ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)
Vol. 2, Issue 3 (July - Sept. 2015)
International Journal of Advanced Research in Education & Technology (IJARET)

# Isolation Preserving Access Control Mechanism for Delicate Fitness Information

[I]S.Suganya, [II]Dr. S.Dhanalakshmi
[I]M.Phil Full Time Research Scholar, [II]Head of the Department
[I,II]Dept. of Computer Science, Vivekananda College of Arts and Sciences for Women (Autonomous), Namakkal, Tamilnadu, India

**Abstract**
*Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. Personal health record (PHR) 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. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The security schemes are used to protect personal data from public access. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing .In this paper we propose novel patient-centric framework and suite of mechanism for data access control to PHR's stored in semi-trusted servers Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Data owner update the personal data into third party cloud data centers. Multiple data owners can access the same data values. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.*

**Key Words**
*Personal health records; cloud computing; data privacy; fine-grained access control; attribute- based encryption.*

## I. Introduction

In recent years, personal health record (PHR) has e- merged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed in .While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A feasible and promising approach would be to en- crypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the user s who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. However, the goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users access requests are generally unpredictable, it is difficult for an owner to determine a list of them. On the other hand, different from the single data owner scenario considered in most of the existing works in a PHR system, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority (i.e., cause the key escrow problem). In this paper, we endeavor to study the patient- centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based 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 know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions: (1) We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To ad- dress the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributively by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications requirements, while incurring minimal key management overhead for both owners and users in the system. In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios. (2) In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. Furthermore, we enhance MA-ABE by putting forward an efficient and on-demand user/attribute revocation scheme, and prove its security under standard security assumptions. In this way, patients have full.

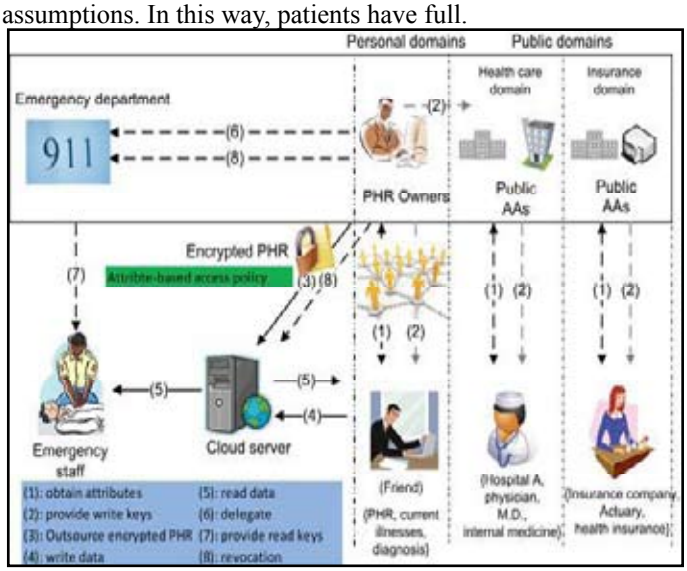


Fig 1 : System Architecture

## II. Related Work:

### Key-Policy Attribute-based Encryption (KP-ABE):

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

### Cipher text Policy Attribute based Encryption (CP-ABE):

CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential.

### Multi-Authority Attribute-Based Encryption (MA-ABE):

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

### 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 EHR systems, where each patient,s EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et.al applied ciphertext policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/ professional domains. I, Akinyele et al. investigated using ABE to gen-erate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline. 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 since the TA can access all the encrypted files, opening the door for potential privacy exposure.

In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users, attributes or roles and generating secret keys. In fact, different organizations usually form their own (sub) domains and become suitable authorities to define and certify different sets of attributes belonging to their (sub) domains (i.e., divide and rule). For example, a professional association would be responsible for certifying medical specialties, while a regional health provider would certify the job ranks of its staffs. Second, there still lacks an efficient and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, which are essential parts of secure PHR sharing. Finally, most of the existing works do not differentiate between the personal and public do-mains, which have different attribute dentitions, key management requirements and scalability issues.

Our idea of conceptually dividing the system into two types of domains is similar with that in, however a key difference is in a single TA is still assumed to govern the whole professional

domain. 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 user secret keys to the cloud server.

### A. Disadvantages of Existing System:

The concept of privacy-preservation for sensitive data can require the enforcement of privacy policies or the protection against identity disclosure by satisfying some privacy requirements. Investigate privacy-preservation from the anonymity aspect. The sensitive information, even after the removal of identifying attributes, is still susceptible to linking attacks by the authorized users. Minimize the imprecision aggregate for all queries. The imprecision added to each permission/query in the anonymized micro data is not known. Not satisfying accuracy constraints for individual permissions in a policy/workload.

## III. Proposed System

Personal Health Record is an internet based application that allows people to access and co-ordinate their lifelong health information and make if appropriate parts of its available to those who need. Personal Health Records security and protection of its data have been of great concern and a subject of research over the years. There are many different forms of cryptographic mechanisms like AES, MD5 proposed to guarantee data security. In this work we propose a unique authentication and encryption technique using AES algorithm.

In PHR data refers to the information that is collected, analyzed and stored. Example Medical history, List of medical problems, Medication history. The PHR owner herself should decide how to encrypt her file and to allow which set of users to obtain access to each file. In PHR infrastructure is the computing platform which processes or exchanges healthcare data such as software package and website.

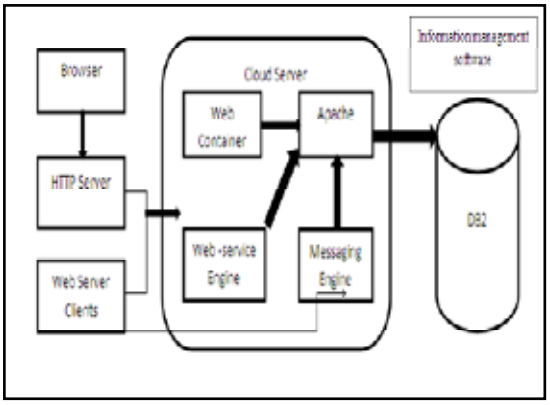



Fig. 1 : System Architecture

### Advantages of Proposed System

- Quickly find out information of patient details.
- In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.
- If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.
- To provide easy and faster access information. To provide user friendly environment.
- To provide data confidentiality and write access control.

### Implementation

Using attribute based encryption technique we are providing security to the database. A sensitive data is shared and stored on cloud server, there will be a need to encrypt data stored at third party.

In Attribute based encryption cipher text labeled with set of attribute. Private key associated with access structure that control which cipher text a user is able to decrypt.

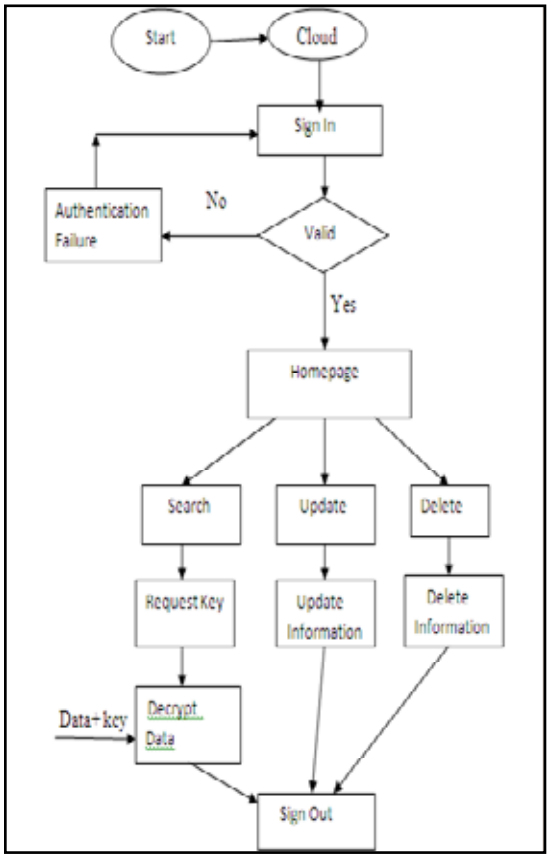



Fig. 2 : System Flow Diagram

The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this system can be achieved only when user and server are in a trusted domain. So, the new access control scheme that is Attribute Based Encryption (ABE) scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control.

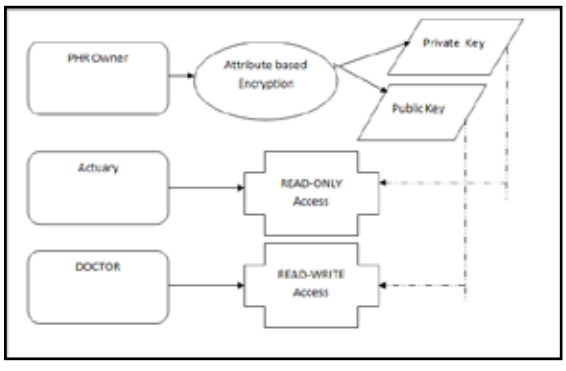



Fig. 3 : ABE Architecture

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. Akinyele et al investigated using ABE to generate self-protecting EMRs, which can either be stored on cell phones or cloud servers so that EMR could be accessed when health provider is in offline also.

