J Med Syst (2019) 43: 171
https://doi.org/10.1007/s10916-019-1301-x

TRANSACTIONAL PROCESSING SYSTEMS

Securing Personal Health Record System in Cloud Using User Usage Based Encryption

Dhina Suresh[1] · **M. Lilly Florence**[2]

Received: 17 January 2019 / Accepted: 22 April 2019 / Published online: 7 May 2019

Abstract

Cloud-based Personal Health Record (PHR) in the electronic and information system has become next generation cloud platform for facilitating efficient, secure and scalable data access to foster the collaborative care. Data owner prefers to outsource their confidential electronic data to the cloud for effective retrieval and storage without provoking the depletion or losses due to data management and maintenance. Secure data sharing and searching are vital. Be that as it may, secure search for the outsourced data is a formidable errand, which may easily incur the leakage of sensitive personal information. In this research, we propose a novel diversified access control framework composed of User Usage Based Encryption (UUBE) which is normally based on the searchable encryption scheme. In the UUBE demonstrate, Usage is mapped as credential/accreditation with time allotment to each event, where the event is considered as security trait or a privacy attribute. Data user/client can decipher an event if and only if there is a match between the accreditation and credential related to the event. A searchable encryption enables efficient routing of encrypted events using data or feature extraction algorithm as an important technique. Multicredential routing is modelled as an event dissemination strategy to strengthen weak data user confidentiality. The data user is permitted to maintain the accreditations/credentials as per their usage category. Private keys are assigned to the user/client as labels with the accreditations or credentials. A data owner/proprietor associates and relates each enciphered event with a set of credentials.

Keywords Credentials · Data sharing · Personal health record · Searching · User usage based encryption

Introduction

As the outsourcing of data to the cloud server is developing in a hazardous way, electronic personal and health information has been outsourced to the cloud as it provides greater flexibility and reliable storage services. Besides its availability, there exist numerous challenges against securing the real-time has the highest priority as well as a concern [18]. It can be accomplished with an approach that is methodical, systematic, adoptable and well-structured. Fine-grained access control mechanisms are primarily considered as well framed structured architectures such as Attribute Based Encryption (ABE), Public Key Encryption (PKE) models, Searchable Encryption (SE) and Proxy Re-Encryption (PRE) scheme has envisioned some solution to mitigate the data leakage by intruders and hackers through employment of the data mining solutions in terms of similarity pattern search and record linkage techniques. It consists of an analysis of security components and rationale to protect the data. The noteworthy difficulties and challenges emerge by specified techniques and procedures are revocation/disavowal of the user from the delegation in scalable time and size which rise for solutions of effective and powerful trust computation models.

This article is part of the Topical Collection on *Wearable Computing Techniques for Smart Health*

✉ Dhina Suresh
dhinadulcy@gmail.com

M. Lilly Florence
lilly_swamy@yahoo.co.in

[1] Department of Computer Science, St.Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, India

[2] Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Cloud computing

Cloud computing in the distributed environment is a general term used to describe a class of network based

on computing [16] that takes place over the network, also it is an expression used to describe and portray an assortment of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. A cloud-based EHR is a scalable, flexible, intuitive, cost-effective solution for maintaining patient health files in the cloud rather than on internal servers located at a medical facility or practice. A cloud-based EHR [10] is essentially very similar to a traditional EHR in the sense that functionality and basic features attempt to accomplish the same processes. Both systems enable collecting patient information, maintaining accurate health records, sorting, organizing and compiling data into actionable information and shareable formats, facilitating effective communication with medical providers, third-party payers and patients.

Cloud models

- **Public Cloud:** The public cloud allows systems and services to be easily accessible to the general public. Public cloud may be less secure because of its openness. Public cloud is a fully virtualized environment.
- **Private Cloud:** The private cloud allows systems and services to be accessible within an organization. It is more secure because of its private nature. The private cloud is the one in which cloud infrastructure is set aside for exclusive use by the single organization. It is owned, managed and operated by the organization, third party or combination of both.
- **Community Cloud:** The community cloud allows systems and services to be accessible by a group of organizations. The model type community cloud shares the cloud infrastructure across several organizations to support specific community having common concerns.
- **Hybrid Cloud:** The hybrid cloud is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using the public cloud.

Service models

Cloud computing is based on service models (Anthes, 2010). These are categorized into three basic service models which are discussed below.

- **Infrastructure as a Service:** IaaS (Infrastructure as a Service) is one of the fundamental service models of cloud computing alongside PaaS (Platform as a Service). It provides computing infrastructure like virtual server space, network connections, bandwidth, load balancers and IP addresses.
- **Platform as a Service:** PaaS provides the runtime environment for applications, development and deployment tools, etc. Platform-as-a-Service is referred to as PaaS. This service is hosted in the cloud and accessed by the users via the internet. It includes software support and management services, storage, networking, deploying, testing, collaborating, hosting and maintaining applications.
- **Software as a Service:** Through the internet, this service is available to user's anywhere in the world. Traditionally, software application needed to be purchased upfront and then installed it onto your computer. SaaS users on the other hand, instead of purchasing the software subscribes to it, usually on monthly basis via the internet. s

Electronic health record

Electronic Health Records (EHR) framework [6], will make therapeutic records to be computerized with the capacity to forestall furthermore avoids restorative blunders. EHR framework is accessed through the web. EHR benefits a patient to create, oversee, manage, and regulate her/his personal health information in one place through the web. It will facilitate and also encourage a patient to create his own health information in one hospital and oversee or share the information with others in different hospitals.

