Protected Distribution of PHR Using Attribute Based Encryption in Cloud Computing

Mr.Markad Shrikant K, Prof.Rahul B. Mapari

***Abstract*— This paper describes the planning and utilization of private Health Records and provides defend to them whereas they're hold on at third party like cloud. To assure the patients' management over access to their own PHRs, it's a promising methodology to cypher the PHRs before outsourcing. Personal Health Record is net based mostly application that permits folks to access and co-ordinate their health info. The patient have management over access to their own PHR. to protect of private health records we tend to use the attribute based mostly secret writing to cypher the info before outsourcing it. Here we tend to target multiple styles of PHR owner state of affairs and division of private health records users into multiple security domains that cut back key management complexness for homeowners and users. A high degree of patient's privacy is secured. Our theme provides personal health record owner full management of his/her knowledge. in depth security and performance analysis shows that the planned theme is extremely economical. Personal health record (PHR) is associate degree rising patient-centric model of health info exchange, that is usually outsourced to be hold on at a 3rd party, like cloud suppliers. However, there are wide privacy issues as personal health info can be exposed to those third party servers and to unauthorized parties.**

***Index Terms*— cloud computing, attribute-based encryption,data security,shielded sharing, Personal Health Record.**

I. INTRODUCTION

PHR system shows that how it'll be useful and a patient centrical model as overall control of patient‟s data is with patient.A PHR s allows a patient to make, manage, and control his/her personal health data in one place through the net, that has created the storage, retrieval, and sharing of the medical info additional efficient. Especially, every patient is promised the total control of her medical records and might share her health data with a wide range of users, as well as healthcare providers, family or friends. as a result of the high value of develop and sustain specialized big data centers, many PHR services square measure expand to or provided by third-party service providers, for example, Microsoft HealthVault.While it is exciting to own convenient PHR services for everyone, there square measure many security and privacy risks that could impede its wide adoption. the most concern is concerning

whether or not the patients could truly control the sharing of their sensitive personal health info (PHI), especially once they square measure hold on on a third-party server which individuals may not totally trust. On the one hand, although there exist healthcare laws such as HIPAA that is recently amended to include business associates [4], cloud providers square measure sometimes not coated entities [5]. On the other hand, as a result of the high price of the sensitive alphabetic character, the third-party storage servers square measure usually the targets of assorted malicious behaviors which may cause exposure of the alphabetic character.

Manuscript received September 17, 2014.

Mr.Markad Shrikant K, PG Sclolar, MIT Aurangabad, Maharashtra, India 431028

Prof.Rahul B. Mapari, Computer Science and Engg Department, MIT Aurangabad, Maharashtra India 431028

II. LITERATURE SURVEY

Personal Health Record could be a internet based application that permits of us to access and co-ordinate their long health information and build if acceptable elements of its accessible to those that would love. Personal Health Record‟s security and protection of its data area unit of nice concern and a subject matter of research over the years. There unit of measurement many different kinds of subject mechanisms like AES, MD5 projected to confirm data security.This paper is usually related to works in cryptographically implemented access management for outsourced data and attribute based secret writing. to understand fine-grained access management, the quality public key secret writing (PKE)-based schemes [8], [10] either incur high key management overhead, or would like encrypting multiple copies of a file exploitation fully totally different users' keys. to boost upon the quality of the on high of solutions, one-to-many secret writing ways like ABE are used. In Goyal et al.'s seminal paper on ABE [11], data unit of measurement encrypted below a bunch of attributes therefore multiple users World Health Organization possess correct keys can decipher. This most likely makes secret writing and key management plenty of economical [12]. A elementary property of ABE is preventing against user collusion. to boot, the encryptor is not required to know the ACL. the foremost perform of cloud server is to create interface between application and user. The authentication of the username and parole is distributed. If user is authentic then he get access to his record.

