International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1		**VOL**	02
Website	icssccet.org		**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016		**Accepted**	10 - March – 2016
Article ID	ICSSCCET048		**eAID**	ICSSCCET.2016.048

Survey of Design and Implementation of Fine-Grained Authorized Access Control for Health Care Application on Cloud

Abinayakumari T[1], Akshitha Vijaylakshmi G[2], Deenak Johnson[3], Hasim S[4]
[1,2,3,4] UG Scholar, Department of IT, Karpagam Institute of Technology, Coimbatore, Tamilnadu, India.

Abstract: *Personal health record (PHR) was an emerging patient centric model in health information exchange, which was very often outsourced in stored at third party, such as cloud providers. However, there have been wide privacy concerns as personal health information will be exposed to those third parties servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it was promising method to encrypt the PHRs before outsourcing. The issues such as risks of data exposure, scalability of the key management, very flexibleaccess, and efficient user revocation, will be remain as the important challenge inorder to achieve fine-grained, cryptographically enforced data access control. In this paper, we proposed a novel patient-centric framework and a suite of mechanism for the data access control to PHRs will be stored the in semi-trusted servers. Inorder to get a fine-grained and scalable data access control for PHRs, the attribute-based encryption (ABE) technique inorder encrypt each patient's PHR file. Different from previous works in the secure data outsourcing, and we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that will greatly reduce the key management complexity for owners and users. High degree of patient privacy is been guaranteed simultaneously by exploiting multiauthority Attribute Based Encryption .The scheme enables dynamic modification of access policies or file attributes, supports in efficient on-demand user/attribute revocation and break-glass access under the emergency scenario. Extensive analytical and experimental results were presented which shows the needs for security, scalability, and the efficiency of our proposed scheme.*

Keywords: *Cloud storage, re privacy preserving, homomorhic based encryption, DES encryption, attribute based encryption*

INTRODUCTION

Access control is concerned to protect system resources against unauthorized accessing. It also defines the process by which the usage of system resources is regulated according to an access control policy.It is exclusively permitted by an authorized entities (users, programs, processes, or other systems) according to the policy. Role-Based Access Control (RBAC) models are receiving increase in attention as a recent generalized approach to the access control. It also differs from the traditional identity based access control in that it can take some advantage of the concept of the role related to that system and then simplifies authorization administration because the security administrator needs only to revoke and to assign the new appropriate role membership if an user changes the job function. Traditional RBAC will not be able to specify a sufficient fine-grained authorized policy or constraints that must be applied to a system access control policy. It is not flexible with the complicated access control requirements inherent to the current healthcare systems. In modern healthcare domain, a patient's EHR can find scattered throughout the entire healthcare sector. From the clinical perspective, in order to deliver a quality patient care, it is really critical to access an integrated patient's healthcare information is collected at the point of care ensuring the freshness of time-sensitive data. Further it requires an efficient, secure and low-cost mechanism for sharing EHRs among multiple healthcare providers. Health care applications which requires access control and the environment in which they operates are becoming more complex. An acute needs for the better ways to manage the access control rules has arisen. There is a new

Cite this article as: Abinayakumari T, Akshitha Vijaylakshmi G, Deenak Johnson, Hasim S. "Survey of Design and Implementation of Fine-Grained Authorized Access Control for Health Care Application on Cloud". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 253-257. Print.

way for doing access control is to go for ABAC. In this most basic form. As new subjects get joins the organization, no modifications to existing rules or object attributes and are required as long as the subject is assigned the some attributes necessary for the access to the required objects,. These benefits are often referredas accommodating the external user and is the primary benefits of employing ABAC. Attribute-Based Access Control (ABAC) is used for employing multiple attributes for authorization decision, which enables some security system to be more flexible, interoperable, and multifunctional. ABAC recommendation to the access control model is for promoting the information sharing between diverse and disparate organizations.

