED, [24]). to forestall from abuse of break-glass choice, the emergency employees must contact the impotence to verify her identity and also the emergency scenario, and acquire temporary scan keys [25]. When the emergency is over, the patient will revoke the nascent access via the impotence.

CONCLUSION

In this project, we've designed the planned framework for the attribute encoding primarily based PHR sharing with authentication. The total management of the non-public health record are perpetually remained the patient and therefore the privacy is assured through the encoding. We tend to use varied attribute primarily based encoding techniques to cipher the PHR files. So the patient will permit access to users supported the attributes provided by the patient. The information attributes area unit outlined for private domain users and role attributes for the users publicly domain. The patient can even revoke a user expeditiously during this planned theme.

Acknowledgments: We would in earnest convey our Supervisor for all his valuable comments and active support.

REFERENCES

1. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based coding for fine-grained access management of encrypted information,” in CCS '06, 2006, pp. 89–98
2. H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, “Securing the E-Health Cloud,” Proc. initial ACM Int’l Health science Symp.(IHI ’10), pp. 220-229, 2010
3. M. Li, S. Yu, N. Cao, and W. Lou, “Authorized personal Keyword Search over Encrypted Personal Health Records in Cloud Computing,” Proc. thirty first Int’l Conf. Distributed Computing Systems (ICDCS ’11), June 2011
4. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled encryption: guaranteeing privacy of electronic medical records,” in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 103–114.
5. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable and fine-grained information access management in cloud computing” in IEEE INFOCOM'10, 2010.
6. S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based mostly information Sharing with Attribute Revocation,” Proc. Fifth ACM Symp. data, pc and Comm. Security (ASIACCS ’10), 2010.
7. K.D. Mandl, P. Szolovits, and I.S. Kohane, “Public Standards and Patients’ Control: the way to Keep Electronic Medical Records Accessible however personal,” BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.
8. J. Hur And D.K. Noh, “Attribute-Based Access management With economical Revocation In information Outsourcing Systems,” IEEE Trans. Parallel And Distributed Systems, Vol. 22, No. 7, Pp. 1214-1221, July 2011.