ABE for Fine-Grained Data Access Control

There is an increasing interest in applying ABE to secure electronic aid records (EHRs). Recently, Narayan et al. planned AN attribute-based infrastructure for EHR systems, wherever every patient's EHR files square measure encrypted employing a broadcast variant of CP-ABE [16] that enables direct revocation. However, the ciphertext length grows linearly with the quantity of unrevoked users. However, there square measure many common drawbacks of the on top of

works. First, they sometimes assume the employment of one trustworthy authority (TA) within the system. This not solely might produce a load bottleneck, however conjointly suffers from the key written agreement downside since the tantalum will access all the encrypted files, gap the door for potential privacy exposure. additionally, it's not sensible to delegate all attribute management tasks to at least one tantalum, as well as certifying all users' attributes or roles and generating secret keys. In fact, totally {different|completely different} organizations sometimes kind their own (sub)domains and become appropriate authorities to outline and certify different sets of attributes happiness to their (sub)domains (i.e., divide and rule). for instance, an expert association would be chargeable for certifying medical specialties, whereas a regional health supplier would certify the duty ranks of its staffs. Second, there still lacks AN economical and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, that square measure essential components of secure PHR sharing. Finally, most of the prevailing works don't differentiate between the non-public and public domains (PUDs), that have completely different attribute definitions, key management necessities, and measurability problems. Our plan of conceptually dividing the system into 2 forms of domains is comparable therewith in [18]; but, a key distinction is in [18] one tantalum remains assumed to control the complete skilled domain.

$\mathcal{U}_D, \mathcal{U}_R$	The attribute universes for data and roles
$\mathcal{T}, L(\mathcal{T})$	A user access tree and its leaf node set
$\mathbb{A}_k^c$	Attributes in the ciphertext (from the kth AA)
$\mathbb{A}_k^u$	User u's attributes given by the kth AA
A, a	An attribute type, a specific attribute value of that type
$\mathcal{P}$	Access policy for a PHR document
P	A key-policy assigned to a user
MK, PK	Master key and public key in ABE
SK	A user's secret key in ABE
$rk_j^{(k)}$	Proxy re-key for attribute j and version k

TABLE 1
Frequently used notaions

A. *Varying ABE*

Recently, [23] and [24] projected two CP-ABE schemes with immediate attribute revocation capability, instead of periodical revocation. However, they weren't designed for MA-ABE.In addition, Ruj et al. [25] projected AN alternate resolution for identical draw back in our paper exploitation Lewko and Waters's (LW) decentralized ABE theme [26]. the foremost advantage of their resolution is, each user can get secret keys from any set of the TAs at intervals the system, in distinction to the CC MA-ABE. The substance ABE theme enjoys higher policy expressive-ness, and it's extended by [25] to support user revocation. On the flinch, the communication overhead of key revocation remains high, as a result of it desires a data owner to transmit Associate in Nursing updated ciphertext part to every nonrevoked user. They in addition do not differentiate personal and public domains.In this paper, we've got an inclination to bridge the on prime of gaps by proposing a unified security framework for patient-centric sharing of PHRs throughout a multidomain, multiauthority PHR system with many users. The framework captures application-level wants of every public and personal use of a patient's PHRs, and distributes users' trust to multiple authorities that higher reflects reality. we've got an inclination to in addition propose a group of access management mechanisms by unambiguously combining the technical strengths of every CC MA-ABE [21] and conjointly the YWRL ABE theme [9]. exploitation our theme, patients can choose and enforce their own access policy for each PHR file, and may revoke a user whereas not involving high overhead. we've got an inclination to in addition implement a locality of our resolution throughout a example PHR system

III. STRUCTURE FOR PATIENT-CENTRIC,DUCTILE AND SHIELDED PHR SHARING

In this section, we focus on patient-centric secure data sharing framework for cloud-based PHR systems. The main notations are summarized in Table 1.

A. *Problem Definition*

We think about a PHR system wherever there are multiple PHR house owners and PHR users. The house owners see patients World Health Organization have full management over their own PHR knowledge, i.e., they'll produce, manage, and delete it. there's a central server happiness to the PHR service supplier that stores all the owners' PHRs. The users could come back from varied aspects; as an example, a friend, a caregiver or a man of science. Users access the PHR documents through the server so as to scan or write to someone's PHR, and a user will at the same time have access to multiple owners' knowledge.A typical PHR system uses normal knowledge formats. as an example, continuity-of-care (CCR) (based on XML knowledge structure), that is wide utilized in representative PHR systems together with Indivo [27], associate degree ASCII text file PHR system adopted by Boston Children's Hospital. owing to the character of XML, the PHR files ar logically organized by their classes in a very hierarchical means [8], [20].

