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 4, September 2014

Proficient Sharing of Personal Health Reports in Cloud

Brindha Kundavaran[1], G. Tagore Sai Prasad[2]

2nd Year,M. Tech[1], Dept. of C. S. E, Sree Venkateswara Engineering College for Women, Tirupati, India

Assistant Professor[2], Dept. of C. S. E, Sree Venkateswara Engineering College for Women, Tirupat, India

ABSTRACT: A personal health report, or PHR, is a health report where health data and information cognate to the care of a patient is maintained by the patient. PHRs have the potential to avail analyze an individual's health profile and identify health threats and amendment opportunities predicated on an analysis of drug interaction, current best medical practices, gaps in current medical care plans, and identification of medical errors. Hence it is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. To have patients control it is very consequential to encrypt them afore outsourcing. The critical issues such as privacy, key management, flexible access and efficient utilizer revocation must be addressed. We utilize Attribute Predicated Encryption (ABE) to encrypt the PHR data, so that patients can sanction access not only by personal users, but withal sundry users from public domains with different professional roles, qualifications, and affiliations-thus enabling fine-grained and scalable data access control. The patient-centric framework provides a high degree of patient privacy by utilizing Attribute –Based Encryption techniques. The users in the PHR system are divided into multiple security domains that greatly reduce the key management intricacy for owners and users. This scheme additionally enables dynamic modification of access policies or files attributes, efficient on demand utilizer revocation and break glass access under emergency scenarios.

KEYWORDS: Personal health reports, cloud computing, privacy, multi authority, attribute-based encryption

I. Introduction

PHRs have the ability to benefit the public health sector by providing health monitoring, outbreak monitoring, empowerment, linking to accommodations, and research. PHRs can give consumers the potential to play an immensely colossal role in for fending and promoting the public's health. The desiderata for outsourcing our PHR are to Prepare your family for emergency, access all of your family's paramount health information, track your status and stay motivated, monitor chronic condition and apportion with your medico. A PHR accommodation must provide the accommodations to engender, manage, and control her personal health data in one place through the web, so that the storage, retrieval, and sharing of the medical information more efficient. Each patient must be assured to have the full control of her medical reports and can apportion her health data with a wide range of users, including healthcare providers, family members or friends. While it is exhilarating to have convenient PHR accommodations for everyone, there are many security and privacy risks which could obviate its wide adoption. The main concern is about whether the patients could genuinely control the sharing of their sensitive personal health information (PHI), mainly when they are stored on a third-party server which people may not planarity trust. To ascertain patient-centric privacy control over their own PHRs, it is paramount to have efficient data access control mechanisms that work with semi trusted servers.

An efficient approach would be to encrypt the data afore outsourcing. The PHR owner herself should decide how to encrypt her files and to sanction which set of users to obtain access to each file. The patient always has the right to not only grant, but additionally revoke access privileges when they feel it is indispensable. The sanctioned users may either need to access the PHR for personal use or professional purposes. Examples of the personal use are family member and friends, while the professional use can be medical medicos, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively to have scalable key management.

We adopt attribute predicated encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed predicated on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to ken a consummate list of users.

The main contributions are as follows.

1. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains (PSDs).
2. In the public domain, we utilize multi-authority ABE (MA-ABE) to amend key management. Each attribute ascendancy (AA) in it governs a disjoint subset of utilizer role attributes, while none of them alone is able to control the security of the whole system. In personal domains we utilize key policy ABE (KP-ABE)

II. RELATED WORK

Our scheme is designed to mainly have fine-grained access control and to overcome the traditional public key encryption schemes [8],[10] which incur high key management overhead or require multiple facsimiles of a file utilizing different users keys. In ABE scheme [11], they proposed to encrypt data under a set of attributes so that multiple users can decrypt. This makes encryption and key management more efficient.

Attribute Based Encryption:

Many works used ABE to have fine-grained data access control for outsourced data. There has been incrementing interest to apply ABE to secure EHR‟s. They are:

1. By utilizing CP-ABE Narayan et.al [1] proposed an attribute infrastructure for HER systems that sanctions direct revocation. But in this the cipher-text length grows linearly with the number of unrevoked users.

2. Lbraimi et.al [2] applied CP-ABE to manage the sharing of PHR and introduced the concept of gregarious/professional domains.However, there are many prevalent drawbacks of the above works. They customarily postulate the utilization of a single trusted ascendancy (TA) in the system. This not only engender a load bottleneck, but additionally suffers key escrow quandary as the TA can access all the encrypted files.It is withal not practical to delegate all the attribute management tasks to one TA, including certifying all users attributes or roles and engendering secret keys.

3. Most of the subsisting works do not differentiate between the persona and public domains, which have different attribute definitions, key management requisites and scalability issues.

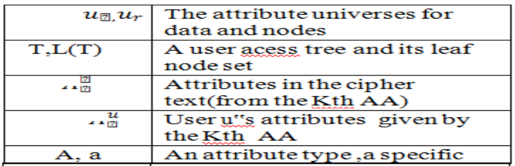
4. [3][4] Yu et.al applied key-policy ABE to secure outsourced data in the cloud, where single data owner can encrypt her data and apportion with multiple sanctioned users, by distributing keys to them that contain attribute predicated access policies.

The framework considers application-level requisites of both public and personal utilization of a patient‟s PHRs, and distributes users‟ trust to multiple ascendant entities. We withal propose a suite of access control mechanisms by uniquely amalgamating the technical strengths of both CC MA-ABE [21] and the YWRL ABE scheme [9]. Using our scheme, patients can optate and enforce their own access policy for each PHR file, and can revoke a utilizer without involving high overhead.

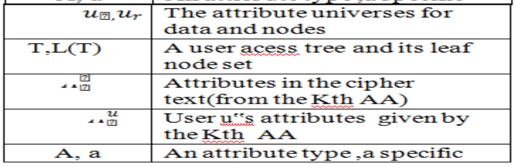
III. FRAMEWORK

Here we describe the patient-centric secure data sharing framework. The main notations are summarized below:

Frequently Used Notations:



$u_{⍰}, u_r$	The attribute universes for data and nodes
T,L(T)	A user acess tree and its leaf node set
..$^{⍰}_{⍰}$	Attributes in the cipher text(from the Kth AA)
..$^{u}_{⍰}$	User u‟s attributes given by the Kth AA
A, a	An attribute type ,a specific



$u_{⍰}, u_r$	The attribute universes for data and nodes
T,L(T)	A user acess tree and its leaf node set
..$^{⍰}_{⍰}$	Attributes in the cipher text(from the Kth AA)
..$^{u}_{⍰}$	User u‟s attributes given by the Kth AA
A, a	An attribute type ,a specific

Problem definition:
We consider a system with multiple PHR owners and PHR users. The owners refer to patients, who have full control over their own PHR data, i.e., they can engender, manage, and expunge it. There is a central server that stores all the owners" PHRs. The users may emanate from sundry aspects; for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server and a utilizer can simultaneously have access to multiple owners" data.

Security Model:
In our framework we consider that the server will endeavor to ascertain as much secret information in the stored PHR files as possible, but they will veraciously follow the protocol in general. Some users will additionally endeavor to access the files beyond their privileges, so we surmise each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-replication protocols

Requirements:
The core requisite is that each patient can control who are sanctioned to access to her own PHR documents. The security and performance requisites are as follows:

- Data confidentiality: Only the sanctioned users who have sufficient attributes gratifying the access policies can decrypt the PHR document.
- On-demand revocation: The utilizer whose attribute is no longer valid, should not be able to access future PHR files utilizing that attribute.
- Write access control: Only the sanctioned contributors can gain indite-access to owners" PHRs.
- The data access policies should be flexible, i.e., having dynamic changes to the predefined policies
- Scalability, efficiency, and usability: The system should be highly scalable, in terms of involution in key management, communication, computation and storage.

IV. OVERVIEW

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management concurrently. There are multiple owners, multiple AAs, and multiple users. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains (PSDs). The owners upload ABE-encrypted PHR files to the server the PHR owner herself should decide how to encrypt her files and to sanction which set of users to obtain access to each file

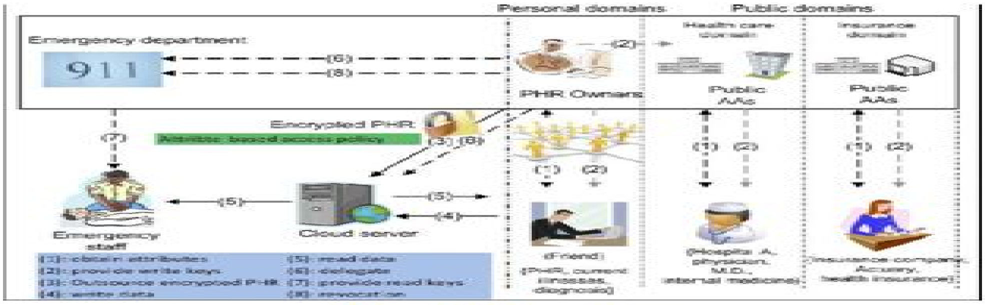


Fig 1: Architechture

Details of the Framework:

In Public Utilizer Domain:

- Multiauthority ABE is utilized, in which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. Role attributes are defined for PUDs, representing the professional role or obligations of a PUD utilizer.
- Users in PUDs obtain their attribute-predicated secret keys from the AAs, without directly interacting with the owners.
- To control access from PUD users, owners are in liberty to designate role-predicated fine-grained access policies for her PHR files, while do not require to ken the list of sanctioned users when doing encryption.

In Personal utilizer domain:

- Each data owner (e.g., patient) is a trusted ascendancy of her own PSD, who utilizes a KP-ABE system to manage the secret keys and access rights of users in her PSD. The owner grants utilizer access privileges on a case-by-case substructure.

Setup and Key Distribution:

There are two ways for distributing secret keys:

- First, when first utilizing the PHR accommodation, a PHR owner can designate the access privilege of a data reader in her PSD.
- Second, a reader in PSD could obtain the secret key by sending a request to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Predicated on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to engender the utilizer secret key that embeds her access structure.

Break-glass Policy:

- Each owner‟s PHR‟s access right is additionally delegated to an emergency department ED to avert from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain ephemeral read keys.

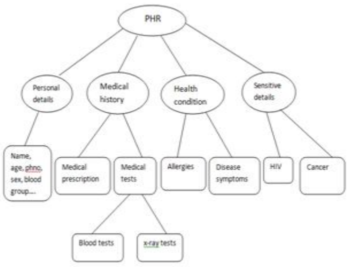


Fig 2: The attribute hierarchy of files

V. MAIN DESIGN ISSUES

Here we address several design issues in secure and scalable sharing of Personal Health Reports in cloud computing, under proposed framework.

Using MA-ABE in the Public Domain:

In order to achieve more vigorous privacy guarantee for data owners, the Chase-Chow MA-ABE scheme is utilized where each ascendancy governs the disjoint set of attributes distributely. There is one technical challenge is that CC MA-ABE is essentially a KP-ABE scheme, where the access policies are enforced in users secret keys, and those key-policies do not directly translate to document access policies do not directly translate to document access policies from the owner‟s perspective.CC MA-ABE can fortify owner-designated document access policies with some degree of flexibility.

For example in the first AA (AMA) in "license status" is associated with "profession," and vocation is a primary type. That denotes physician‟s possible set of license status do not intersect with that of a nurse‟s or a pharmacist‟s. An "MD".license is always associated with "physician", while elderly license is always associated with nurse

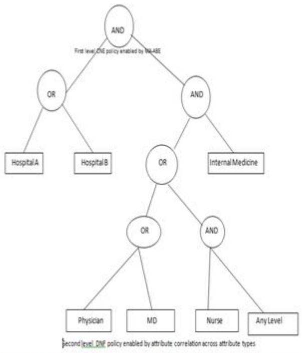

AND
First level CNF policy enabled by MA-ABE
OR
AND
Hospital A
Hospital B
OR
Internal Medicine
OR
AND
Physician
MD
Nurse
Any Level
Second level DNF policy enabled by attribute correlation across attribute types

Fig 3: An example policy realizable under our framework using MA-ABE

Enhancing MA-ABE for Utilizer Revocation:

The pristine CC MA-ABE scheme does not enable efficient and on-demand utilizer revocation .In particular, an ascendancy can revoke a utilizer or user"s attributes immediately by re-encrypting the cipher texts and updating user"s secret keys, while a major part of these operations can be delegated to the server which enhances efficiency.

To revoke a utilizer in MA-ABE, one needs to ascertain a minimal subset of attributes such that without it the user„s secret key"s access structure will never be satiated.

The enhanced CCMA-ABE scheme with immediate revocation capabilities is formally described by following algorithms.

Enforce Indite Access Control:

If there is no restrictions on indite access, anyone may indite to someone"s PHR utilizing only public keys, which is undesirable. By granting indite access a data contributor should obtain felicitous sanction from the organization. For example a medico should be sanctioned to indite only during her office hours. On the other hand the medico must not be able to indite to patients that are not treated by her. Therefore, we cumulate signatures with the hash chain techniques to achieve our goals. Only if both holds and the contributor is granted indite access and the server accepts the contents uploaded subsequently.

Handle Dynamic Policy Changes:

Our scheme should fortify the dynamic integrate/modify/expunge part of the document access policies or data attributes by the owner. For example if a patient does not optate medicos to view her PHR after she culminates a visit to the hospital, she can simply expunge the cipher text components to attribute medico in her PHR files.

VI. SECURITY ANALYSIS

Here we achieve data confidentiality by proving the enhanced MA-ABE scheme to be secure under the attribute selective set model.

Data Confidentiality:

The primary security goal is to keep the owners encrypted data confidential with regards to non-sanctioned users. For CC MA-ABE, since we utilize it in a way akin to CP-ABE the security interpretation should be, a utilizer who does not have a set of role attributes that satiate the PHR files access policy cannot decrypt.

Collusion Resistance:

Our scheme is resistant to users collusion, which is implicatively insinuated by the security of the adopted ABE-schemes. In this way as long as less than N-1 AAs are corrupted, there is still one AA* with a dummy attribute not corrupted. It withal sanctions trade-offs between collusion resistance and efficiency .It is facile to optically discern that the scheme is secure as long as atleast two of the AAs are not corrupted.

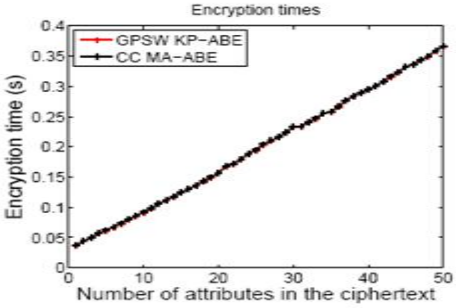
Forward Secrecy:

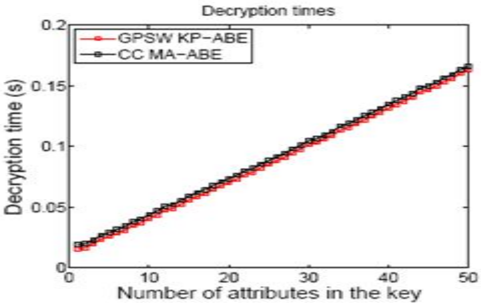
Forward secrecy denotes that, any utilizer who loses an attribute should be obviated from accessing the plaintext of subsequent data exchanged afterwards, unless her remaining valid attributes gratify the access policy.

Security of Indite Access Control:

The indite access is enforced by the scheme in security. It can be visually perceived that our scheme achieves high privacy guarantee and on-demand revocation. In integration, our proposed concretely address the access requisites in cloud predicated health report management system by logically dividing the system into PUD and PSD"s which consider both personal and professional users.

VII. RESULTS





VIII. CONCLUSION

Here, we have proposed a framework for secure sharing of personal health reports in cloud computing. The framework is very efficient and solves the unique challenges brought by multiple PHR owners and users, it solves the intricacy of key management while enhance the privacy guarantees compared with antecedent works. We use ABE to encrypt the PHR data, so that patients can sanction access not only by personal users, but additionally wide range of users from public domains. Furthermore, we enhance a subsisting MA-ABE scheme to handle efficient and on-demand utilizer revocation, and prove its security.

REFERENCES

[1] S. Narayan, M. Gagne´, and R. Safavi-Naini, “Privacy PreservingEHR System Using Attribute-Based Infrastructure,” Proc. ACM Cloud Computing Security Workshop (CCSW ‟10), pp. 47-52,
2010.

[2]L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Reports by Applying Attribute-Based Encryption,” technical report, Univ. of Twente, 2009.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM ‟10, 2010.

[4] C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers,” J. Computer Security, vol. 19, pp. 367-397, 2010.

[5] S. Narayan, M. Gagne´, and R. Safavi-Naini, “Privacy Preserving EHR System Using Attribute-Based Infrastructure,” Proc. ACM Cloud Computing Security Workshop (CCSW ‟10), pp. 47-52, 2010.

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

[7] M. Chase and S.S. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS ‟09), pp. 121-130, 2009.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,”Proc. IEEE INFOCOM ‟10, 2010.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,” Proc. IEEE 10th Int‟l Conf. Trust, Security and Privacy in Computing and Comm. (TrustCom), 2011.

[10]J. Hur and D.K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July

BIOGRAPHY

Brindha Kundavaran is a M.Tech Student in the Computer Science And Engineering Department, College of Sree Venkateshwara Engineering College For Women, JNTU-Ananthapur. She Received Bachelors of Information Technology(IT) degree in 2011 from SVNE,Rangampet,Tirupati,India. Her Research interests are Computer Networks, Algorithms, Programming etc.

G. Tagore Sai Prasad is an Assistant Professor in the Computer Science And Engineering Department, College of Sree Venkateshwara Engineering College For Women, JNTU-Ananthapur. He Received Masters of computer Science degree in 2011 from JNTU Kakinada,India. His research interests are Computer Networks, Data Mining UML etc.