ISSN (Online): 2349-7084

GLOBAL IMPACT FACTOR 0.238

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS VOLUME 1, ISSUE 4, OCTOBER 2014, PP 214-219

Securing Personal Health Records in Cloud Utilizing Multi Authority Attribute Based Encryption

Meghana A [1], **Gaddam Gowthami**[2], **Mahendrakar Kavitha Bai** [3], M.**Srilakshmi** [4]

Department of IT, G.Pullaiah College of Engineering and Technology. Kurnool
JNTU Anatapur, Andhra Pradesh, India

Abstract: Personal health record is keep up in the bring together server to keep up patient's personal and diagnosis information Personal health record (PHR) is a developing patient-driven model of wellbeing data trade, which is regularly outsourced to be put away at an outsider, for example, cloud providers. Nonetheless, there have been wide security concerns as personal health data could be presented to those outsider servers and to unapproved gatherings. The security plans are utilized to ensure individual information from free. To guarantee the patients' control over access to their PHRs, it is a swearing up and down to method to scramble the PHRs before outsourcing .In this paper we propose novel patient-driven framework and suite of component for information access control to PHR's put away in semi trusted servers. To accomplish fine-grained and versatile information access control for PHRs, we influence attribute based encryption (ABE) methods to scramble each patient's PHR record. Information holder redesigns the Personal information into outsider cloud server farms. Various information managers can get to the same information values. Our scheme helps effective on-interest client/attribute renouncement.

Keywords: Attribute-based encryption, cloud computing, data privacy, fine-grained access control, Personal health records, revocation

1. INTRODUCTION

Cloud computing is a rising figuring innovation where applications and all the administration are given by means of Web. It is a model for empowering on- interest system access to pool assets. Cloud computing can be considered as a processing ideal model with more noteworthy adaptability and accessibility at lower cost. In late year, Personal Health Record (PHR) has created as the developing pattern in the health awareness engineering and by which the patients are effectively ready to make, oversee and impart their individual wellbeing data. This PHR is currently a day's put away in the mists for the expense decrease reason and for the simple imparting and access instrument. The primary worry about this PHR is that whether the patient has the capacity controls their information or not. It is exceptionally fundamental to have the fine grained access control over the information with the semi-trusted server. Anyway in this the PHR framework, the security, protection and wellbeing information privacy are making difficulties to the clients when the PHR put away in the outsider stockpiling region like cloud administrations. The PHR information ought to be secured from the outer assailants furthermore it ought to be secure from the inner aggressors such that from the cloud server association itself. At the point when the PHR manager transfer the PHR information to the cloud server, the holder is losing the physical control over the information and accordingly the cloud server will get the right to gain entrance on the plain content information and it will make loads of security difficulties to the PHR protection and secrecy. The encryption of information before outsourcing it to the outsider is considered as the guaranteeing methodology towards information security and classifiedness towards the outsider stockpiling. Security dangers accomplished by clients of administrations offered by Fruit Inc. Google Inc., Amazon Inc.[1] are clear evidences that cloud is inherently shaky from a client's perspective point. Since clients don't have entry to cloud administration suppliers inside operations safeguarding security of client in cloud environment is a test for analysts. Cloud computing administrations profit from economies of scale attained through flexible utilization of assets, specialization, and different efficiencies. The Web has developed into an universe of its own, and its colossal space now offers abilities that could help Doctors in their obligations in various ways. As of late, is a rising pattern and PHR is a patient-driven model of wellbeing data trade and administration. Generally, PHR administration permits a client to make, oversee, and control her individual wellbeing information in one spot through the web, which has made the stockpiling, recovery, and offering of the therapeutic data more productive.

In Cloud computing, there are distinctive existing plans that give security, information secrecy and access control. Clients need to impart touchy items to others focused around the beneficiary's capacity to fulfill an arrangement in circulated frameworks. This paper is basically identified with works in cryptographically authorized access control for outsourced information and trait based encryption. To acknowledge fine-grained access control, the customary Public key encryption (Pke) based plans [8] either acquire high key oversee men overhead, or oblige scrambling various duplicates of a record utilizing diverse clients' keys. To enhance the adaptability of the above arrangements, one-to-numerous en-grave particle techniques, for example, ABE can be utilized. In Goya let. all's fundamental paper on ABE [11], information is encoded under a situated of qualities so that numerous clients who have fitting keys can unscramble. This conceivably makes encryption and key administration more proficient [12]. Crucial property of ABE is avoiding against client agreement. At the early phases of the Cloud computing and Personal Health Record the customary encryption methods were connected to the Personal Health Record and now a days the progressed encryption procedures

2. RELATED WORK

Key-Policy Attribute-based Encryption (KP-ABE): KP-ABE is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet.

