International Journal of Research
eISSN: 2348-6848 & pISSN: **2348-795X***Vol-4 Special Issue-6*
National Conference on Innovations in Information and Communication Technology
Held on 17-03-2017, Organized by Department of Information Technology,Meenakshi Sundararajan Engineering College,
363,Arcot Road Kodambakkam, Chennai 600024, India

AN EFFICIENT DATA SHARING ATTRIBUTE BASED ENCRYPTION AND TIME ACCESS CONTROL SCHEME IN CLOUD COMPUTING

R.Chitraa,M.Harrini,P.Keerthana

Department of Computer Science and Engineering, MeenakshiSundararajan Engineering College, Kodambakkam, Chennai, Tamilnadu, India

chitraaramachandran@gmail.com,harrini96@gmail.com,keertugp@gmail.com

Abstract- ***The personal health information managed by the third party cloud servers is shared across distributed health care providers for medical consultation which could possibly be leaked and misused. The secrecy and time efficiency present in cloud is of a questionable state in current scenario, even when it's customized by providing faceless user Id. Personal health records are sensitive information which the user might not wish to dismiss to anyone unless they are trustworthy. The problem possesses a serious stage that these insecure data records could be used in illegal insurance claims and organ trade. In addition to handling all these issues, there is a need to deal with sharing of medical records as well in emergency situations for personal consulting. Cipher text-policy with Attribute Based Encryption (ABE) authentication scheme with time based Authorized Accessible Privacy Model (AAPM) in the distributed m-health care using cloud computing system is proposed to facilitate sharing of personal health information securely and efficiently in cloud. This kind of system will resolve the challenge of keeping the patient's data with very high confidentiality and keeps the identity of the patient or the data owner private.***

Keywords-*Cloud computing with data privacy, data sharing, fine grained access control, CP-ABE (CIPHER TEXT POLICY –ATTRIBUTE BASED ENCRYPTION, TIMER.*

I. INTRODUCTION:

Cloud computing assists a massive number of users to access, store and share sensitive information and application present in distant location over untrusted cloud servers, hence enhancing the security features in cloud has become mandatory particularly in the field of healthcare and military.Cloud computing security involves a set of policies and techniques that protects the information and data application associated with it. One such policy is the usage of ABE (Attribute Based Encryption) in the PHR (Personal Health Records) system. ABE is a public key encryption scheme where the private key of the user and the cipher text that will be generated depends upon the set of attributes selected for encryption.CP-ABE (Cipher text Policy-ABE) has been a preferred encryption technique to solve the challenging problem of secure data sharing in
cloud computing [5].

ABE is a technique where the attributes are used to describe the user credentials and the formulas to be applied over these credentials are attached to the cipher text by the encrypting party the shared file in a PHR system is usually a group of files namely personal information, health records etc. Which possess a hierarchical structure that can be exploited efficiently to implement a fine grained access control.

International Journal of Research
eISSN: 2348-6848 & *pISSN:* **2348-795X***Vol-4 Special Issue-6*
National Conference on Innovations in Information and Communication Technology
Held on 17-03-2017, Organized by Department of Information Technology,Meenakshi Sundararajan Engineering College,
363,Arcot Road Kodambakkam, Chennai 600024, India

II.EXISTING STRUCTURE:

The existing structure of a distributed m-healthcare system enabled the patient to manage their Electronic Medical Records (EMR) in a centralized way by storing them in the cloud provided by the cloud service provider who is a semi-trusted party. It allows the patient to manage their personal health records with utmost flexibility for data sharing and scalability but it is admin-centric which had an impact on the system and it also supported revocation mechanism thereby making it difficult to identify the root which had an adverse impact on data privacy. One of the major pitfalls of the existing system used for storing PHR (Personal Health Record) was illegal insurance claims, organ trade and there was no level of categorization among the data that was stored.

Hence in order to protect the sensitive information, the encryption scheme namely

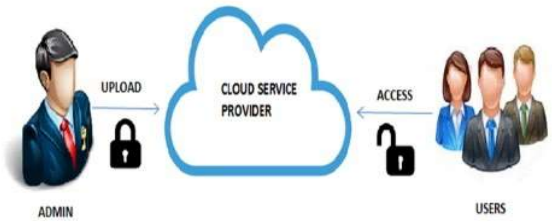


Fig2.1. A representation of existing system

symmetric where a single shared private key is used or asymmetric encryption where two different keys namely the public key for encryption and the private key for decryption are used. Hence there is a prevalence of asymmetric encryption over symmetric encryption.