A cloud-based public health record (PHR), electronic health record (EHR), or electronic medical record (EMR), is the systematized collection of patient electronically-stored health information in a digital format. These records can be shared across different health care settings.

Fundamental concepts of attribute based encryption

Attribute based Encryption is a sort of public key encryption in which the secret key of a client and the enciphered text are reliant upon attributes. Attribute based Encryption accomplishes fine-grained access control to the outsourced data. A pivotal security aspect of Attribute Based Encryption (ABE) is collusion resistance. Attribute based encryption is classified into the following two categories.

- **Key Policy ABE:** In KP-ABE the secret key of the user is generated with the access policy [13] and the cipher text is generated by the attributes.

- **Ciphertext Policy ABE:** In CP-ABE the secret key of the user is generated with the attributes [2] and the cipher text is generated by the policy.
- **Single-authority ABE:** In Single-authority ABE, each user's keys are generated using different random and secretly shared values such that keys generated for different users cannot be combined, which prevents collusion attacks.
- **Multi Authority ABE:** For decentralizing multi-authority ABE, the private keys of users can be generated by different authorities that do not communicate [3]. The crucial technical challenge for decentralizing multi-authority ABE is constructing a secret sharing value to resist collusion attacks. The Attribute Authorities (AA) supervises the attributes with both secret keys and public keys in the system [4]. It is more expressive, efficient with revocable data access control features.

Existing systems

Secret key cryptography (SKC)

Uses a single key for both encryption and decryption also called symmetric encryption. Primarily used for privacy and confidentiality. Secret key cryptography as methods employ a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography [15] is also called symmetric encryption.

Situation based access control

Situation-Based Access Control (SBAC) model has been analyzed toward securing the health record against various kind of attacks. It is a conceptual model, which defines scenarios where patient's data access is permitted or denied. The main concept underlying this model is the Situation Schema (SS), whichis a pattern consisting of the entities Data-Requestor, Patient, EHR, Access Task, Legal-Authorization, and Response, along with their properties and relations. The various data access scenarios are expressed via Situation Instances. While we focus on the medical domain, the model is generic and can be adapted to other domains [14].

Role based access control (RBAC)

RBAC is to set the access permission to the access data [20] which is governed based on the role that the user holds. RBAC is also known as non-discretionary access control because the user inherits privileges that are tied to his role. The user does not have a control over the role that he will be assigned.

Feature extraction and feature selection

Feature extraction is a most commonly used technique for dimensionality reduction. Feature selection, also known as attribute selection. It involves reducing the amount of resources required to describe a large set of data especially cloud. FE involves in a process to extract a subset of new features from the original set keeping as much information in the data as possible [5]. Conventional Principal Component Analysis (PCA) is one of the most commonly used feature extraction techniques.

Public key encryption with keyword search

According to [1], Public Key Encryption with Keyword Search (PKE-KS) enables and encourages a server to search from a collection of enciphered documents given an enciphered keyword which is provided by the data user. The keyword guessing attack and secure channel permit the server to search for a keyword in the enciphered index structure for enciphered data files.

Efficient verifiable public key encryption with keyword search based on KP-ABE

The public key encryption with keyword search (PKE-KS) technique is analyzed as it empowers clients to search on encrypted data, and hence applicable to the setting of cloud computing. PKE-KS conspire can allow a user to search enciphered data confidentially, though it failed in verifying the searched result as the system did not specify and allocate the users for encrypted data files stored on the cloud server [9].

Securing patient-centric personal health records sharing system in cloud computing

Personal health record (PHR) empowers data proprietor to manage and administer their own electronic medical records (EMR) in a centralized way as it bestows and imparts flexible way to outsource their information to be stored in a third-party server. In this literature review, a secure, taut and scalable system for imparting PHRs is analyzed by focusing on the multiple data owner scenarios, and divide the users in the system into multiple security domains that greatly diminishes the key management complication for proprietors and users [17].

Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption

Personal Health Record (PHR) is considered as 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. To assure the patient's control over access to their own PHR's, it is a promising method to encrypt the PHR's before outsourcing. 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. In this literature, unique patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers are analyzed in depth [8]. To achieve fine-grained and scalable data access control for PHR's, Attribute-Based Encryption (ABE) techniques to encrypt each patient's PHR file is leveraged. Different from previous works in secure data outsourcing, multiple data owner scenarios are focused and divides 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 multiauthority ABE.