Cipher text Policy Attribute based Encryption (CP-ABE): CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential [9].

Multi-Authority Attribute-Based Encryption (MA-ABE): MA-ABE method allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k [10].

3. PROPOSED SYSTEM

Personal Health Record is an online primarily based application that enables individuals to access and co-ordinate their lifelong health information and build if acceptable elements of its accessible to people who would like. Personal Health Record’s security and protection of its information are of nice concern and a subject matter of analysis over the years. There square measure many various sorts of cryptanalytic mechanisms like AES, MD5 planned to ensure information security. During this paper, we tend to attempt to study the secure sharing, patient-centric of PHRs keep on trustworthy servers, and target addressing the difficult and complex key management issues. so as to secure the non-public health info keep on trustworthy servers, we tend to use the attribute primarily based encoding (ABE) because the key encoding primitive. victimization the ABE, access policies square measure supported attributes of knowledge or users that modify patient to by selection share her or his PHR among the set of users by scrambling the file beneath set of attributes, while not have to be compelled to apprehend the entire list of users. The complexities for every encoding, key generation and cryptography square measure linear with the quantity of attributes concerned. But, to integrate the ABE into the PHR system, vital problems like dynamic policy updates, key management quantifiability and economical on-demand revocation square measure nontrivial to resolve, and stay open up thus far. To the current finish, we tend to build the subsequent contributions:

i) We tend to propose associate degree ABE-based framework for patient central secure and ascendable sharing of non-public Health info in cloud computing, beneath the multi owner settings. The users within the system square measure divided into 2 kinds of domains, particularly Public and private Domains (PSDs), so as to handle the key management challenges.

ii) Within the property right, we tend to use the Multi Authority ABE (MA-ABE) to extend the protection and to avert key written agreement drawback. Each Attribute Authority (AA) in it supervises a disjoint separation of user attributes, whereas none of them is in a position to regulate the protection of the complete system. The mechanisms square measure planned for encoding and key distribution so PHR house owners will enumerate personalized fine-grained role-based access policies throughout file encoding.

iii) We offer associate degree analysis of the quantifiability and quality of our planned safe PHR sharing answer, in terms of multiple metrics in calculation, storage, communication, and key management.

4. METHODOLOGY

4.1 Requirements:

The most vital task is to attain patient-centric PHR sharing. That means, the patient ought to contain the elemental management over their own health record. It additionally determines that users ought to have access to their medical information. The user management write/read access and revocation square measure 2 main security functions for any kind of electronic health record system. The write access management is controlled by the person to forestall in PHR context entitles by the unauthorized users to induce access on the record and to modifying it.

4.2 Framework:

The purpose of our framework is to supply security of patient-centric PHR access and economical key management at identical time. If users attribute isn't valid, then the user is unable to access future PHR files victimization that attribute. The PHR information ought to support users from the non-public domain similarly as property right. The general public domain might have a lot of variety of users United Nations agency could also be in vast quantity and unpredictable, system ought to be extremely ascendable in terms of quality in key Management system communication, computation and storage. The owner's Endeavour in managing users and keys should be reduced to relish usability. By victimization attribute primarily based encoding we are able to encipher personal health records self-protective that's they will access solely licensed users even on a semi trustworthy server. By victimization ABE to handle the key management Challenges, we tend to divide the users into 2 kinds of domains; they're public and private domain. For private domain KP-ABE theme is employed. For property right MA-ABE theme is employed and therefore the PHR is in restraint of source agent. Here we tend to propose a completely unique plan that is associate degree enhance MA-ABE so; the user can have full management on their own PHR.