Related Work

2.1 Traditional Access Control for EHRs

Traditionally, research on access control in electronic health records (EHRs) often places full trust on the health care providers where the EHR data are often resided in, and the access policies are implemented and enforced by the health providers. Various access control models have been proposed and applied, including role-based (RBAC) and attribute-based access control (ABAC). In RBAC, each user's access right is determined based on his/her roles and the role-specific privileges associated with them. The ABAC extends the role concept in RBAC to Attributes, such as properties of the resource, entities, and the environment. Compared with RBAC, the ABAC is more favorable in the context of health care due to its potential flexibility in policy descriptions. A line of research aims at improving the expressiveness and flexibility of the access control policies. For personal health records (PHRs) in cloud computing environments, the PHR service providers may not be in the same trust domains with the patients'. Thus patient-centric privacy is hard to guarantee when full trust is placed on the cloud servers, since the patients lose physical control to their sensitive data. Therefore, the PHR needs to be encrypted in a way that enforces each patient's personalized privacy policy, which is the focus of this paper.

2.2 Cryptographically Enforced Access Control for Outsourced Data

For access control of outsourced data, partially trusted servers are often assumed. With cryptographic techniques, the goal is trying to enforce that who has access to which parts of a patient's PHR documents in a fine-grained way. Symmetric key cryptography (SKC) based solutions. Vimercati et.al. Proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods, which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable, files in a PHR are organized by hierarchical categories in order to make key distribution more efficient. User revocation is not supported, an owner's data is encrypted block-by-block, and a binary key tree is constructed over the block keys to reduce the number of keys given to each user. The SKC-based solutions have several key limitations. First, the key management overhead is high when there are a large number of users and owners, which is the case in a PHR system. The key distribution can be very inconvenient when there are multiple owners, since it requires each owner to always be online. Second, user revocation is inefficient, since upon revocation of one user, all the remaining users will be affected and the data need to be re-encr ypted. Furthermore, users' write and read rights are not separable. Public key cryptography (PKC) based solutions. PKC based solutions were proposed due to its ability to separate write and read privileges.

2.3 Cloud Computing

Cloud computing is the recent trend of cyber world that has the very great potential to change the Information Technology by deploying cyber infrasystems. The basic idea in this cloud computing is to move computing tasks from individual systems to the cloud, which will provide us hardware and software resources over the network . Cloud providers will deploy cloud computing, storage and network infrastructure and assurances to the customers, either for an individual or a group. The main advantage of cloud computing is that the customers of Cloud computing is the recent trend in the cyber world that has a good potential to change the Information Technology on deploying cyber infrastructures. The basic idea in cloud computing that we can move computing tasks from individual systems to the cloud, which provides hardware and software resources over the network. Cloud providers deploy computing, storage and network infrastructure and provide service assurances to their customers, either an individual or a group .The main advantage of cloud computing is that the customers will be able to avoid capital expenditure on hardware, software, and service but pay only for what they use a cloud provider. With the advent of cloud computing as a new computing paradigm, flexible services can be transparently provided to users over the dynamic cloud environment where the multiple systems will be able interact with each other. By tapping into the cloud infrastructure, users can gain fast access to best -of-breed applications and drastically boost computing resources in a cost-effective way. Users can also improve their information technology's agility and reliability, and obtain device and location independence. Void capital expenditure on hardware, software, and service but pay for what they use in cloud .With that of cloud computing as a new computing paradigm, flexible services transparently gives the user over the dynamic cloud environment where multiple systems interact among them. By tapping into the cloud infrastructure, they can gain a very fast accessing to the best -of-breed application and drastically on computing resource in cost-effective way. Companies can improve their information technology's agilities and reliabilities to obtain device and location independence.

Cite this article as: Abinayakumari T, Akshitha Vijaylakshmi G, Deenak Johnson, Hasim S. "Survey of Design and Implementation of Fine-Grained Authorized Access Control for Health Care Application on Cloud". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 253-257. Print.

