ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group f Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Protected Patients Data Centre in Cloud Computing

Ms.M.Shanthi[1], Mr. P. Ranjithkumar[2]
M.E II year, Department of Computer Science and Engineering, Sri Subramanya College Of Engineering and Technology, Palani, Dindigul, Tamilnadu, India-624 615[1]
Assistant Professor, Department of Computer Science and Engineering, Sri Subramanya College Of Engineering and Technology, Palani, Dindigul, Tamilnadu, India-624 615[2]

ABSTRACT- Patients Data Centre (PDC) is a coming forth patient- centric framework of health data interchange, large scale data centric applications. In which the data is been outsourced to be stored to general IT providers, such as cloud providers and how to assure their private data while being stored in the cloud servers and to untrusted parties. To secure the patients information governs over entree to their own PDC, it is a hopeful method to encrypt the PDC and personal information before outwards. Yet, effects such as danger of privacy view, measurability in key management, compromising entree and efficient user revocation, have continued the most significant disputes accomplishing fine-grained, cryptographically imposed information entree assure. In this thesis, propose a new patient data centric role model and a suit of method for information access control to personal profiles put in half-believed servers. To reached close–grained and measurable information entree assure for PDC's, and gained Distributed Multi Authority-Attribute Based Encryption (DMA-ABE) method to generation cipher text of data through ECC (Elliptic Curve Cryptography) algorithm for encrypt each patient's data file. Different from past works in assure information outsourcing, focus on the more than one data proprietor security script, and split the users in the PDC scheme into multiple assured area that heavily shrinks the key management complexity for proprietors and consumers. A peak of data privacy is ensured at the same time by working distributed multi-authority ABE. Our scheme also enables dynamic alteration of access policies or file attribute, confirms efficient availability of data that can be needed by users/attribute revocation and break-glass approach under casualty assumption. Extended analytical and observational outcomes are presented which show the protection, measurable and efficiency of proposed system.

KEYWORDS: Patient Data Centre, Cloud computing, distributed multi-authority Attribute Based Encryption, key management, protection.

I. INTRODUCTION

Recent advances in IT have greatly facilitated remote data storage and sharing.New applications such as online social networks and online documents provide very convenient ways for people to store and share various data including Personal profile, electronic documents and etc. on remote online data. Recent advances in IT have greatly facilitated remote data storage and sharing.New applications such as online social networks and online documents provide very convenient ways for people to store and share various data including personal profile, electronic documents and etc. on remote online data servers. Cloud Computing, regarded as the future IT architecture, and even promises to provide unlimited and elastic storage resource as a service to cloud users in a very cost-effective way. Although still at its early stage, Cloud Computing has already drawn great attention, and its benefits have attracted an increasing number of users to outsource their local data centres to remote cloud servers. Data security is a critical issue for remote data storage. In particular, study a novel Distributed Multi Authority – Attribute Based Encryption (ABE), and enhance it toward providing a full-fledged cryptographic basis for a secure data sharing scheme on untrusted storage. Comparing with the preliminary version of this paper, there are several additional contribution:1) Clarify and extend the usage of DMA-ABE in the various domain, and formally show how and which types of user-defined file access policies are realized. 2) Clarify the proposed revocable DMA-ABE scheme, and provide a formal security proof it. 3) Carry out both real-world experiments and simulations to evaluate the performance of the proposed solution in this paper.

II. RELATED WORK

This thesis is mostly related to works in cryptographically enforced access control for outsourced data and DMA-based encryption. To realize fine-grained access control, either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. To improve upon the scalability of the solutions, one-to-many encryption methods such as ABE can be used. In Goyal et al.'s seminal paper on ABE [2], data are encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient [4]. A fundamental property of ABE is preventing against user collusion. In addition, the encryption or is not required to know the ACL.

A. Achieving secure, scalable and fine-grained data access control in cloud computing

Cloud computing is a fairly new concept that offers a lot of opportunities for business and companies. As any new system it faces a lot of challenges. One of the most important issues is how to make companies trust cloud providers and how to secure their private data while being stored in the cloud without direct monitoring over it. A trivial and effective solution is to encrypt data while being in the cloud. On the other hand, this solution introduces performance and key management issues. This paper targets the second issue, by introducing a combined system between key policy attribute-based encryption (KP-ABE), Proxy encryption (PRE) and lazy re-encryption.

This system offers secure, scalable, and self-key managed system. The scalability of the systems comes from KP-ABE's properties. The complexity of the system and operations depends on the number of attributes in the system not on the number of users using the system. The system is secured in two ways, first that the data is encrypted in the cloud, but also any communication between any entities requires the use of data signature in order for the receiver to be able to validate the data and its source.

B. Self-Protecting Electronic Medical Records using Attribute-Based Encryption

In additional C.U. Lehmann, M.D. Green, M.W [3] has proposed Self-Protecting Electronic Medical Records Using Attribute-Based Encryption**.** In general, EMRs over the potential for greater privacy and better access to records when they are needed. The shift towards EMRs has highlighted the need to develop meaningful techniques for securing records, both inside and outside of the hospital environment. There are emerging XML-based standards for representing EMRs, such as the Continuity of Care Record (CCR) and Continuity of Care Document (CCD). These standards call for protecting EMRs, but they do not provide enough guidance as to how such protection can be achieved. The Standard Speciation for Continuity of Care Record states: The CCR document instance must be self-protecting when possible, and the nil point has particular salience in the context of EMR protection. In this thesis, describes aborts to provide ovine, available self-protecting EMRs utilizing recent developments in attribute-based encryption (ABE).

The work is collaboration between security researchers at Johns Hopkins University and medical practitioners at the Johns Hopkins Medical Institution (JHMI).Our approach to access control using ABE facilitates granular role-based and content- based access control for EMRs, without the need for a single, vulnerable centralized server. Providers place a greater emphasis on the availability of medical records in their work than on issues such as security and privacy.

C. Securing the E-Health Cloud

In contrast to PHRs, which are managed by the patients, Electronic Health Records (EHR) are managed by health professionals only. In most countries this involves different legal requirements and a clear distinction between PHRs and EHRs. As a result, infrastructures that involve EHRs are usually more complex than our simple e-health cloud model. The advanced model, which not only involves more parties (e.g., health insurances), but also includes some technical means to enforce data security and privacy of EHRs. The general requirement in this model is still the functional and semantic interoperability of the data stored in EHRs. The EHRs are created, maintained, and managed by health care providers, and can be shared (via the central EHR server in the cloud) with other health professionals.

But storing and processing EHRs is not the only service that can be outsourced to the cloud. The health care providers can use billing services that manage their billing and accounting with the health insurances of the patients.

This is a typical scenario that can be found in practice: Many doctors outsource the billing to third party providers. Those billing services accumulate the billing of several patients for different health insurances, but also for various health care providers at the same time. As a consequence, privacy becomes an even more important aspect in this model because health insurances or billing services should not be able to access private details of EHRs. To protect the EHR data, smartcards are typically used to (1) authenticate health professionals and patients, (2) sign EHR documents to provide authenticity, (3) encrypt the EHR data before they are stored in the cloud, and (4)authorize the access to EHR data. Data and services of the e-health cloud can only be accessed with special interface connections to the telematics infrastructure boundary.

This interface connection is typically a special hardware device that establishes secure network connections via a Virtual Private Network (VPN) to the e-health data centres. Due to the increased privacy requirements, many countries define standards and specifications for national e-health infrastructures that include technical means for security and privacy.

However, existing security concepts in e-health concentrate on controlling access to data (e.g., smartcard-based access control to web-based PHRs and EHRs), protection of data transfer (encryption for confidentiality, digital signatures for integrity and authenticity), and network security. The latter focuses on the separation of different networks, e.g., administrative networks of health insurances from EHR servers and from other applications. However, little care is taken on what happens after access to data is allowed, i.e., how data is processed and stored on end-user client platforms. Viruses or Trojan horse programs can corrupt data and eavesdrop on patient's records, violating both legal and individual privacy requirements.

Example: The German electronic Health Card (eHC) system under development defines that in the compulsory health insurance system, each patient has an eHC smartcard.

III. MODELS AND ASSUMPTIONS

A .System Models

Assume that the system is composed of the following parties: the Data Owner, many Data Consumers, many Cloud Servers, and a third Party Auditor if necessary. To access data files shared by the data owner, Data consumers, or users for brevity, download data files of their interest from Cloud Servers and then decrypt. Neither the data owner nor users will be always online. They come online just on the necessity basis. For simplicity, we assume that the only access privilege for users is data file reading. Extending our proposed scheme to support data file writing is trivial by asking the data writer to sign the new data file on each update as does. From now on, it will also call data files by files for brevity. Cloud Servers are always online and operated by the Cloud Service Provider (CSP).