To enhance such encryption scheme present in cloud ABE is used where either of the two commercially strong encryption algorithm namely AES (Advanced Encryption Standard), DES (Data Encryption Standard) could be used.

III.RELATED WORKS:

Provably secure ciphertext policy ABE by Ling Cheung an Calvin Newport – This paper basically concentrates on enhancing the security of the sensitive data like transaction details, legal document details, health records by means of fine grained access control on data. Here secret key used in the process is related to a set of attributes and the corresponding cipher text generated is associated to access structure. Decryption of data is possible only when the access structure of cipher text satisfies user's set of attributes thus ensuring that no unauthorized user can access such confidential data.

The scheme that is used here is chosen plaintext(CPA) along with the application of Decisional Bilinear Diffie-Hellman(DBDH) assumptions with the AND gates on positive and negative attributes used as access scheme.[2] The security of data is achieved by using one time signature to obtain Chosen Ciphertext(CCA) which forms a proof of security to the CP-ABE scheme under use. This provably secure scheme provides high level of data security suitable in distributed environment as well, because it supports complex access policies which can be used in both trusted or a centralized server without any online interactions.

Mediated cipher text policy attribute based encryption (mCP-ABE) by Laun Ibraimi,Milan Petkovic,Svetla Nikova,Pieter Hartel and Willem Jonker- This paper extends the concept of CP-ABE by improving the security of data as it

provides the means to have instantaneous revocation. In CP-ABE attributes are valid only within specified time frame, so there is no way to revoke attributes before expiration time. Whereas in mCP- ABE it is possible to handle revocation problem by dividing the secret key into 2: one for

International Journal of Research
eISSN: 2348-6848 & *pISSN:* **2348-795X***Vol-4 Special Issue-6*
National Conference on Innovations in Information and Communication Technology
Held on 17-03-2017, Organized by Department of Information Technology,Meenakshi Sundararajan Engineering College,
363,Arcot Road Kodambakkam, Chennai 600024, India

the mediator and another for the end user.[4] Here the mediator has the attribute revocation list and thereby refuses to issue token for revoked attributes.

The CP-ABE runs four steps:

- Setup (key): This phase takes the security parameters such as encryption scheme as input and outputs the public key (PK) and the master security key (MSK). The responsibility is held by Trusted Authority (TA)

- Keygen (€, MSK): The key generation phase is run by the Trusted Authority (TA) who takes the input MK and € (attribute set) and then outputs the secret key (SK) associated with €

- Encrypt (M, T, PK): This phase converts the message into random sized ciphertext(CT). This phase is run by the encryptor, where the input taken isM (message), T (access policy), PK (public key) and output generated is cipher text (CT)

- Decrypt (CT, SK): This phase converts the cipher text into the original message that is intended to be received. This phase is run by the message receiver, who takes ciphertext(CT) and secret key(SK) as input and outputs the message(M). The usage of secret key maintains the integrity and confidentiality of the message.

TIMER: Secure and Reliable Cloud Storage against Data Re-outsourcing by Tao,Xiaofeng,Jin,Duncan, Jianfeng, Joseph was basically introduced to improve data security in cloud by using probabilistic challenge-response scheme[6] and also resist collusion of cloud server. It is mainly proposed for sensitive data of legitimate concern.