a) safety Model

In this paper, we tend to take into account the server to be semitrusted, i.e., honest however curious as those in [28] and [15]. which means the server can try and establish the maximum amount secret info within the hold on PHR files as attainable, however they'll honestly follow the protocol normally. On the opposite hand, some users will try and access the files on the far side their privileges. for instance, a pharmacy might want to get the prescriptions of patients for promoting and boosting its profits. To do so, they'll conspire with different users, or maybe with the server. additionally, we tend to assume every party in our system is preloaded with a public/private key try, and entity authentication will be done by ancient challenge-response protocols.

b) Specification Requirements

To achieve "patient-centric" PHR sharing, a core demand is that every patient will management World Health

Organization area unit licensed to access to her own PHR documents. Especially, user-controlled read/write access and revocation area unit the 2 core security objectives for any electronic health record system, acknowledged by Mandl et al. [7] in as early as 2001. the safety and performance necessities area unit summarized as follows:

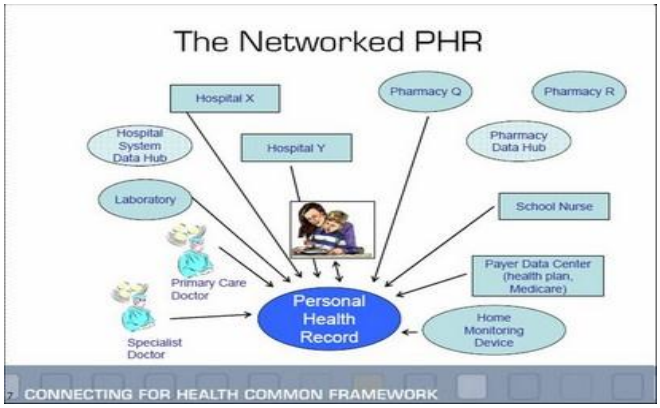
security: Unauthorized users (including the server) World Health Organization don't possess enough attributes satisfying the access policy or don't have correct key access privileges ought to be prevented from decrypting a PHR document, even below user collusion. Fine-grained access management ought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

On time cancellation: Whenever a user's attribute isn't any longer valid, the user mustn't be able to access future PHR files victimisation that attribute. this can be typically referred to as attribute revocation, and also the corresponding security property is forward secrecy [23]. there's additionally user revocation, wherever all of a user's access privileges area unit revoked.

Write access management: we have a tendency to shall stop the unauthor-ized contributors to realize write-access to owners' PHRs, whereas the legitimate contributors ought to access the server with responsibility.The data access policies ought to be versatile, i.e., dynamic changes to the predefined policies shall be allowed, particularly the PHRs ought to be accessible below emergency situations.

c) Analysis Framework

The main goal of our framework is to produce secure patient-centric PHR access and economical key management at constant time. The key plan is to divide the system into multiple security domains (namely, public domains and private domains) in step with the various users' knowledge access necessities. The PUDs comprises users WHO build access supported their skilled roles, like doctors, nurses, and medical researchers. In apply, a course are often mapped to associate degree freelance sector within the society, like the health care, government, or insurance sector. for every PSD, its users area unit in person related to an information owner (such as relations or shut friends), and that they build accesses to PHRs supported access rights assigned by the owner.In each forms of security domains, we tend to utilize ABE to comprehend cryptographically implemented, patient-centric PHR access. Especially, during a course multiauthority ABE is employed, within which there area unit multiple "attribute authorities" (AAs), every governing a disjoint set of attributes. Role attributes area unit outlined for PUDs, representing the skilled role or obligations of a course user. Users in PUDs get their attribute-based secret keys from the AAs, while not directly interacting with the house owners. to manage access from course users, house owners area unit liberated to specify role-based fine-grained access policies for her PHR files, whereas don't ought to apprehend the list of licensed users once doing encoding. Since the PUDs contain the bulk of users, it greatly reduces the key management overhead for each the house owners and users.Each knowledge owner (e.g., patient) may be a trustworthy authority of her own PSD, WHO uses a KP-ABE system to manage the key keys and access rights of users in her PSD. Since the users area unit in person far-famed by the PHR owner, to comprehend patient-centric access, the owner is at the simplest position to grant user access privileges on a individual basis.