They are assumed to have abundant storage capacity and computation power. The Third Party Auditor is also an online party which is used for auditing every file access event. In addition, also assume that the data owner can not only store data files but also run his own code on cloud Servers to manage his data files.

B. Assurity Models

In this work, just consider Honest but Curious Cloud Servers as does. That is to say, Cloud Servers will follow our proposed protocol in general, but try to find out as much secret information as possible based on their inputs. More specifically, assume Cloud Servers are more interested in file contents and user access privilege information than other secret information. Cloud Servers might collude with a small number of malicious users for the purpose of harvesting file contents when it is highly beneficial. Communication channel between the data owner/users and Cloud Servers are assumed to be secured under existing security protocols such as SSL.

Users would try to access files either within or outside the scope of their access privileges. To achieve this goal, unauthorized users may work independently or cooperatively. In addition, each party is preloaded with a public/private key pair and the public key can be easily obtained by other parties when necessary.

C. Data Confidentiality Models

The owners upload ABE-encrypted PDR files to the server. Each owner's PDR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server.

D. Cloud Server Models

In this models, consider the server to be semi-trusted. That means the server will try to find out as much secret information in the stored PDR files as possible. Some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

IV OUR PROPOSED SCHEME

A. Main Idea

The main goal of this framework is to provide protected patient-centric PDC access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains and personal domains) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government, or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

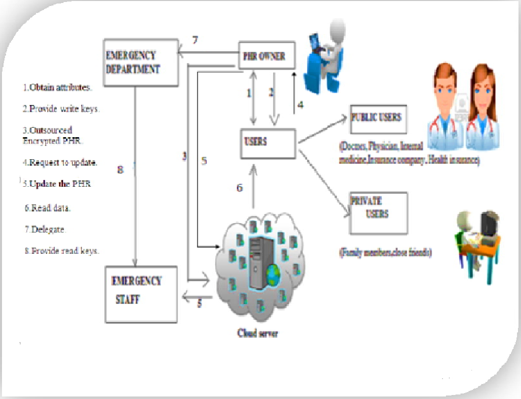

Fig. 1 The proposed framework for protected Patient Centric PDC sharing on semi trusted storage under multi owner scheme.

In both types of security domains, it utilizes ABE to realize cryptographically enforced, patient-centric PDC access. Especially, Distributed Multi Authority - ABE is used, in which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. Each data owner (e.g., patient) is a trusted authority of own PSD, to manage the secret keys and access rights of users. Since the users are personally known by the PDC owner, to realize patient centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties.

For PSD, data attributes are defined which refer to the intrinsic properties of the PDC data, such as the category of a PDC file. For the purpose of PSD access, each PDC file is labelled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. The multi domain approach best models different user types and access requirements in a PDC system. The data contributors will be granted write access to someone's PDC, if they present proper write keys. The use of DMA-ABE makes the encrypted PHRs self-protective, i.e., they can be accessed by only authorized users even when storing on a semi trusted server, and when the owner is not online.

In addition, efficient and on-demand user revocation is made possible via our DMA-ABE enhancements. Frequently used notation are given in the below table.1

NOTATION	DESCRIPTION
PK,MK	system public key and master key
SK,ASK	Symmetric and asymmetric key
T,L(T)	A user access tree and its leaf node set
Ti	public key component for attribute i
P	Access Policy for a PDC document
Ti	master key component for attribute i
SK	user secret key
Ski	user secret key component for attribute i
I	attribute set assigned to a data file
DEK	symmetric data encryption key of a data
AttD	the dummy attribute
UL	the system user list
AHLi	attribute history list for attribute i.

Table.1frequently used Notation in our scheme description

V. DETAILS OF THE PROPOSED FRAMEWORK

In our framework, there are multiple owners, multiple AAs, and multiple users in addition, DMA-ABE is used. The framework is illustrated in Fig. 1.in this users having read and write access as data readers and contributors, respectively.

*A. **System Setup*** in this operation, the data owner chooses a security parameter κ and calls the algorithm level interface *Setup*(κ), which outputs the system public parameter *PK* and the system master key *MK*. The data owner then signs each component of *PK* and sends *PK* along with these signatures to Cloud Servers.

*B.**PDC Encryption and Access***. The owners upload ABE encrypted PDC files to the server. Each owner's PDC file is encrypted both under a certain fine-grained and role based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root. For example, in Fig. 2, an "allergy" file's attributes are PDC; medical history; allergy.

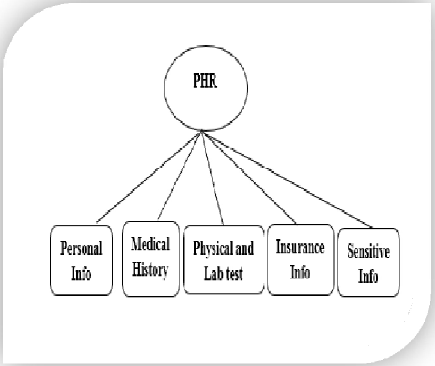

Fig. 2 The attribute Hierarchy of files

Personal Information: Name, Date Of Birth,Age,Sex,Height,SSN

Medical History: Conditions,Allergies,Medications/Perscriptions

Examination: Physical Test include Pulse, Heart rate, etc

Lab Test include X-ray images, Blood test

Sensitive Info: HIV/Profile and sensible information of patient.

C. Break-Glass

Introduced break-glass refers to quick means for extending a person's access rights in exceptional cases. Of course, the usage of exceptional access rights needs to be documented for later audits and reviews. Usually, break-glass solutions are based on authenticating the user and, therefore, are not directly applicable to ABE-based access control system. Based on our break-glass approach assume an access control policy p based on an access control model.

D. Revocation: Revocation is a vital open problem in almost every cryptosystem dealing with malicious behaviours. The revocation problem in a traditional ABE scheme, limited choices are available. One is the revocation of a single attribute shown in Fig 3, which is not in connection with users behaviour's but more likely to be periodical update of universal attribute set of the whole system. Another possible solution is to revoke one attribute set corresponding to one specific set of users.

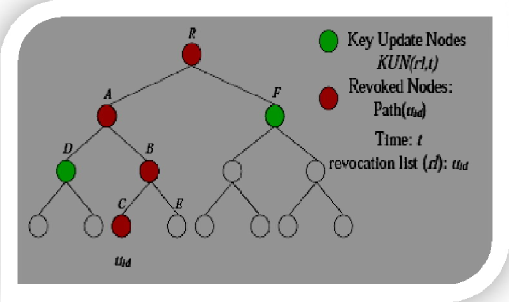

Fig 3.Revocation Tree T

There are several possible cases:1)revocation of one or more role attributes of a public domain user; 2)Revocation of a personal domain user's access privileges;4) revocation of a personal domain user. These can be initiated through the PHR owner's client application in a similar way.

E. ***Policy updates***. A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the cipher text. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.

VI. PERFORMANCE MEASURES

The results are given in Table 2. The cipher text size only accounts for the encryption of FEK. In our scheme, for simplicity assume there is only one PUD, thus the cipher text includes m additional wildcard attributes and up to N - 1 dummy attributes. In this scheme requires a secret key size that is linear, the number of attributes of each user, while in the E-Health and HIPA schemes this is linear with since a user needs to obtain at least one key from each owner whose PHR file the user wants to access.

SCHEME	SECURITY	USERDOMAIN	ACCESS POLICY	REVOCATION MEANS
E-Health [2]	Not against user-server collusion	All	ACL level	ACL level, immediate
HIPA [3]	No collusion risk	PUD	ACL level	ACL level, immediate
EMD [1]	Single TA	PUD	Attribute and ID-based policy	Attribute-level, immediate
Our scheme	Against N-2 AA collusion	All (PSD &PUD)	Conjunctive form with wildcard	Attribute-level, immediate

Table 2 Comparision of Security

VI. CONCLUSION

In this thesis, have utilized DMA-ABE to encrypt the PDC data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. To enhance DMA-ABE (Distributed Multi Authority-Attribute Based Encryption) theme to handle efficient and on-demand user revocation, and prove its security. Because of distributed MA-ABE records are share in secure way, also manage the key escrow problem, on-demand efficient user/attribute revocation, multiple authority can be used for PDC owners and users, fully protect the data from the unauthorized users. Through implementation and simulation, show that our resolution is each ascendible and economical.

REFERENCES

[1]Ming Li, Member,ShuchengYu,WenjingLou"Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption ", 2013.

[2] J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, (2010) "Self-Protecting Electronic Medical Records UsingAttribute-Based Encryption," Cryptology ePrint Archive, Report 2010/565, http://eprint.iacr.org/.

[3] Lohr H, Sadeghi AR, Winandy M. (2010) "Securing the e-health cloud. Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010; 220–229.

[4] Yu, C. Wang, K. Ren, and W. Lou, (2010)"Achieving Secure, Scalable, and Fine-GrainedData Access Control in Cloud Computing," Proc. IEEE INFOCOM.