### The Attribute Hierarchy

We are using attribute based encryption for providing security. For that we use following distribution of attributes that are mainly important.

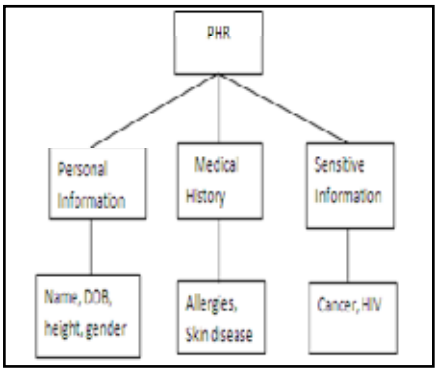



Fig. 4 : The attribute

**ALGORITHM**

**Attribute-Based Encryption:**

ABE with multiple authorities as proposed by Lewko and Waters proceeds as follows;

**Setup (λ, U) → (PK, MK).**

The setup algorithm takes as input a security parameter λ and a universe description U, which defines the set of allowed attributes in the system. It outputs the public parameters PK and the master secret key MK.

**Encrypt (PK, M, S) → CT.**

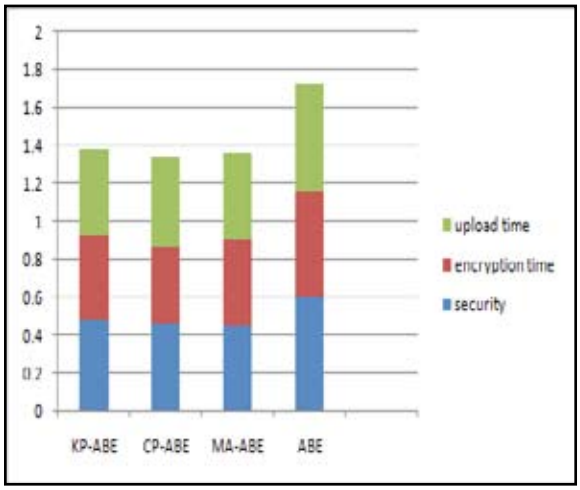
The encryption algorithm takes as input the public parameters PK, a message M and a set of attributes S and outputs a cipher text CT associated with the attribute set.

**KeyGen (MK, A) → SK.**

The key generation algorithm takes as input the master secret key MK and an access structure A and outputs a private key SK associated with the attributes.

**Decrypt (SK, CT) → M.**

The decryption algorithm takes as input a private key SK associated with access structure A and a cipher text CT associated with attribute set S and outputs a message M if S satisfies A or the error message ⊥ otherwise. The correctness property requires that for all sufficiently large λ ∈ N, all universe descriptions U, all (PK, MK) ∈ Setup(λ, U), all S ⊆ U, all SK ∈ KeyGen(MK, A), all M ∈ M, all A ∈ G and all CT ∈ Encrypt(PK, M, S), if S satisfies A, then Decrypt(SK, CT) outputs M.




**Result**

Fig. 5 : Result Analysis Graph

The upload time, Encryption time and security for ABE is better than the other related methods. It provides better performance result in security purpose. The above graph shows the performance analysis of the paper.

### VI. Conclusion and Future Work

In this paper made a survey on the Improving the Security on Public Health Record System in Cloud Computing. And also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. It is efficient in the Conjunctive Property. But somewhat limitations on MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation. Because it can be affect the non-revoked users. So move to the Attribute Based Broadcast Encryption. It satisfies the Disjunctive Property also and handles the revocation perfectly. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. homomorphic encryption with data auditing is used to verify the trustworthiness of third party auditor.

The personal health record system needs security against attackers and hackers. Scalable and Secure sharing includes basic securities to protect the information from unauthorized access and loss. This paper proposed the new approach for existing PHR system for providing more security using attribute based encryption which plays an important role because these are unique and not easily hackable. We are reducing key management problem and also we enhance privacy guarantee.

### 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," in Secure Comm,10, Sept.2010, pp. 89–106.*

[2] *H.Lohr, A.R.Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI, 10, 2010, pp. 220–229.*

[3] *M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121–130.*

[4] *S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASSIACCS,10,*

*2010.*

*[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM,10, 2010.*

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

*[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.*

*[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.*

*[9] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.*

*[10] Melissa Chase "Multi-authority Attribute based Encryption," Computer Science Department Brown University Providence, RI 02912*