Problem definition

Due to the high cost of building and maintaining specialized data centers, numerous Electronic Health Record (EHR) services are outsourced or provided by third-party service providers, this situation may prompt to several privacy and security risks in terms of attacks such as eavesdropping and guessing attacks by a user of the electronic health record. Keeping in mind the end goal to prevent the access control towards the patient record a feasible and promising approach would be to encrypt the data before outsourcing using a public key cryptosystem or through access control constraints and limitations.

- **Data Confidentiality:** It is the ability to hide information from those people unauthorized to view it. Multi-credential routing, is modelled as an event dissemination strategy to strengthen weak data user confidentiality. The data user is permitted to keep up accreditations/credentials as indicated by their usage category. Private keys are allotted to the data user as labels with the credentials. A data owner associates each enciphered event with a set of credentials or rules.
- **Data Integrity:** It is the ability to ensure and verify that data which is outsourced to the cloud is an accurate and unchanged representation of the original information in a multi-user data sharing environment. The encryption is carried out using ECC Algorithm [12] to generate the ciphertext to the preserved attributes.
- **Data Availability:** It ensures that a data is readily accessible to the authorized user upon the user's request has been approved by access control mechanism or access policy defined by the data owner. Data user issues the data request along with the trapdoor for the queried keyword utilizing the private key (accreditation).
- **User Revocation:** In order to fulfill the requirement, we present a model attempting a novel access control mechanism using as User Usage (UU) on the encryption and the searchable encryption to ensure the robust privacy preservation and automatic user revocation based on usage.

Furthermore, our proposed scheme allows the user to access the record without deciphering it perpetually. To best of our insight, it is considered as more and supplemental secure against various threats in the cloud framework. Additionally this bestows reliable and flexible solution for automatic delegation of the user based on time and behaviour in the data sharing. Behaviour analysis is a major novelty in the work.

Proposed model for secured cloud based PHR using user usage based encryption

The proposed model is devised as a novel access control mechanism named as User Usage Based Encryption (UUBE) based on the Searchable Encryption (SE) scheme to ensure the robust privacy preservation. Usage is mapped as a credential with a time frame to each attribute set of the patient health record, an event considered as privacy attribute. Data user can decipher an event which is represented as feature set if and only if there is a match between the credentials related with the feature set. We analyze the cloud based personal Health Record in the Cloud platform which facilitating efficient, Secure and scalable data access to foster the collaborative care. In these model, Data owner outsources their confidential personal health files to clouds server for effective retrieval by healthcare provider and towards storage service which avoids incurring losses due to data management and maintenance in the local systems.

However, healthcare provider requires the medical record for the medical processing as they demand record through search mechanism in the cloud. A secure search model is also designed for the outsourced data as a formidable task, which may easily incur the leakage of sensitive personal information. Efficient data sharing and searching with security is of critical importance. The proposed model is devised as a novel access control mechanism named as User usage based encryption (UUBE) based on the searchable encryption to ensure the robust privacy preservation. Usage is mapped as a credential with the time-frame to each attribute set of the patient health record, an event considered as privacy attribute. The data user can decrypt an event which represented as the feature set only if there is a match between the credentials associated with the feature set.

A searchable encryption [11] enables efficient routing of encrypted events using data or feature extraction algorithm. Multi-credential routing is modelled as an event dissemination strategy to strengthen weak data user confidentiality. The data user is allowed and authorized to maintain credentials according to their usage category. Private keys are allotted to the data clients as labels with the credentials. A data owner associates and imparts each enciphered event with a set of credentials.

The Singular Value Decomposition (SVD) [19] is applied to unused or less used attribute in order to dimensionally reduced feature set or attribute set before the encryption. Additionally, we address the issue of data user confidentiality in the presence of semantic clustering of data user. A weaker notion of data user confidentiality is defined and a secure overlay maintenance protocol is designed to preserve the weak data user confidentiality.

System model

Access control model defined in this section is modelled with three entities of the health record system such as,

Data owner: The data owner to store the data in the cloud, will outsource their personal health record to the third-party database in the cloud data center. The health records are encrypted using encryption model such as attribute based encryption type with multi user setting will be stored in form of ciphertext and finally, it placed in the databases.

Data user: Data user generates a trapdoor to search personal health records using the category of a user as key and institution as key by the data owner. After receiving the request from the data user, data center computes the matching for encrypted keyword search in the personal health record and returns the relevant information as an outcome in the encrypted or decrypted form.

Cloud data center: The cloud data center performs the store, search and delete operations of the outsourced health records after the access construction and policy generation to generate the key pair for data encryption by the trusted third-party application. The usage based encryption is designated for access of the data outsourced to the cloud based data user with specified time after which it has to lead to revocation of the data user. The architecture of UUBE is depicted in Fig. 1.