d) Stuctured Framework

In this paper, there are multiple SDs, multiple house owners, multiple AAs, and multiple users. additionally, 2 ABE systems are involved: for every PSD the YWRL's voidable KP-ABE theme [9] is adopted; for every pudding, our projected voidable MA-ABE theme (described in Section 4) is employed. The framework is illustrated in Fig. 1. we tend to term the users having scan and write access as information readers and contributors, severally.System setup and key distribution. The system initial defines a typical universe of information attributes shared by each PSD, like "basic profile," "medical history," "allergies," and "prescriptions." associate emergency attribute is additionally outlined for break-glass access. every PHR owner's consumer application generates its corresponding public/master keys. the general public keys may be revealed via user's profile in an internet health care social-network (HSN) (which may well be a part of the PHR service; e.g., the Indivo system [27]). There are 2 ways in which for distributing secret keys. First, once initial mistreatment the PHR service, a PHR owner will specify the access privilege of an information reader in her PSD, and let her application generate and distribute corresponding key to the latter, in an exceedingly method resembling invites in GoogleDoc. Second, a reader in PSD might get the key key by causing asking (indicating that styles of files she needs to access) to the PHR owner via HSN, and also the owner can grant her a set of requested information varieties. supported that, the policy engine of the applying mechanically derives associate access structure, and runs keygen of KP-ABE to come up with the user secret key that embeds her access structure. additionally, the information attributes may be organized in an exceedingly gradable manner for economical policy generation, see Fig. 2. once the user is granted all the file varieties below a class, her access privilege are pictured by that class instead. For the PUDs, the system defines role attributes, and a reader in an exceedingly pudding obtains secret key from AAs, that binds the user to her claimed attributes/roles. for instance, a MD in it might receive "hospital A, physician, M.D., internal medicine" as her attributes from the AAs. In follow, there exist multiple AAs

every governing a special set of role attributes. as an example, hospital staffs shall have a special AA from pharmacy specialists. this is often mirrored by (1) in Fig. 1. MA-ABE is employed to code the information,and the concrete mechanism are bestowed in Section four. additionally, the AAs distribute write keys that let contributors in their pudding to write down to some patients' PHR (2).PHR secret writing and access. The house owners transfer ABE-encrypted PHR files to the server (3). every owner's PHR file is encrypted each below a precise fine-grained and role-based access policy for users from the pudding to access, and below a particular set of information attributes that permits access from users within the PSD. solely approved users will rewrite the PHR files, excluding the server. For up potency, the information attributes can embrace all the intermediate file varieties from a leaf node to the basis. for instance, in Fig. 2, associate "allergy" file's attributes are fPHR; medical history; allergyg. the information readers transfer PHR files from the server, and that they will rewrite the files on condition that they need appropriate attribute-based keys (5). the information contributors are granted write access to someone's PHR, if they gift correct write keys (4).User revocation. Here, we tend to take into account revocation of an information reader or her attributes/access privileges. There are many attainable cases:

1. revocation of one or more role attributes of a public domain user;
2. revocation of a public domain user which is equiva-lent to revoking all of that user's attributes. These operations are done by the AA that the user belongs to, where the actual computations can be delegated to the server to improve efficiency (8).

Policy updates. A PHR owner will update her sharing policy for an existing PHR document by change the attributes (or access policy) within the ciphertext. The supported operations embody add/delete/modify, which might be done by the server on behalf of the user.Break-glass. once Associate in Nursing emergency happens, the regular access policies might not be applicable. To handle this example, break-glass access is required to access the victim's PHR. In our framework, every owner's PHR's access right is additionally delegated to Associate in Nursing emergency department (ED, (6)). to stop from abuse of break-glass possibility, the emergency workers must contact the ED to verify her identity .

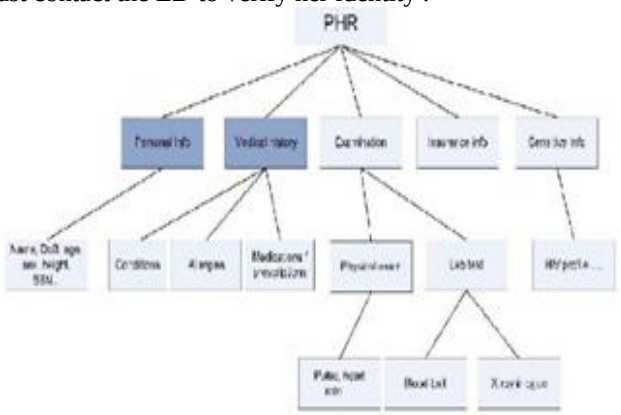


Fig. 2. The attribute hierarchy of files—leaf nodes are atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader have access to.