2.4 Access Control

Researchers have developed various access control methods to access a resource in computing systems .Between commonly deployed methods access control lists, which attaches list of approvals to each object, and access governor matrix , which symbolizes the rights of each subject with respect to every object, are not suitable for large organizations that have many subjects and objects. Discretionary access control depends on the discretion of an object's owner who is authorized to control the information resource access. Discretionary access control is tenure based and doesn't provide high degree of security in distributed systems. In compulsory access control a central authority determines what information is to be accessible by whom. Security tagging in mandatory access control is not lithe and is not expedient for task accomplishment. In role-based access control (RBAC), access rights are associated with roles, and users are assigned to fitting roles. Figure 1 shows the basic components of role-based access control, i.e., user, role, session and permission. Role Grading allows the senior role to receive from junior roles. This model has been considered in health systems. Being aninert access control model, role-based access control fails in capturing dynamic responsibilities of users to support workflows, which need dynamic activation of access rights for certain tasks. In task-based authorization control permissions are started or disabled according to the current task or process state. Task-based authorization control is an active access control model based on tasks but there is no separation between roles and tasks. In Task-Role-Based Access Control (T-RBAC), users have connection with say-sos through roles and tasks. T-RBAC is an active access control model band delivers partial authority inheritance in role hierarchy.

2.5 Electronic Medical Record

Electronic medical records (EMR) is a type of medical record that electronically access, transmit, accept, save, retrieve, connect, and process multimedia information of past, present, and future records of patients' physiological and psychological conditions. EMRs are increasingly in demand, necessitating legal and practical coordination needs to help institutions promote its employment. Various NGOs in the United States are currently outlining electronic medical record standards such as ASTM, HL7, and HIMSS. EMR standards in Europe are being overseen by TC/251 of CEN. The Internationalized TC215 has also taken into account standards setup by other organizations to setup standards of its own. On 24 November, 2005, Taiwan's Department of Health promulgated an approach to the production and management of EMRs by medical institutes specifying regulations and provisions on EMRs to order to implement and popularize EMRs among medical institutes at various levels. Amendments and improvements were also made to previous EMR regulations such as the Electronic Signature Act, the Physician Act, Medical Law, etc., establishing a legal basis for electronic medical records. The personal health record (PHR) is proposed as an innovative solution to the problems of fragmented communication and lack of interoperability among diverse EMR systems. It provides for a single source (the patient's PHR) for authentication and remote access of the health information data from all EMR systems.

2.6 Personal Health Record

In 2005, the National Committee on Vital and Health Statistics (NCVHS) [6] outlined properties of the PHR and the PHR system as follows: 1) Scope and Nature of Content: All PHR systems must have consumer health information, personal health journals, and information about benefits and/or providers. 2) Source of Information: PHR data may come from the patient, caregiver, healthcare provider, payer, etc. 3) Features and Functions: PHR systems should offer a wide variety of features, including the ability to view personal health data, exchange secure messages with providers, schedule appointments, renew prescriptions, etc. 4) Custodian of the Record: The physical record may be operated by a number of parties, including the consumer or patient, an independent third party, or an insurance company. 5) Data storage: Data may be stored in a variety of locations, including an Internet-accessible database, provider's EHR, consumer/patient's home computer, or portable devices such as smart card or thumb drive. 6) Technical approaches: Current PHR and PHR systems are generally not interoperable, and they vary in how they handle security, authentication, and other technical issues. 7) Party Controlling Access to the Data: While consumers or patients always have access to their own data, they do not always determine who else may access it. From the above listed properties, it can be inferred that the PHR data is compiled and integrated from diverse sources to provide a patient-centric health information exchange model that can be further distributed to different authorized users in part(s) or whole. As the PHR has broaden its scope, it is gradually being developed as a software, platform, or cloud application service integrating personal health services with the information and communications technology industry.