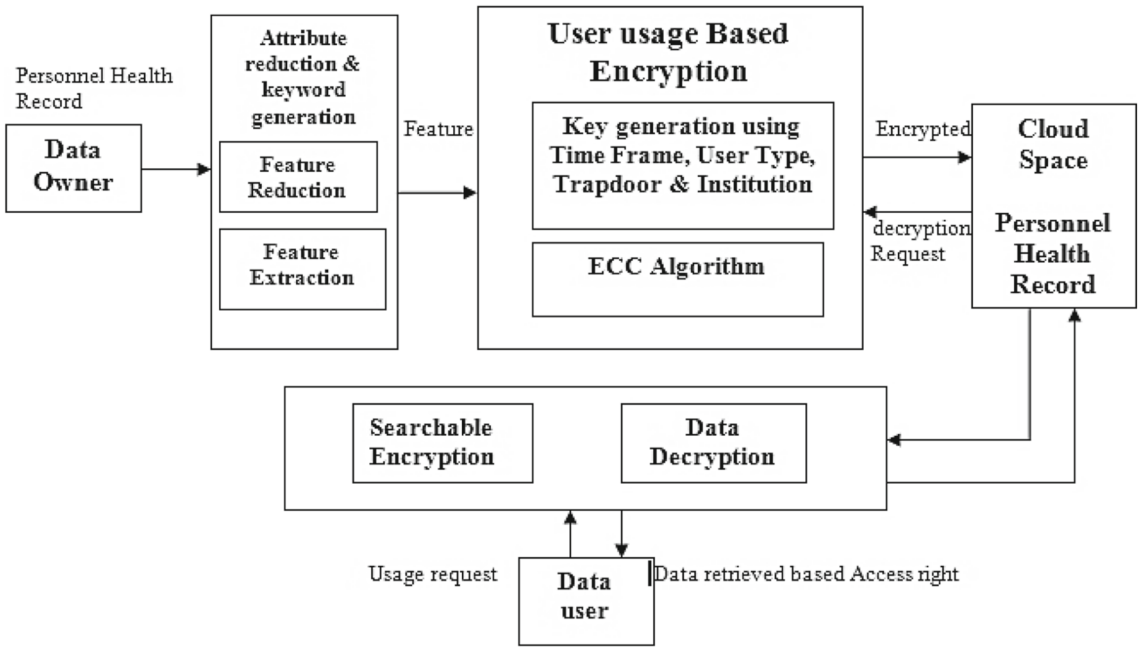

Fig. 1 Architecture of user usage based encryption

In the system, the PHR of the patients are encrypted by an asymmetric encryption algorithm named as Elliptic Curve Cryptography [7]. The algorithm focus on the searchable keyword encryption and the timing controlled data rendering function. The proposed model is resistant to key leakage attacks through the usage of ECC.

In particular, it employs a sophisticated key generation mechanism to blind the decryption key of a user on the access policy specification, so that any third-party can deny compromising the key and cannot effectively recover a valid ciphertext even if the attribute set of the key satisfies the access policy of the ciphertext. Specifically, both the public key and the user secret key are involved in the algorithm. Table 1 provides the notation used in this chapter.

Set up and preliminaries

Setup $(\lambda, S) \rightarrow (P_K, M_K)$: The setup algorithm takes as input the security parameter λ and an attribute universe description S.

It defines a bilinear group G of prime order p with a generator g.

It is used to outputs the public parameters P_K and the master secret key M_K.

The master secret key M_K is kept secret.

Step 1 Attribute Generation:

The algorithm defines the access structure and the attributes with the following constraints as follows.

Table 1 Notations

Notation	Description
$A_1, A_2, ..., A_n$	Events(Attribute Set)
P_k	Public key
M_k	Master key
S_K	Private key
G	Access tree space
S	Universe set of attributes
A_U	User set of attributes
A	Access structure
$R_1, ..., R_n$	Set of health records
$U_1, ..., U_n$	Set of users
$U_n P_n$	User policy
T_s	Time seal
I	Index
T_w	Set of keywords used for creating a trapdoor
T_d	Trapdoor
F_E	Keywords after feature extraction
C_T	Ciphertext

Let $S = \{P_1, P_2, ..., P_n\}$ be an sttribute set.

Say $S = \{Doctor, Neuro, Cardio, Allen, >50, Agent, Relative, Dean, ..., P_n\}$.

A monotone access structure

$$A \subseteq 2^{\{P_1, P_2, ..., P_n\}}, \tag{1}$$

is defined for each user, so that

$$\forall B, C : B \epsilon A, B \subseteq C \rightarrow C \subseteq A. \tag{2}$$

Users $U_1, ..., U_n$ with a set of attributes that are included in the A are authorized users and are allowed access to the data.

Step 2 Group Generation:

G_1, G_2 are bilinear groups of prime order p, g is generator group G_1 and therefore,

$$e : G_1 X G_2 \rightarrow G_2. \tag{3}$$

Step 3 User List Generation:

The user list generation algorithm takes as input P_k and the user identity ID and a time seal T_s. It outputs the user list UL for a data to be accessed normally. If user's attributes and access policies are matched successfully along with the time seal, ciphertext will be decrypted to plain text automatically.

If $(T_s) \leq DelegationTime$, The user is revocated automatically.

If the time seal does not match the user will be revocated automatically. Manual revocation of the user is also possible by the user if he is not satisfied with the behaviour of the user. Each user is given a set of attributes.

$$U_1 \rightarrow (\text{Doctor}, >50, \text{Dean}) + (T_s),$$
$$U_2 \rightarrow (\text{Neuro}, \text{Allen}, \text{Dean}) + (T_s),$$
$$U_3 \rightarrow (\text{Cardio}, \text{Neuro}, \text{Realtive}, >50) + (T_s).$$

Step 4 Policy Generation:

The access methods are generally cryptographically encrypted to provide an access policy. The policy is generated along with the time seal (T_s). Time limits are specified for the attributes for attribute revocation. Revocation can also be done by the user before the time seal.

If the above-mentioned requirements are fulfilled by the newly defined attribute-based encryption. For each

user according to their attributes, policies are generated individually.

$$U_1P_1 \rightarrow ((\text{Doctor AND } >50) \text{ OR Dean}) + (T_s)$$
$$U_1P_2 \rightarrow (\text{Neuro OR Allen OR Dean}) + (T_s)$$
$$U_1P_3 \rightarrow (\text{Cardio AND } >50) \text{ OR } (\text{Neuro AND Relative}) + (T_s)$$

Key generation

In this section the keys are generated for encryption and decryption.

Step 1 ECC Parameters:
Elliptic curve over finite field equation is given by,

$$y^2 = x^3 + ax + \{b\}mod\{p\} \quad (4)$$

Step 2 Key Generation:
With the generator G, time seal T_s and user attribute set $A_U = A_1, ..., A_n$ where $A_U \epsilon S$ as input, the algorithm generates a key pair, a public key P_k known to all and a private key S_k kept secret for the particular user.

$$\{G, T_s, A_U\} \rightarrow (P_k, S_k) \quad (5)$$

Time Seal is used to automatically revoke the user by the data owner. The ASCII values of the attributes are grouped to perform a cryptographic operation on the group to obtain the key pair.

BuildIndex

Let $R_1, ..., R_n$ be a set of health records.

Let $R_1, ..., R_n$ be the input, using the feature extraction and feature selection algorithm set of keywords are generated to form the index.

Step 1 Feature Extraction:
The common words are removed after feature extraction. The features F_E are extracted from each record $R_1, ..., R_n$.

Step 2 Stemming, Stop-words, Weightage:
The Bag of Words (BOW) is calculated by the following equation.

$$(PHR)_{NxM} = \sum_{n-1}^{n} Word_{nton-1}(Text). \quad (6)$$

Where N is the number of unique terms in the record, M is the total number of terms in the record.

The words are selected based on the following equation

$$Select_{n-1 \leq N \leq n} |Word_{nton-1}(Text)|. \quad (7)$$

Weightage for a word is calculated. To check the availability of particular terms in documents based on the Document Frequency. The word fever occurs frequently in documents, so the term frequency is high. The terms that occur in every document collection does not help to distinguish the documents from each word. Hence, term feverish is less valuable. To avoid these types of drawbacks, we calculate term frequency and document frequency using TF/IDF.

It takes the Public Key P_k and the record set $R_1, ..., R_n$ as input. An index I is generated and encrypted with the P_k. Along with the index I, data owner generates a trapdoor for fast retrieval of data.

Hence an Index I is generated by $R_1, ..., R_n \rightarrow afterfeatureextraction \rightarrow I$ and Trapdoor T_d is generated by $R_1, ..., R_n \rightarrow afterfeatureextraction \rightarrow I \rightarrow T_w \rightarrow T_d$.

Encryption

WithT_d, P_k, T_s, A_p, PHR as the input,the file is encrypted the file is stored in the Cloud Server.

ECC algorithm for encryption is

$$C_T = k * G, Message + k * P_k \quad (8)$$

where G is the generator and P_k is the public key and k is a random value.

Decryption

The decryption algorith process is as follows.

Step 1 Search: Using the search function $Search(I, T_d)$ searching is done on the secure Index I with the help of T_d.

The Attributes are mapped and grouping of the attributes is carried out.

Decryption is done when the user enters any keyword.

The private key of the user S_K which contains the Time Seal T_s, Events(Attribute Set) $A_1, A_2, ..., A_n$ are verified.

It checks if the Time Seal $T_s \leq$ the Delegation Time.

If Time Seal $T_s >$ the Delegation Time, the request will be rejected.

If Time Seal $T_s \leq$ the Delegation Time, Check if the Attributes $A_1, A_2, ..., A_n$ in the Key == Access Policy A_p .

The policy, attributes must match with the key of the user.

Step 2 Decryption: If the Attributes $A_1, A_2, ..., A_n$== Access Policy A_p, then the keyword along with the trapdoor T_d is searched over the Encrypted Index I.

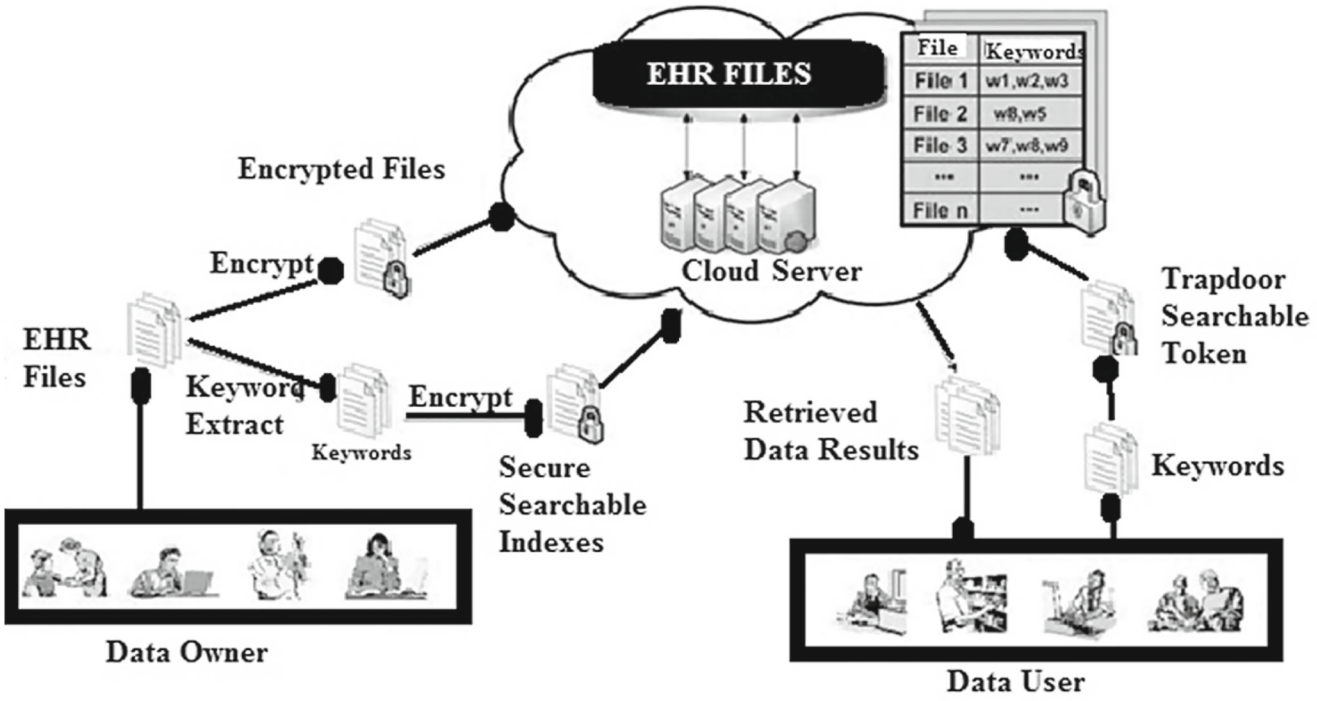

Fig. 2 User usage based encryption process

(I, Td). The overall process of the UUBE is described in Fig. 2.

Results and discussions

To test the robustness and effectiveness of the proposed algorithm different database size has been created with 50, 100, 150 and 200 GB record sizes. The database is created in such a way that it can cover a wide range of difficulty and discrimination degrees. In this part, the experimental results of the proposed framework are obtained with an Intel Core I3 processor with 2620 Processors (2.0 GHz) and 4 GB RAM 400GB transfer and 300 GB storage by creating security framework to prevent unauthorized data access using java programming. The user interface is designed using web programming in Eclipse Environment and MYSQL server is maintained for storing the file and records of the data owner and user information.

Comparision of the performance analysis of the proposed work UUBE WITH MA-ABE

Initially the performance assessment of effectiveness measures to compare Encryption Time ET(MS) in MilliSeconds, Decryption Time DT(MS) in MilliSeconds, Communication Cost (CMCost) in MegaBytes, Memory Utilization (Mem)in MegaBytes and Computation Cost (CPCost) in MilliSeconds for Multi-Authority Attribute Based Encryption and User Usage Based Encryption was analyzed for various data sizes.

Computation time: Analysis of encryption time and decryption time

The computation time for encryption and decryption utilized for securing of the data using public key encryption and through the implementation of the proxy re-encryption

Table 2 Computational cost in milli seconds

No of Users	MA-ABE	UUBE
5	7.53	6.69
10	8.11	7.34
20	10.27	8.19
25	13.79	10.25
30	14.69	10.41
35	15.75	11.16

Table 3 Decryption analysis with maximum number of attributes

No of attributes	UUBE	MA-ABE
5	0.123	0.052
10	0.147	0.056
20	0.15	0.1
50	0.226	0.152
70	0.276	0.2
80	0.3	0.231

Table 4 Performance assessment of effectiveness measures for a database size of 150 GB

Technique	ET(MS)	DT(MS)	CMCost(MB)	Mem(MB)	CPCost(MS)
UUBE	180	160	20	13	360
MA ABE	320	290	26	21	750

scheme for the second level of data delegation along UUBE shows our proposed model is better when compared to MA-ABE. The computational cost describes the duration of waiting state between the users. It is measured in milliseconds. The computational cost values as shown in Table 2 are less compared to existing methodology.

Table 3 compares the decryption time with a various number of attributes for the proposed scheme and MA-ABE.

Efficiency analysis: Memory utilization and communication cost

The users do not have to request an individual record and rely on an intersection calculation to obtain what they need. To the best of our knowledge, there is no existing searchable encryption scheme could provide the search capability without requiring a random oracle. Our scheme has solved this open problem.

Security analysis

Proposed System is an effective approach to prevent the eavesdropping attacks over a cloud environment has it has strongly anonymized. User usage based encryption (UUBE) based on the searchable encryption ensures the robust privacy preservation and automatic user revocation based on usage. Usage is mapped as a credential with a time frame to each event, an event considered as privacy attribute. Multi-Credential routing is modeled as an event dissemination strategy to strengthen weak data user confidentiality.

User revocation

The data user will be terminated from access after the specified time to achieve the data owner defined rule to data access. The server firstly verifies whether the current time is within the delegation time period. If it is outside the delegation period, the request will be rejected. The user is enforced with data access in the attribute selection.

Keyword search

In order to aid the searchable encryption, the data owner creates the collection of keywords using the feature extraction algorithm technique. In order to reduce the

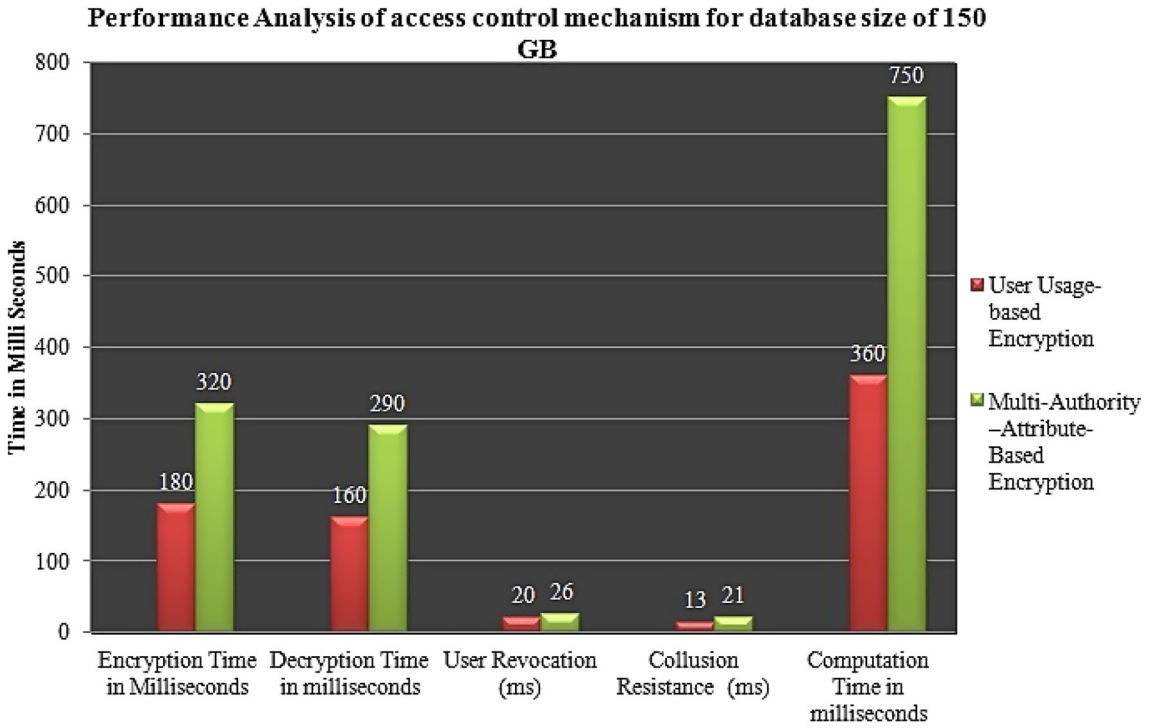

Fig. 3 Performance assessment of effectiveness measures for a database size of 150 GB

communication overhead of the data transmission, the data owner stores a copy of encrypted index tree in the cloud to improve the search efficiency of the system. A user can only write provided the cloud is able to validate its access claim. An invalid user cannot receive attributes. For the sake of simplicity during the analysis, the system assumes that all of the techniques utilize the less memory of the data size. The cipher-text of each attribute to the root of the corresponding attribute. All the cipher-texts of an event are labeled with a unique value such as sequence number of the event. This helps data to identify all the cipher-text of an event. The proposed scheme provides high confidentiality and data integrity against unauthorized user and cloud administrator through the implementation of key generation, key set up and encryption for policy and rules. The security of the system is evaluated against the automatic revocation of the user after time seal. Table 4 and Fig. 3 compares the proposed system with MA-ABE for the data size of 150 GB.

