International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

# Attribute Based Access Control in Personal Health Records Using Cloud Computing

**Supriya D. Patil[1], Komal S. Talekar[2], Reshma M. Raskar[3], Pooja A. Chavans[4], Prof. Rupali Kadu[5]**

*[1,2,3,4]B.E. student, AES COET, Wadwadi (Maharashtra)*
*[5]Professor, Dept. of Computer Engineering, AES COET, Wadwadi (Maharashtra), INDIA*

---

***Abstract***- *Personal health records (PHR) Associate in Nursing rising health data exchange model, that facilitates PHR homeowners to expeditiously share their personal health knowledge among a spread of users as well as attention professionals still as family and friends. to confirm PHR owners' management of their outsourced PHR knowledge, attribute based mostly encoding (ABE) mechanisms are thought of. A patient-centric, attribute based mostly PHR sharing theme which might give versatile access for each skilled users like doctors still as personal users like family and friends. every PHR file is encrypted Associate in Nursingd hold on in a very attention cloud at the side of an attribute based mostly access policy that controls the access to the encrypted resource. In projected system Associate in Nursing attribute based mostly authorization mechanism wont to authorize access requesting users to access a given PHR resource supported the associated access policy whereas utilizing a proxy re-encryption theme to facilitate the approved users to decode the specified PHR files. additionally use Multi authority attribute based mostly encoding theme. It provides the safety and confidentiality to the PHR knowledge.*

**Keywords:** ***PHR, ABE, Cloud Computing*****.**

## I. Introduction

In recent year, Personal Health Record (PHR) has developed because the rising trend within the care technology and by that the patients area unit expeditiously able to produce, manage and share their personal health info. This PHR is currently a day's keep within the clouds for the value reduction purpose and for the straightforward sharing and access mechanism. the most concern concerning this PHR is that whether or not the patient is in a position to regulate their knowledge or not. Cloud storage permits the PHRs to be outsourced to cloud infrastructures rather than storing them regionally. This approach doubtless ends up in higher handiness of health knowledge likewise as relieving the patients from the burden of maintaining them. it's terribly essential to possess the fine grained access management over the info with the semi-trusted server. however during this the PHR system, the safety, privacy and health knowledge confidentiality area unit creating challenges to the users once the PHR keep within the third party storage area unit like cloud services. The PHR knowledge ought to be secured from the external attackers and conjointly it ought to be shield from the inner attackers such from the cloud server organization itself.

### Personal Health Record (PHR)

In recent year, Personal Health Record (PHR) has developed because the rising trend within the care technology and by that the patients area unit expeditiously able to produce, manage and share their personal health info. This PHR is currently a day's keep within the clouds for the value reduction purpose and for the straightforward sharing and access mechanism. the most concern concerning this PHR is that whether or not the patient is in a position to regulate their knowledge or not. Cloud storage permits the PHRs to be outsourced to cloud infrastructures rather than storing them regionally. This approach doubtless ends up in higher handiness of health knowledge likewise as relieving the patients from the burden of maintaining them. it's terribly essential to possess the fine grained access management over the info with the semi-trusted server. however during this the PHR system, the safety, privacy and health knowledge confidentiality area unit creating challenges to the users once the PHR keep within the third party storage area unit like cloud services. The PHR knowledge ought to be secured from the external attackers and conjointly it ought to be shield from the inner attackers such from the cloud server organization itself.

## II. Literature Survey

### [1] A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing (2016)

The attribute based encryption (ABE) technique is employed that during which the PHR owner encrypts the data according to associate degree access policy which determines the potential users UN agency are eligible to access.

### [2]Removing Barriers in Using Personal Health Record Systems (2016)

Barriers and encourage individuals to adopt PHRS in order that they will manage their health by observation

and dominant their clinical knowledge mistreatment PHRS. For distinctive barriers from half-dozen completely different aspects are there - motivation, usability, ownership, ability, privacy and security, and movableness.

**[3]Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) Systems**

This system projected associate degree hierarchal comparison-based encryption(HCBE) theme and a dynamic policy updating(DPU) theme for achieving dynamic access management in cloud-based PHR systems. The HCBE theme supports time comparison in attribute-based secret writing in associate degree economical approach by incorporating attribute hierarchy into CBE. The DPU theme utilizes the PRE technique to delegate the policy change operations to the cloud.

**[4]Collaborative and secure sharing of healthcare data in multi-clouds**

The safety & privacy measures are employed in these theme are RBAC i.e. Role Access management privileges are granted to roles not for person attribute based encryption(ABE). encipher the information over user attribute additionally secure sharing of the information is mistreatment RSA rule of cryptography additionally privacy protective share identifires used SHA-1 algorithms.

**[5]Distributed clinical data sharing via dynamic access-control policy transformation**

The Delivery of health care knowledge firmly in EHR systems is resolved during this paper. The cloud based mostly EHR system uses ABE technique for access management of information. The EHR design for secure knowledge sharing supported many cryptographical building blocks & secret sharing with Role-based Access Control (RBAC) to safeguard patients privacy.

**[6]Preserving Privacy of Patients based on Re-identification Risk (2015)**

The system used ARX for protective the privacy of patient's knowledge. The privacy is measured through re-identification risk supported the individuality of records within the dataset. a mix of anonymization techniques like k-Anonymity, l-Diversity & t-Closeness is applied to cut back the re-identification Srisk and thence the privacy of the patients is preserved.

**[7]Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges (2016)**

These systems are able to monitor vital health things use web of Things—IoT and cloud computing. The ABE and IBE, along side their variants ar employed in this method for health care cloud knowledge privacy. totally homomorphic encryption is taken into account for maintaining knowledge privacy in these systems.

## III. Attribute-Based Encoding (ABE)

Attribute-based encoding could also be a sort of public-key cryptography among that the key key of a user and additionally the ciphertext square measure dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the secret writing of a ciphertext is possible providing the set of attributes of the user key matches the attributes of the ciphertext. There square measure primarily two sorts of attribute-based cryptography schemes: Key policy attribute-based cryptography (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE).

Main challenges are:

- Key coordination
- Key legal document
- Key revocation

ABE uses a tree-based access structure which ought to be proud of a given set of attributes therefore on rewrite the knowledge. The tree-based access structure permits the encryptor to specify that attributes can decrypt the knowledge.

An (Key-Policy) Attribute based encoding theme consists of 4 algorithms.

**Setup**

This is a randomised rule that takes no input aside from the implicit security parameter. It outputs the general public parameters PK and a passkey MK.

**Encryption**

This is a randomised rule that takes as input a message m, a group of attributes γ, and also the public parameters PK. It outputs the ciphertext E.

**Key Generation**

This is a randomised rule that takes as input – associate access structure A, the key MK and also the public parameters PK. It outputs a decipherment key D.

**Decryption**

This rule takes as input – the ciphertext E that was encrypted below the set γ of attributes, the decipherment keyD for access management structure A and the general public parameters PK. It outputs the message M if γ ∈

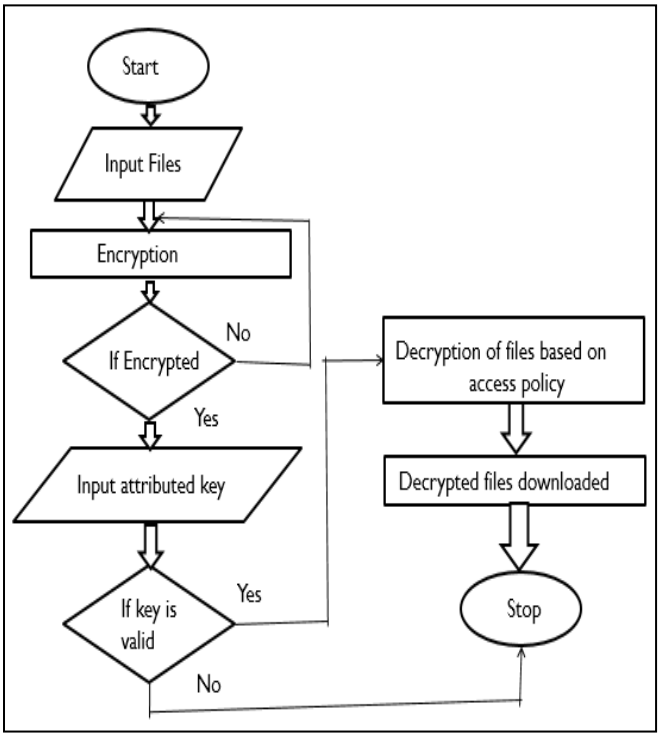


**Fig. III.1.** Attribute Based Encryption

## IV. Architecture Diagram

To assure the patients' management over access to their own PHRs, it's a promising technique to encode the PHRs before outsourcing. The system is novel patient-centric framework and a set of mechanisms for information access management to PHRs keep in semi-trusted servers s.to realize ne-grained and ascendible knowledge access management for PHRs, system leverage attribute based encoding (ABE) techniques to encode every patient's attribute.