2.7 Medical Services and Cloud Computing

The fundamental service models of Cloud computing are: 1) Software as a Service (Saas): This service model provides software through the Internet with manufacturers installing applications on a cloud server. Clients do not acquire the software peruse, but rents web-based software that are updated and maintained by the vendor. 2) Platform as a Service (PaaS): Cloud providers offer a computing platform to its clients where they can deploy applications of its own, program languages of its own, all without having to maintain or control the cloud equipment. 3) Infrastructure as a Service (IaaS): Vendors integrate basic infrastructure such as IT systems and database and then rents them to clients. Cloud computing contains several features. Computation resources gathered through resource pooling allows vendors to feature Multi-tenant mode. Rapid elasticity grant unlimited possible configuration in dynamic distribution of resources according to user demand. Measured service can also monitor resource use to achieve automatic control and optimization of the cloud system. Users can also connect anywhere to cloud computing services, reducing user's dependence on terminal management equipment and related information technology expertise. There have been serious privacy concerns about outsourcing patients' PHR data to cloud servers, not only because cloud providers are generally not covered entities under HIPAA, but also due to an increasing number of cloud data breach incidents breaking out in recent years. International Journal of Information and Electronics Engineering, Vol. 3, No. 3, May 2013 330 According to recent studies , we list some of the major concerns facing PHR development in cloud environment: 1) Abuse and nefarious use of cloud computing 2) Insecure interface and application programming interface 3) Malicious insiders 4) Shared technology issues 5) Data loss or leakage 6) Account or service hijack 7) Unknown risk profile To deal with the risk of potential exposure of privacy, they should allow patients, the custodians of PHR full control of choice and options to medical record sharing. Undoubtedly, the use of encryption mechanisms can provide appropriate solutions to protecting medical information; but in addition to the traditional disposition of having service providers encrypting the data for the custodians, the PHR dispense users with access control mechanism .As under cloud environment patients' PHR are stored with outsourced providers, patients not only lose real control of these sensitive data, but faces elevated security risks. It has been difficult to achieve assurance on individual privacy when these patient-centric PHR access models are transferred to cloud servers to provide user access. Thus, our primary goal is to ensure the security of PHR, and provide for an ideal PHR with desired features of continuous real-time update and interactivity, as well as interoperability.

2.8 Cryptography and Encryption Systems

Following is a brief introduction to cryptography and encryption systems. 1) Basic cryptography: Generally speaking, to oversee system security, a password system must at least have the following four functions: confidentiality, authentication, integrity, and non-repudiation. In accordance with mathematical variances in keys, cryptography systems are divided into two major systems: private key cryptosystem, and public key cryptosystem. 2) Private keycryptosystem: By using the same secret key for encryption and decryption, private key cryptosystems facilitate efficient, quick, and low computation load. However, it has the following disadvantages: Key distribution problem: During the negotiation process of what private key is to be used between the message sender and the receiver, the ultimate decided private key has to be transmitted between the two parties, thus subjecting to security concern of possible theft during the key distribution process. Key management issues: As both sender and receiver must possess the secret key, when the number of users increases, the number of senders and receivers possessing the secret key will also increase. Difficulty in achieving non-repudiation: As both sides of the communication end possess the same encryption and decryption key, the encrypt or can disavow previously encrypted sent messages, making it impossible for the third party to distinguish who is the real encryptor. 3) Public key cryptosystem: Public key cryptosystem is also known as asymmetric cryptosystem, or two-key cryptosystem. Public key cryptography has the following advantages: Protects information privacy: Anyone can use the public key of the recipient to encrypt plaintext messages into cipher text. Simplifies allocation and management of keys: As the sender and recipient only need to store their own key pairs, and do not have to store other private keys even with the increase in the number of users, this simplifies key distribution and management problems. Possess non-repudiation: If the message is first signed□ with a private key, from the resulting signature, anyone can use the corresponding public key for verification.

2.9 ABE for Fine-grained Data Access Control

A number of works used ABE to realize fine-grained access control for outsourced data. Especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs) recently, Narayan et al proposed an attribute-based infrastructure for HER systems , where each patient's HER files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number unrevoked user. In , a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. However there are several common drawbacks of the above works. First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck but also suffers from the key escrow problem. Recently, Yu et al. (YWRL) applied key-policy ABE to secure outsourced data in the cloud, where a single data owner can encrypt her data and share with multiple authorized users, by distributing keys to them that contain attribute based access privileges. They also propose a method for the data owner to revoke a user efficiently by delegating the updates of affected cipher texts and use secret keys to the cloud server. Since the key update operations can be aggregated over time, their scheme achieves low amortized overhead however in the YWRL scheme the data owner is also a TA at the same time.. A use needs to obtain one part of her key from each A. this scheme prevents against collusion among at most N-2 TAs, in addition to use collusion resistance.

2.10 Access Control for PIPE

There exist a series of constructions for authorized access control of patients' personal health information. As we discussed in the previous section, they mainly study the issue of data confidentiality in the central cloud computing architecture, while leaving the challenging problem of realizing different security and privacy-preserving levels with respect to kinds of physicians accessing distributed cloud servers unsolved. On the other hand, anonymous identification schemes are emerging by exploiting pseudonyms and other privacy preserving techniques. Lin et. al. proposed SAGE achieving not only the content-oriented privacy but also the contextual privacy against a strong global adversary. Sun et. al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number generator and proof of knowledge. Lu et. al. proposed a privacy preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained. J. Misic et al. suggested patients have to consent to treatment and be alerted every time when associated physicians access their records. Riedlet. al. presented a new architecture of pseudonymiaztion for protecting privacy in E-health (PIPE). Slamaniget. al. integrated pseudonymization of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclosure attacks and statistical analysis in and suggested a secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a central mhealthcare cloud server . Schechter et. al. proposed an anonymous authentication of membership in dynamic groups. However, since the anonymous authentication mentioned above are established based on public key infrastructure (PKI), the need of an online certificate authority (CA) and one unique public key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed. In this paper, the security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying GBDH problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios. It is noticed that our construction essentially differs from the recently published trivial combination of attribute based encryption (ABE) and designated verifier signature (DVS)

Conclusion

This work is based on cloud patient privacy system. PHR is stored on cloud, and can be accessed throughout the web portal by multiple users. The patient who is the owner of the PHR encrypts it and stores the cipher text in the cloud server. When an access request is sent, then the policy associated with the requested object is checked at first to see whether the user has the required authentication or not. If the requester holds the correct pseudorole, rules and policies are then checked for an additional constraints in order to approve or deny the access request. The program will produce assistance along with the physicians or a medical practitioners, since it facilitates their work on comparing the manual system presently in use. With this system large number of patients will be attended in limited time and the patients record can be accessed from any part in the world along with security.

REFERENCE

1. Frode Hansen, et al, "Application of role-based access control in wireless healthcare information systems", The College of Information Sciences and Technology © 2007-2013 The Pennsylvania State University.
2. Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu. "Secure Sharing of Electronic Health Records in Clouds"; in Proceedings of Collaborate Com 2012, pp. 711-718. http://dx.doi.org/10.4108/icst.collaboratecom.2012.250497
3. Alhaqbani, Bandar S. and Fidge, Colin J, "Access control requirements for processing electronic health records," in Proceedings Business Process Management 2007 Workshops: First International Workshop on Process-Oriented Information Systems in Healthcare (Pro Health 2007) 4928, pages pp. 371-382, Brisbane - Australia.
4. Lillian Rostad, "Access control in healthcare information systems", PhD. thesis, Norwegian University of Science and Technology, Trondheim, January 2009.
5. Li-Qun Kuang, Yuan Zhang, Xie Han, "Access Control Policies for Web Services in Medical Aid System," in 2009 International Conference on Information Management, Innovation Management and Industrial Engineering. http://dx.doi.org/10.1109/ICIII.2009.199
6. R. S. Sandhu and R. K. Thomas, "Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management", in proceedings of the IFIP WG11.3Workshop on Database Security, August 1997.
7. Mary Ellen Zurko and Richard Simon, "Separation of duty in role-based environments", Proceedings of the 10th IEEE Computer Security Foundations Workshop (CSFW '97), pages 183.194, 1997.

Cite this article as: Abinayakumari T, Akshitha Vijaylakshmi G, Deenak Johnson, Hasim S. "Survey of Design and Implementation of Fine-Grained Authorized Access Control for Health Care Application on Cloud". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 253-257. Print.