Conclusion and future work

In this work, we designed and implemented the proposed framework utilizing the following mechanism named as user usage based encryption for privacy preserving of the personal health Record. This model addresses the unique challenges in the data center. Key management is greatly reduced also privacy is enhanced to a high extent. When compared with state of art of other approaches our system guarentees high scalability and efficiency. The cloud space has enabled the database to support the categorical data. We utilize this model to allow access to various users from a different category with different professional roles, qualification and affiliations. Revocation of the access is based on the timing is an adds a clinch to our system. Proposed Solution is resistant to various attack explorations in the data center. This model guarantee a high-security level towards data sharing. Our proposed system has proved efficiently strong in case misconduct in the data access and the diverse attacks by the revocation of the user. Additionally, Multi-Credential routing is applied to strengthen the confidentiality of the fragile records. It would be interesting to develop a real-world system where the proposed patient centric data access control schemes in this thesis could be integrated. To reduce the computational complexity, novel cryptographic designs are needed which should make a balance between security and usability. Biometric inclusion can be used for key generation process in the searchable technique.

Acknowledgements I would like to thank THE LORD MY SAVIOR for guiding and showering HIS blessings throughout my life. I take immense pleasure in thanking my guide Dr. M. Lilly Florence for rendering her valuable knowledge and guidance. I would like to thank my husband for his love and support. I would like to thank my parents and my son for their patience and care.

References

1. Baek, J., Safavi-Naini, R., and Susilo, W., Public key encryption with keyword search revisited. In: *Proc. International Conference on Computational Science and Its Applications (ICCSA)*, Vol. 5072, p. 12491259. Springer, 2008.
2. Bethencourt, J., Sahai, A., and Waters, B., Ciphertext-Policy Attribute-Based Encryption. Security and Privacy IEEE Symposium on, IEEE pp. 321–334, 2007.
3. Chase, M., Multi-authority attribute based encryption. In: *Proceedings of the 4th conference on Theory of cryptography*, Berlin, pp. 515–534, 2007.
4. Chase, M., and Chow, S. S., Improving privacy and security in multi-authority attribute-based encryption. In: *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ACM, pp. 121–130, 2009.
5. Fukunaga, K., *Introduction to Statistical Pattern Recognition*. London: Academic Press, 1991.
6. Ghani, M. K., and Wen, L. C., The design of flexible pervasive electronic health record (PEHR), Humanities, Science and Engineering (CHUSER), 249–254, 2011.
7. Karakoyunlu, D., Gurkaynak, F., Sunar, B., and Leblebici, Y., Efficient and side-channel-aware implementations of elliptic curve cryptosystems over prime fields. *IET Inf. Secur.* 4(1):30–43, 2010.
8. Li, M., Yu, S., Zheng, Y., Ren, K., and Lou, W., Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* 24(1):131–143, 2013.
9. Liu, P., Wang, J., Ma, H., and Nie, H., Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE. In: *Ninth International Conference on Broadband and Wireless Computing, Communication and Applications*, IEEE, pp. 584–589, 2014.
10. Lohr, H., Sadeghi, A. R., and Winandy, M., Securing the e-health cloud. In: *Proceedings of the 1st ACM International Health Informatics Symposium*, pp. 220–229, 2010.
11. Lv, Z., Zhang, M., and Feng, D., Multi-user searchable encryption with efficient access control for cloud storage. In: *IEEE 6th International Conference on Cloud Computing Technology and Science*, pp. 366–373. Singapore: IEEE, 2014.
12. Miller, V. S., and Williams, H. C., Use of elliptic curves in cryptography. *Advances in Cryptology - CRYTO '85* 128:417–426, 1985.
13. Pandey, O., Goyal, V., Sahai, A., and Waters, B., Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.
14. Peleg, M., Beimel, D., Dori, D., and Denekamp, Y., Situation-based access control: Privacy management via modeling of patient data access scenarios. *J. Biomed. Inform.* 41(6):1028–1040, 2008.
15. Mehta, P., Bansal, M., and Upadhyaya, A., Stream cipher and block cipher based performance analysis of symmetric

cryptography algorithms: AES and DES In: *International Journal of Modem Trends in Engineering and Research*, vol. 2, no. 7, 2015.
16. Sagar, B., Vhatkar, P. A., and Gajwani, J., Towards Secure and Dependable Storage Services in Cloud Computing. International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163. 57–64, 2014.
17. Smitha, S., Squicciarini, A. C., and Lin, D., Ensuring distributed accountability for data sharing in the cloud. *IEEE Trans. Dependable Secure Comput.* 9(4):556–568, 2012.
18. Tim, M., Kumaraswamy, S., and Latif, S., *Cloud Security and Privacy*, p. 95472. Sebastopol: O'Reilly Media, 2009.
19. Yinlai, J., Hayashi, I., and Wang, S., Knowledge acquisition method based on singular value decomposition for human motion analysis. *IEEE Trans. Knowl. Data Eng.* 26(12):3038–3050, 2014.
20. Tiayni, Z., Weidong, L., and Jiaxing, S., An Efficient role based access control system for cloud computing, In: *11th IEEE International Conference on Computer and Information Technology*, 2011.