The system is provides the fine-grained access management to the system by exploitation the various attribute based encoding schemes. during this system, the users are classed into 2 security domains known as Personal Security Domain and public security Domain. The users like members of the family, friends are enclosed within the personal domain and therefore the users from the health care organization and insurance recent are considering because the

information users from the general public domain. For each the 2 totally different set of user domain the variations of attribute based encoding is employed. For the private security domain the reversible Key-policy attribute based encoding theme is employed. For the general public security domain the Multiple-Authority attribute theme is planned.

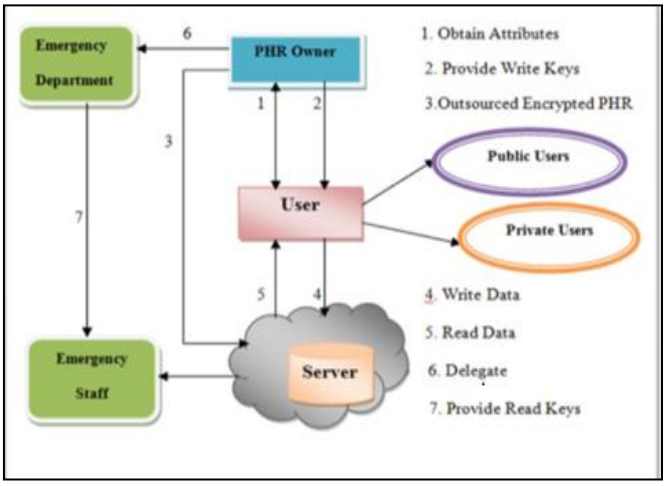


**Fig.IV.1.Architecture Diagram of PHR System**

## V. Planned PHR System design

The system achieves information confidentiality by proving the improved MA-ABE theme. additionally within the security domain, it achieves the forward secrecy and security of write access management. therefore this technique have the advantages of fully-patient central management over the private health record by the patient it extremely reduces the key management overhead and it enhances the privacy guarantee. The state of affairs provides the thought concerning the requirement for a system that full the subsequent security requirements:

Protect health records from network assaulter. So, information is to be encrypted before it's sent to the net PHR. Health records protected against third parties United Nations agency store PHRs. The third party manages internet PHRs that aren't accessible to the plain information. The access policy involved with the encrypted information, specified solely those users having a secret key related to set of attributes that satisfies the policy may be capable of decrypting it. Users from the skilled domain and users from the social domain each ought to be properly echt and approved to access the info.

## VI. Conclusion

We have planned a secure and versatile attribute primarily based PHR sharing theme mistreatment cloud computing that satisfies the supposed security and privacy needs. to confirm patient-centric PHR sharing, PHR homeowners should have full management of outsourced non-public PHR information. Thus, it's vital to store PHR information in AN encrypted format in third-party cloud platforms. once the PHR information square measure keep in AN encrypted format, achieving fine-grained access is sort of difficult.. Most outstanding existing cloud primarily based PHR schemes have used ABE schemes to alter fine grained PHR access. For future

work, we have a tendency to conceive to implement a paradigm of the planned theme and thereby analyze its performance and effectiveness.

## VII. References

1. Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk "A Patient-Centric Attribute Based Access ControlScheme for Secur..e Sharing of Personal HealthRecords Using Cloud Computing" Dept. of Information and Communication Technology, University of Agder (UiA) 2016

2. Mohammad Alyami,Yeong-Tae Song "Removing Barriers in Using Personal Health Record Systems" IEEE ICIS 2016

3. Benjamin Fabian, Tatiana Ermakova" Collaborative and secure sharing of healthcare data in multi-clouds"Institute of Information system Spandaure

4. Xuhuiliu,Qinliu" Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) System" Preprint submitted to Information Sciences June 23, 2016

5. F. Rezaeibagha, Y. Mu "Distributed clinical data sharing via dynamic access-control policy transformation " International Journal of Medical Informatics 89 (2016) 25–31

6. Anam Sajid, Haider Abbas" Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges" Springer Science+Business Media New york 2016

7. Himanshu Taneja , Kapil" Preserving Privacy of Patients based on Re-identification Risk "Procedia Computer Science 70 ( 2015 ) 448 – 454.