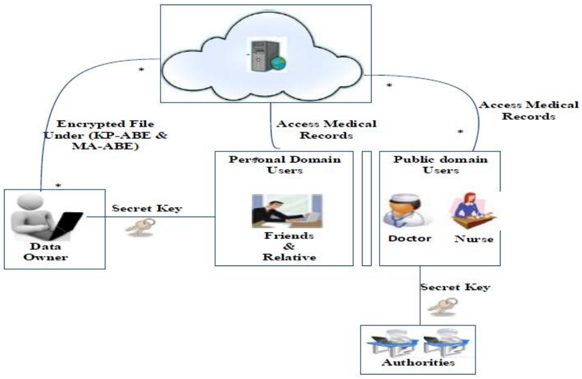

Fig 1 Architecture of Sharing Patient Health Record

Multi-authority Attribute Based Encryption

The multi-authority attribute based encryption writing theme is a sophisticated attribute based encryption writing within which it'll have several attribute authority for handling varied set of users from various domains [5]. within the PHR system the users are going to be from completely different domain just like the doctors from health care organizations, the buddies and family from personal relations and alternative users from insurance domain too. Therefore every user is going to be having completely different access management mechanism supported the relation with the patient or owner. So the MA-ABE theme can extremely utilize.

Key Policy Attribute based Encryption:

It is the changed sort of the classical model of ABE. Exploring KP-ABE theme, attribute policies area unit associated with keys and information is related to attributes. The keys solely related to the policy that's to be happy by the attributes that area unit associating the info will decode the info. Key Policy Attribute based encryption (KP-ABE) theme may be a public key secret writing technique that's designed for onto-many communications. This theme permits a knowledge owner to scale back most of the procedure overhead to cloud servers. The employment of this Attribute based encryption KP-ABE provides fine-grained access management.

Enhanced Key-Policy Generation Rule: additionally to the fundamental key-policy generation rule, the attribute tuples assigned by an equivalent AA for various users don't ran into with one another, as long as their primary attribute sorts area unit distinct.

Enhanced secret writing Rule: additionally to the fundamental secret writing rule, as long as there is a unit multiple attributes of an equivalent primary sort, corresponding no intersected Attribute tuples area unit enclosed within the cipher text's attribute set.

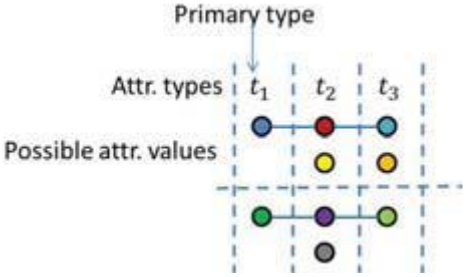

Fig 2. Illustration of the enhanced key-policy generation rule. Solid horizontal lines represent possible attribute associations for two users.

5. TECHNIQUES

5.1 Attribute Based Encryption

The information security is provided by mistreatment using Attribute Based Encryption techniques. During this the sensitive info is shared and keeps within the cloud provider; it's required to code cipher text that is assessed by set of attributes. The personal secret is related to access build to manage with cipher text a user is ready to decode. Here we have a tendency to area unit mistreatment Attribute Based Encryption (ABE) because the principal cryptography primitive. By mistreatment ABE access policies area unit declared supported the Attributes of user information, that change to by selection share her/his, PHR among a collection of users to encrypting the file underneath a collection of attributes, while not a desire of complete users. The complexness per cryptography, security key generation, and decoding area unit solely linear with multi range of attributes area unit enclosed. After we integrate ABE into an outsized scale of PHR system, the necessary dispute like dynamic policy updates, key management and measurability associated an economical on Demand revocation is non-retrieval to resolve.

5.2 Cipher Text Policy Attribute primarily based cryptography

Cipher Text Policy Attribute primarily based cryptography is one in every of the cryptography techniques in associate attribute based cryptography that is employed to code the information supported associate access policy, that relies on the information or the user attributes. If the key secret is matching with the access management policy [3] then the decoding is feasible. The key-plan of the CP-ABE is: the key of the user is expounded with a collection of attributes and every cipher text is enclosed with associate access structure. The message is decrypted by the user given that the attributes of the user's consummated with associate access structure of the cipher text [5].This technique have the profit like the plain text can't be accessed by the third party server, once the key matched with access policy on the user attributes then the decoding is feasible, and each user is needed correct authorization and authentication to access the data. The user revocation is troublesome by this CPABE theme. Whenever the user access right needs to vary by the owner, it's not possible to try and do changes with efficiency with this theme.

5.3 Key-Policy primarily based Encryption:

Key-Policy primarily based Encryption is one in every of the attribute based cryptography technique within which the information is expounded with the attributes, a public key part is outlined for every of this. During this methodology, every user are going to be appointed to associate access structure is appointed by every user that used establish which sort of cipher texts is employed for decoding [6]. The access structure is discovered by this secret key. If the information attribute suit to the user's access structure then solely the user are going to be ready to decode a cipher text. Key-Policy primarily based Encryption and also the key-policy attribute based encryption is sort of functioning during a similar manner, however they need some variation in terms of characteristic the access policy for the users.

5.4 Multi-Authority ABE

A Multi-Authority ABE system is enclosed with k attribute authorities and one central management. The worth dk is appointed to each attribute authority. During this projected system we will use the subsequent algorithmic programs: The random algorithm is +++++passing the central authority or another trustworthy security. It takes input as a security parameter and outputs as a public key and secret key combine for every of the attribute authorities and additionally outputs as a system public key and master secret key, that is employed for central authority.

Attribute Key Generation: A random algorithmic program is pass associate attribute authority. The key secret is to require as associate input for security authority and also the authority's price dk, a user's GID, and a collection of attributes within the authority's domain and output secret key for the user.

Central Key Generation: A central authority is used be pass a random algorithmic program. It takes the master as associate input and a user's GID and outputs secret key for user.

Encryption: This system is passing a sender. Take a collection of attributes as associate input for every authority, and also the system public key. The outputs area unit within the variety of cipher text.

Decryption: This mechanism is done by a receiver. Takes input as a cipher text that was encrypted underneath a collection of decoding keys for attribute set. By mistreatment this ABE and MA-ABE it'll increase the system measurability; there are a unit some Restriction in building PHR system. The ABE doesn't handle it with efficiency. In this state of affairs one might regard with the assistance of attributes primarily based broadcast cryptography.

6. SECURITY MODEL FOR IMPLEMENTATION SYSTEM

6.1 information confidentiality:

This analysis set up reveals the information concerning every user to access on the PHR among each other. The various sets of documents area unit approved by the users to scan the document.

6.2 User Access Privilege Confidentiality: The system doesn't disclose the rights from one person to a different. This ensures the user to access robust confidentiality. And additionally it maintains each property right and personal domain. Secure Sharing of private Health Records System designer maintain Personal Health Records with varied user access points. These information values area units managed underneath a 3rd party cloud supplier system. The cloud supplier can give security for the information. Multiple modules is provided by this technique. Data owner is intended to manage the patient details. With multiple attribute collections the PHR is maintained. Access permission to totally different authorities is appointed by information header. Cloud providers module is employed to store the PHR values. The encrypted PHR is uploaded by the information header to the cloud supplier. Patients will access information and additionally maintained underneath the cloud supplier. Key management is one in every of the most tasks to set up and key values for varied authorities. The owner of the information can update the key values. This dynamic policy relies on key management theme. Patient's area unit accessed by the shopper module. This technique uses the non-public and skilled access pattern. Access classification is employed to produce multiple attributes. Client's access to log maintains to the user request info to method auditing.

7. CONCLUSION

A framework of secure sharing of private health records has been projected during this paper. We will give smart security to our information mistreatment cryptography technique in cloud. Public and private access models mechanism. The framework addresses the distinctive challenges brought by multiple PHR homeowners and users; in this the complexness of key management is greatly reduced. The attribute-based cryptography model is increased to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records area unit maintained with security and privacy.

REFERENCES

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

[2] Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[4] H. L ¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium , ser. IHI ’10, 2010, pp. 220–229.

[5] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertextpolicy attribute-based encryption,” in IEEE S& P ’07,2007, pp. 321–334

[6] X. Liang, R. Lu, X. Lin, and X. S. Shen, “Ciphertext policy attribute based encryption with efficient revocation,” Technical Report, University of Waterloo,2010.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Ciphertext-policy attribute-based threshold decryption with flex- ible delegation and revocation of user attributes,” 2009.

[8] 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,” in SecureComm’10, Sept. 2010, pp. 89–106.

[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] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in ASIACCS’10, 2010

.