IV. DESIGN CONCERNS

In this point we have to discuss some key issues:

A. *MA-ABE in Public Domain*

For the PUDs, our framework delegates the key management functions to multiple attribute authorities. so as to attain stronger privacy guarantee for knowledge house owners, the Chase-Chow (CC) MA-ABE theme [21] is employed, wherever every authority governs a disjoint set of attributes distributively. it's natural to associate the ciphertext of a PHR document with associate degree owner-specified access policy for users from pudding. However, one technical challenge is that CC MA-ABE is actually a KP-ABE theme, wherever the access policies square measure implemented in users' secret keys, and people key-policies don't directly translate to document access policies from the owners' points of read. By our style, we have a tendency to show that by agreeing upon the formats of the key-policies and also the rules of specifying that attributes square measure needed within the ciphertext, the CC MA-ABE will truly support owner-specified docu-ment access policies with some extent of flexibility (such because the one in Fig. 4), i.e., it functions kind of like CP-ABE.2In order to permit the house owners to specify associate degree access policy for every PHR document, we have a tendency to exploit the actual fact that the fundamental CC MA-ABE works in an exceedingly manner kind of like fuzzy-IBE, wherever the brink policies (e.g., k out of n) square measure supported. Since the brink gate has associate degree intrinsic symmetry from each the encryptor and also the user's purpose of views, we will predefine the formats of the allowed document policies in addition as those of the key-policies, so associate degree owner will enforce a file access policy through selecting that set of attributes to be enclosed within the ciphertext.

B. *Usage*

Setup. especially, the AAs initial generate the MKs and PK mistreatment setup as in CC MA-ABE. The kth AA defines a disjoint set of role attributes GB, that are comparatively static properties of the general public users. These attributes are classified by their varieties, like profession and license standing, medicine, and affiliation wherever every sort has multiple attainable values. Basically, every AA monitors a disjoint set of attribute varieties. for instance, within the care domain, the AMA could issue medical skilled licenses like "physi-cian," "M.D.," "nurse," "entry-level license," etc., the ABMS may certify specialties like "internal medication," "surgery," etc; and AHA could outline user affiliations like "hospital A" and "pharmacy D." so as to represent the "do not care" possibility for the homeowners, we tend to add one wildcard attribute "_" in every variety of the attributes.

a) Improvement and End-user Revocation

The original CC MA-ABE theme doesn't modify economical and on-demand user revocation. to realize this for MA-ABE, we tend to mix ideas from YWRL's reversible KP-ABE [9],

[15] (its details area unit shown in supplementary material, accessible online), associated propose an increased MA-ABE theme. specifically, associate authority will revoke a user or user's attributes like a shot by reencrypting the cipher-texts and change users' secret keys, whereas a serious a part of these operations may be delegated to the server which boosts potency.

The idea to revoke one attribute of a user in MA-ABE is as follows: The AA World Health Organization governs this attribute actively updates that attribute for all the affected unrevoked users. to the present finish, the subsequent updates ought to be carried out: 1) the public/master key parts for the affected attribute; (2) the key key element similar to that attribute of every unrevoked user; 3) conjointly, the server shall update all the ciphertexts containing that attribute. so as to cut back the potential machine burden for the AAs, we tend to adopt proxy encoding to delegate operations a pair of and three to the server, and use lazy-revocation to cut back the overhead. specifically, every information attribute i is related to a version range veri. Upon every revocation event, if i is associate affected attribute, the AA submits a rekey rki$i0 ¼ t0i=ti to the server, World Health Organization then reencrypts the affected ciphertexts and will increase their version numbers. The unrevoked users' secret key parts area unit updated via an analogous operation exploitation the rekey. To delegate secret key updates to the server, a dummy attribute has to be in addition outlined by every of N nine one AAs, that area unit perpetually ANDed with every user's key-policy to stop the server from grasping the key keys. This conjointly maintains the resistance against up to N nine a pair of AA collusion of MA-ABE (as are shown by our security proof). exploitation lazy-revocation, the affected cipher-texts associated user secret keys area unit solely updated once an affected unrevoked user logs into the system next time. By the shape of the rekey, all the updates may be aggregate from the last login to the foremost current one.To revoke a user in MA-ABE, one has to ascertain a tokenish set of attributes (_) specified while not it the user's secret key's access structure (Au) can ne'er be glad. as a result of our MA-ABE theme needs conjunctive access policy across the AAs, it suffices to search out a tokenish set by every AAk (_k nine Auk), while not that sea bird won't be glad, then cypher the tokenish set (_kmin) out of all Alaska.