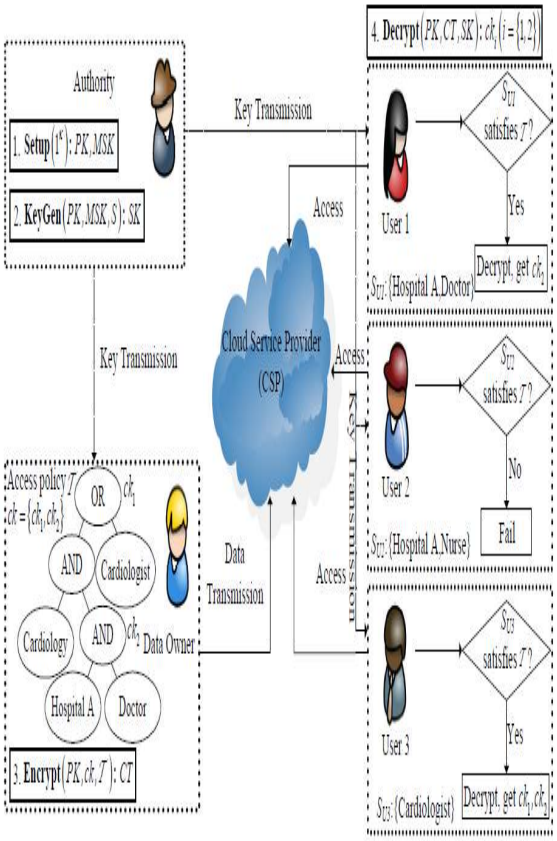


Fig 3.1 A Working example of CP-ABE

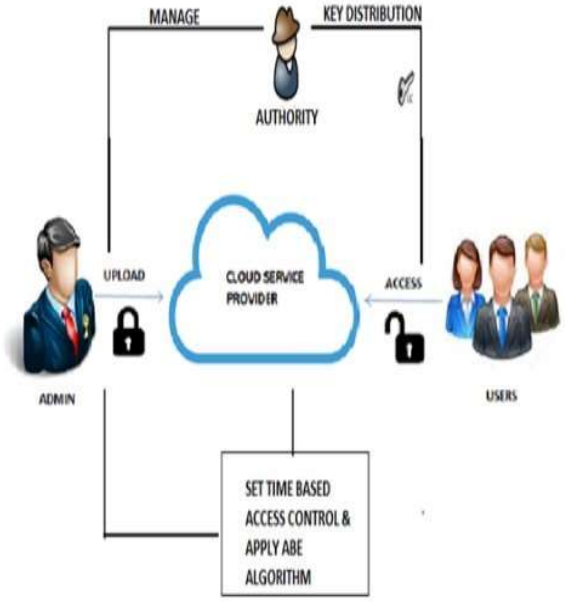
Here the system detects unauthorized or intruder by using response time bound module[6]. Outsourcing of files and collusion are detected and are avoided by means of cryptographic assumptions and network delays. TIMER scheme can also be used to establish a time frame in accessing records from cloud with different keys generated for each session.

IV.PROPOSEDWORKS:

The base idea of this paper is hierarchical file system where the drivers, folders and the files are found in groups which make it easier for the user to view the contents that he is interested in. Hence the search complexity of a system which is based on hierarchical access structure is improved.

International Journal of Research
eISSN: 2348-6848 & *pISSN:* **2348-795X***Vol-4 Special Issue-6*
National Conference on Innovations in Information and Communication Technology
Held on 17-03-2017, Organized by Department of Information Technology,Meenakshi Sundararajan Engineering College,
363,Arcot Road Kodambakkam, Chennai 600024, India

The introduction of file hierarchy in PHR system is done by splitting the medical record of a person into two parts ,one containing their personal information like name, address, contact number and the other containing the health information namely the blood sugar levels, blood pressure levels, heart failure reports, allergy reports etc. From these hierarchical files the set of attributes that are required to be encrypted are selected as per the user's wish. These two parts of medical records of a particular person is identified only by the use of the Aadhar card number or any other national identity number that remains unique to every person. This helps in creating an improved security and keeps the identity private. Hence the cipher text policy attribute based encryption authentication scheme is used in the distributed m-health care in cloud storage system is proposed.



Majority of the data that is required to e stored in a PHE system are images like electrocardiograph images and scan images rather than the subjective concerns. Therefore, the patient or the data owners are allowed to store multiple numbers of scan images and medical reports because of the scalability that the cloud provides. These medical images are encrypted using Advanced Encryption Standard scheme in such a way that intelligible content is not delivered to unauthorized persons. This encryption technique performs a bitwise exclusive OR operation on the set of image pixels along with the 128 bit key which changes every set of pixels present in the image. The time required by Advanced Encryption Standard algorithm for encryption and decryption of intelligible sensitive messages is less when compared to the time required by Data Encryption Standard algorithm. Hence the time efficiency is sufficiently improved.

For example, in case of a tie-up between the hospital and a medical research university to study the case of a particular disease the hospital might be obliged to the research university to provide data sets as well as to the patients stating that their identity and personal information will be kept secure and secret, in that case the hierarchical partitioning of files and encrypting them as set of attributes meets the requirement satisfaction of both ends.

The improved encryption process of introducing access privileges and file hierarchy in CP-ABE involves three levels of security:

- Directly authorized persons like the trusted group of doctors and the consulting physician are offered the access rights to the health records of the data owner(i.e.) the patient.
- Indirectly authorized person like the medical consultant or the biochemical analyst are offered access rights to only a subset of the personal health record.
- Unauthorized person like the nurse or the clerical operator of the PHR system is the one who has no access right to any kind of information in the cloud.

A cooperative authentication is provided to allow the patients or the data owner to authorize the corresponding privileges and access control for different kind of consultants who are located in the distributed health care platform by setting an access tree support for flexible threshold predictions of malicious behavior or illegal activities thereby ensuring the safety of the sensitive information.

In addition to the access control, a time access framework where different keys are generated for different sessions by the trusted authority(TA) and is distributed to the users like doctors or consulting physicians who are authorized by the data owner. These personnel can view the data by using the key generated for that particular session. Hence the PHI (Personal Health Information) can be viewed by the users only for a specific period of time and all these logs of access are being maintained by the admin who identifies any kind of malicious activity based on the response time of the user. In order to generate different keys for each session a completely trusted party called as the authority who do not have access to the cloud is used which creates a situation that only the data owner and his trusted group of pupils can view the data stored in cloud. In order to make the information available to the trusted group of doctors who would prescribe treatment in case of emergency situation is added to the circle of directly trusted user by the patient and hence the consulting physician can view the PHI if the patient is in emergency. The admin allows the request of time frame extension requested by the direct user after the consent from the data owner (i.e.) the patient.

For example, the patients have fixed an appointment to a particular consultant at a particular period of time. Here, the doctors on accepting this appointment can view his personal health information from the cloud server a few hours before the appointment by using the key that was provided by the trusted authority. This key is valid only till the appointment expires after which the information will appear to be encrypted to the doctor. In cases of exception from this normal situation any kind of access that is required by the doctor will be redirected o the admin who takes the necessary actions to keep the data secure and upon the consent from the respective data owner the doctor will be provided the key to access the PHR records.

V.CONCLUSION:

In this paper, the method of storing the PHR details in an encrypted manner (using CP-ABE) and Authorized Accessible Privacy Model (AAP) which enhances security and reduces the cost of storage and computation is explored. It significantly reduces the computation, communication overhead.

The usage of hierarchic file storage mechanism supports categorized data access providing the ease to retrieve the data. This system helps in providing an integrated and flexible time access data. It provides a means to handle the emergency health situations by enabling the patient to generate alert that reaches the close group of health professionals who can give them advice.

REFERENCES:

[1]J. Bethencourt, A. Sahai, and B. Waters, "*Ciphertext-policy attributebased encryption*",IEEE Symposium on Security and PrivacyMay 2007.

[2] Ling Cheung, Calvin Newport,"*Provably Secure Ciphertext Policy ABE",November,2007.*

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-based encryption for fine-grained access control of encrypted data,"* Proceedings ofthe 13th ACM conference on Computer and communications security , October 2006.

[4]Luan Ibraimi, Milan Petkovic, SvetlaNikova, Pieter Hartel, Willem Jonker*," Mediated ciphertext-policy*

attribute-based encryption and its application", 2016.

[5]Shulan Wang, Junwei Zhou , Joseph K. Liu , Jianping Yu, JianyongChen,WeixinXie , " *An Efficient File Hierarchy Attribute- Based Encryption Scheme in Cloud Computing* ",IEEE transactions on cloud computing, vol. 11, no. 6, june2016.

[6].TaoJiang,XiofengChen,JinLiz,Duncan.S.Wong,JiafengMa,JosephK.liu , "*TIMER:Secure and Reliable Cloud Storageagainst Data Re-outsourcing,*2016.

[7] T.H.Yuen,J.K.Liu,M.H.Au,X.Huang,W.Susilo, and J.Zhou,"*ktimes attribute-based anonymous access control for cloud computing*," IEEE Transactions on Computers,September 2015.