b) Enforce Write Access Control

If there's no restrictions on write access, anyone could write to someone's PHR victimisation solely public keys, that is undesirable. By granting write access, we have a tendency to mean an information contributor ought to acquire correct authorization from the organization she is in (and/or from the targeting owner), that shall be able to be verified by the server United Nations agency grants/rejects write access..

A naive means is to let every contributor acquire a signature from her organization on every occasion she intends to jot down. nevertheless this needs the organizations be continuously on-line. The observation is that, it's fascinating and sensible to authorize in line with time periods whose roughness is adjusted. for instance, a doctor ought to be allowable to jot down solely throughout her workplace hours; on the opposite hand, the doctor should not be able to write to patients that aren't treated by her. Therefore, we have a tendency to mix signatures with the hash chain technique to realize our goals

V. SECURITY ANALYSIS

In this paper, we analyze the security of the PHR sharing answer. First we focus to show to achieves knowledge confidentiality by proving the improved MA-ABE scheme to be secure beneath the attribute-based selective-set model [21], [34]. we've the subsequent main theorem.

In addition, our framework achieves forward secrecy, and security of write access management. For elaborate security analysis and proofs, please visit the net supplementary material, obtainable on-line, of this paper.

We conjointly compare the protection of our theme with many existing works, in terms of confidentiality guarantee, access management roughness, and supported revocation methodology, etc. we elect four representative progressive schemes to check with:

1. the VFJPS theme [28] supported access management list (ACL);
2. the BCHL theme supported HIBE [8] wherever every owner acts as a key distribution center;
3. the azoimide revokable CP-ABE theme [23], wherever we have a tendency to adapt it by assumptive victimization one course with one authority and multiple PSDs to suit our setting;
4. the NGS theme in [16] that could be a privacy-preserving EHR system that adopts attribute-based broadcast secret writing to attain knowledge access control;
5. The RNS theme in [25] that enhances the Lewko-Waters MA-ABE with revocation capability

This scheme achieves high privacy guarantee and on-demand revocation. The conjunctive policy restriction only applies for PUD, while in PSD a user's access structure can still be arbitrary monotonic formula. In comparison with the RNS scheme, in RNS the AAs are independent with each other, while in our scheme the AAs issue user secret keys collectively and interactively. Also, the RNS scheme supports arbitrary monotonic Boolean formula as file access policy. However, our user revocation method is more efficient in terms of communication overhead. In RNS, upon each revocation event, the data owner needs to recompute and send new ciphertext components corresponding to revoked attributes to all the remaining users.

VI. SCALABILITY AND EFFICIENCY

A. Storage and Communication Costs

First, we evaluate the scalability and efficiency of our solution in terms of storage, communication, and computa-tion costs. We compare with previous schemes in terms of

TABLE 3
Notations for Efficiency Comparison

S_k	Bit size of a FEK
S_1	Bit size of an element in $\mathbb{G}_1/\mathbb{G}_2$
S_T	Bit size of an element in $\mathbb{G}_T$
S_z	Bit size of an element in $\mathbb{Z}_p^*$
$S_\mathcal{P}$	Bit size of access policy and attribute set in CT
N (or N_i)	Number of AAs in a PUD (or the i-th PUD)
N_o	The number of owners in the system
N_u	The number of data users in the system
N_r	Number of revoked users for a file
N_a	Number of users in an attribute group
m	Number of attribute types in the PUD
t_c, t_u	Total number of attributes appeared in CT, sk_u
l	Depth of file hierarchy of an owner's PHR

Next, we have a tendency to assess the process price of our theme through combined implementation and simulation. we offer the primary implementation of the GPSW KP-ABE theme [35] (to the simplest of our knowledge), and conjointly integrated the ABE algorithms into a image PHR system, Indivo [27], [36]. The GPSW KP-ABE theme is tested on a laptop with three.4 gigacycle processor, exploitation the pairing-based cryptography (PBC) library [37]. the general public para-meters square measure chosen to supply eighty bits security level, and that we use a pairing-friendly type-A 160-bit elliptic curve cluster [37]. This parameter setting has conjointly been adopted in alternative connected works in ABE [19], [38]. we have a tendency to then use the ABE algorithms to encipher at random generated XML-formatted files (since real PHR files square measure tough to obtain), and implement the user-interfaces for information input and output. thanks to area limitations, the main points of image imple-mentation square measure according in [36].

VII. CONCLUSION

In this theme our projected work specifically concentrate on the access needs in cloud-based health record management systems partitioning the sysyem, that considers each personal and skilled PHR users. Our abrogation ways in which for ABE in every styles of domains area unit consistent. The RNS theme alone applies to the course.In this framework of secure sharing of personal health records in cloud comput-ing. Considering half trustworthy cloud servers, we've a bent to argue that to entirely notice the patient-centric construct, patients shall have complete management of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the distinctive challenges brought by multiple PHR owners and users, in that we've a bent to greatly shrink the standard of key management whereas enhance the privacy guarantees compared with previous works. we've a bent to utilize ABE to inscribe the PHR data, thus patients can alter access not alone by personal users, but to boot varied users from public domains with utterly totally different masterly roles, qualifications, and affiliations. Further-more, we've a bent to boost academic degree existing MA-ABE theme to handle economical and on-demand user revocation, and prove its security. Through implementation and simulation, we've a bent to point out that our resolution is every ascendible and economical.

REFERENCES

[1] 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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[2] H. Lo¨hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act," http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safe-guarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[9] 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.

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

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryp-tion with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[16] 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.

[17] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Patient Self-Controllable Access Policy on Phi in Ehealthcare Systems," Proc. Advances in Health Informatics Conf. (AHIC 10), 2010.

[18] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryp-tion," technical report, Univ. of Twente, 2009.

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

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

[21] 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.

[22] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation," technical report, Univ. of Waterloo, 2010.

[23] 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 2011.

[24] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-Based Access

Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2011.

[25] 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.

[26] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," EUROCRYPT: Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588, 2011.

[27] "Indivo." http://indivohealth.org/, 2012.

[28] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 123-134, 2007.

[29] A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," EUROCRYPT: Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588, 2011.

[30] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, "Spins: Security Protocols for Sensor Networks," Wireless Network-ing, vol. 8, pp. 521-534, Sept. 2002.

[31] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004.

[32] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Third Int'l Conf. Palo Alto on Pairing-Based Cryptography-Pairing, pp. 248-265, 2009.

[33] S. Mu¨ller, S. Katzenbeisser, and C. Eckert, "Distributed Attribute-Based Encryption," Proc. 11th Int'l Conf. Information Security and Cryptology (ICISC 08), pp. 20-36, 2009.

[34] S. Chow, "New Privacy-Preserving Architectures for Identity-/ Attribute-Based Encryption," PhD thesis, NYU, 2010.

[35] Y. Zheng, "Key-Policy Attribute-Based Encryption Scheme Im-plementation," http://www.cnsr.ictas.vt.edu/resources.html, 2012.

[36] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst., 2011.

[37] B. Lynn, "The Pbc Library," http://crypto.stanford.edu/pbc/, 2012.

[38] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," J. Computer Security, vol. 18, no. 5, pp. 799-837, 2010.

[39] S. Harris, C. Swamidoss, D. Rafferty, D. Leszcynski, A. Mancini, S. Keil, S. Garwood, and P. Barash, "Use of adap-tive conjoint analysis to determine the optimal configuration for a transesophageal echocardiography workshop
", Society for Technology in Anesthesia, 2003. **Annual**.

[40] North Carolina Department of Health and Human Ser-vices. NC Health Choice Emergency Room Utilization Statis-tics October 1998 Through September 1999. 1999, http://www.dhhs.state.nc.us/dma/CHIP/table9.htm..

[41] AHIMA (American Health Information Management Association). myPHR Personal Health Record: A guide to understanding and managing your personal health informa-tion. http://www.myphr.com/resources/phr_search.asp.

[42] N. Ferris, Finding Foreman, in Government Health IT, 2007, p. 16-21.

[43] IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013.scalable and secure sharing of personal health record using attribute based encryption by Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE.