International Journal of Engineering & Technology, 7 (4.19) (2018) 309-318

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Efficient Model for Secure and Scalable Health Log Management in Cloud using EH-ABE

R. Dhanapal[1*], P. Visalakshi[2], K.G.Parthiban[3]

[1]Associate Professor, Department of Computer Science and Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamilnadu, India.
[2]Professor, Department of Electronics and Communication Engineering, PSG College of Technology, Coimbatore, Tamilnadu, India.
[3]Principal, Department of Electronics and Communication Engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, Tamilnadu, India.
**Corresponding Author E-mail: [1]dhanapalramasamy.p@gmail.com,*

Abstract

Cloud computing is a significant computing archetype from which the resources of the computing framework are afforded as on-demand services over the Internet. Considering the advancements of cloud, so many applications based on Health Log Management (HLM) are being developed. Though this paradigm is promising, it also bears many challenges on security and access control of data when it is shared over cloud server. Applying cryptographic methods is an effective way in order to make the sensitive data more confidential from unauthorized parties. That is, to ensure better access control to patient's health log shared on cloud, it is vital that the records to be encrypted using an efficient technique before outsourcing. Moreover, while focusing on fine grained access control in shared health log, the main consideration has to be on scalable key management and access flexibility. With those concerns, an efficient model has been proposed in this paper using cryptographically enforced security mechanisms. Enhanced Hierarchical-Attribute Based Encryption (EH-ABE) is the technique used here to encrypt the patient/ data owner's health log and it effectively helps to obtain secure and scalable access control on the shared health log. As a novel try in secure data storage, multi data owner model has been accomplished here. This scenario classifies the owners in HLM into collective security domains that significantly minimize the complication in key management both in owner and user sides. And the experimental analysis portrays that the affirmed work considerably reduces the computation complexity, memory and time utilization, and also enables security, flexibility and scalability on Health Log Management in an effective manner.

Keywords: *Cloud computing, data sharing, Health Log Management, data privacy, EH-ABE.*

1. Introduction

In the current scenario, cloud computing incorporates wide range of new applications and technologies that involves in life routine of every single person. Basically, cloud computing is an inherited paradigm that has been developed from the combination of existing and new techniques like virtualization and SOA (Service Oriented Architectures). In such a way, it provides an archetype in which the resources are shared on the basis of on-demand services over the internet. In addition to this new paradigm, several business models have been developed and those models are noted as 'X' and in cloud format, it is said to be anything as a Service (XaaS) [8]. That 'X' could be anything like a hardware, software, infrastructure and data storage, etc,. Figure 1 portrays the various cloud standards and services that are classified under distribution model and service model. As is well known, the distribution mode of cloud is categorised as public, private, community and hybrid whereas the services include Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) and Anything as a Service (XaaS). Amongst all, the main aim of this paper is about Data Storage as a Service and method to resolve its security issues.

As auspicious as it is, cloud computing also faces so many security issues. When there are some data shared over cloud, there are number of issues such as, accountability, integrity availability of data etc, to be considered [1]. Data security, as it abides in many applications, it has become the greatest challenge that acquires the main concentration from the user who stores sensitive data on to the cloud. Moreover, these concepts initiate from the detail that cloud servers are actually operated by the third party commercial providers which are probably to be away of the trusted domain circle of the data users. Hence, data confidentiality in cloud servers is a frequently required by the data owners. Practically, it is a juristic issue in cloud computing and also it is very complex to provide data confidentiality in an effective way. To that concern, this paper covers the major security aspect, Data Confidentiality among ICA that is Integrity Confidentiality and Availability. As it is shown in figure 2, integrity involves in protecting the data being modified by an unauthorized user, confidentiality deals with preventing the data from unauthorized access and finally availability concentrates on providing the on-demand access to the authorized persons.
The main contribution of this work is managing heath log effectively in cloud. As everything is being digitalized in this current technical world, Health Log Management is also a significant think to be upgraded.

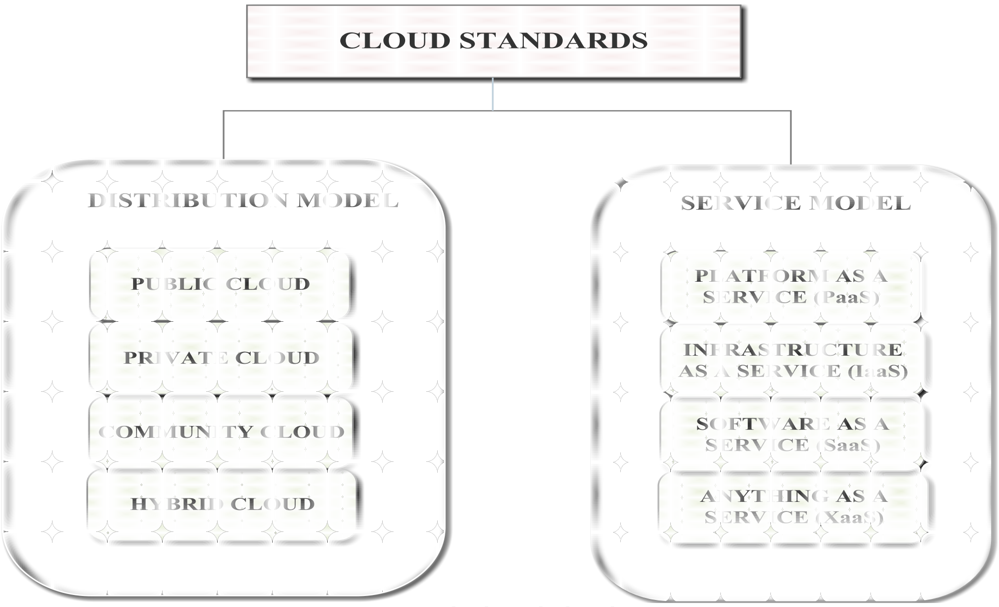
CLOUD STANDARDS
DISTRIBUTION MODEL
PUBLIC CLOUD
PRIVATE CLOUD
COMMUNITY CLOUD
HYBRID CLOUD
SERVICE MODEL
PLATFORM AS A SERVICE (PaaS)
INFRASTRUCTURE AS A SERVICE (IaaS)
SOFTWARE AS A SERVICE (SaaS)
ANYTHING AS A SERVICE (XaaS)

Fig. 1: Various Cloud Standards and Services

In HLM, the patients or the data owners are allowed to create and maintain the particular personal health data through the internet from their own place, which provides an efficient way to store, retrieve and outsource the medical data globally. Specifically, each data owner has the complete rights to control their medical records from the access of health care providers, friends and families.

While thinking about this medical advancement using cloud, there are many risks related to security and privacy on managing the Personal Health Records (PHR) of every individual [15]. The major discussion is about if the patients or the data owners can really control the outsourced personal information, particularly when the log is stored in a third party server which may not be fully trusted by the owner. Since the sensitive values of personal health information are too high, the trusted third party servers are expected to be the targets of several attacks which may lead the outsourced data to be exposed. In order to assure the patient-centric confidentiality on their own health log, it is necessary to have an efficient data access control mechanism.

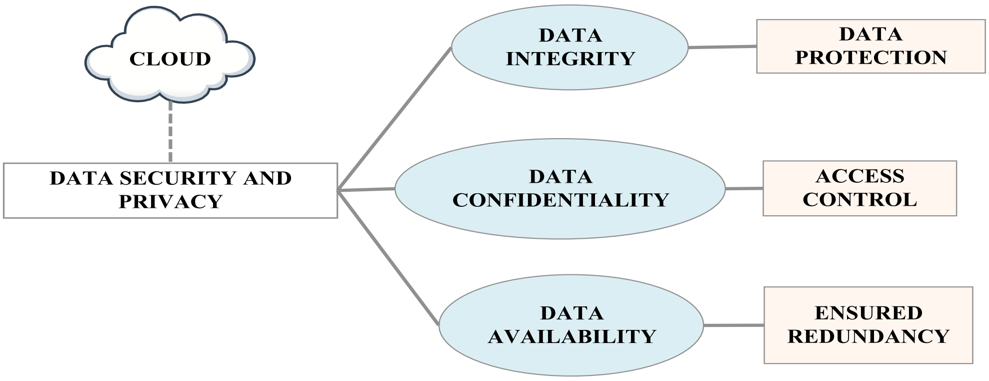

Fig. 2: Various Security Aspects on Data Storage over Cloud

With all these consideration, it is obvious that, encrypting the health data before outsourcing on to the cloud is a feasible way. Generally, the data owner needs to decide the encrypting mechanism and the also the access control method for obtaining the data to be accessed by the right set of people. The stored file should only be avail to certain group of users who are given with the appropriate access, while should remain confidential to the other unauthorized users. Moreover, the patient can also be the deciding authority to deny a particular user from accessing the data when it is necessary. In HLM, the authorized users may refer the stored heath data for two purposes, that is for professional or personal use. For example, let us consider the former can be the data owner’s family members or friends, whereas the latter can be the researchers, doctors or pharmacists. So that, the user side of this health log can be categorized into two: personal and professional domains respectively. As per the aforementioned considerations, the stored data can be accessed by multiple users who may use different set of encryption keys according to the algorithm, when the owner is on offline mode. Hence, these kinds of limitations are also to be considered while developing a secure mechanism for Health Data Management in Cloud.

In this paper, a predominant effort has been made to propose a model for patient-oriented, secure and scalable data sharing of personal health logs on trusted third party servers and also focussed on solving the various complications and challenges in key management. For protecting the health log that is stored in the cloud server, Attribute Based Encryption (ABE) is the main encryption technique adapted here. In ABE, the encryption is made with some set of attributes based on the data or the patient [15]. The complexity during the key generation process for encryption and decryption, it is linear with the taken number of attributes. When it is inherited to a large scale health log management systems, there are so many significant issues are rising based on reliable key management and dynamic access policy modification.

With that note, the proposed work develops a novel method for encryption called Enhanced Hierarchical-Attribute Based Encryption (EH-ABE) technique for patient-oriented secure and scalable data sharing in HLM in cloud servers, with the enforcement of multi owner conditions. In cloud, obviously, cloud service providers are the managers of various cloud services and allot services to the clients based on their requirements. The data owner encrypts the data and stores that on to the cloud, whereas the client downloads it from the CSP and decrypts the data. Explicitly, the shared file may have some hierarchical configuration and here, the encryption process operates based on that configuration by an integrated access structure. It also reduces the execution time and the storage cost of the overall encryption process. The proposed model is as much as efficient to handle different types of health log with reduced key management difficulties in both the owner and the user sides of the system. Dynamic management of access control during emergency cases has also been incorporated through the break glass access to the health log. A thorough examination on the accountability of the work is also provided based on the issues such as multiple parameters in storage, key management, computation and data sharing. The efficacy of this work is demonstrated by executing it in a modern workstation and performing various simulations.

The organization of this paper is as follows: Section 2 provides a deliberation on the related works. Section 3 lays out the detailed construction of the proposed EH-ABE mechanism for effective HLM. The experimental results and comparison charts are given in section 4. Finally, Section 6 concludes the paper with pointers to future work.

2. Related Works

An efficient literature survey work has been made for a clear problem definition on various security and privacy issues of data that is shared over cloud and predominant resolving techniques developed by many researchers. In [5], authors proposed a fuzzy logic based IBE (Identity Based Encryption). That is, encryption has been made with the identity of the user who acted as the data owner in the process. Latterly, this work has been enhanced as Attribute Based Encryption (ABE) and ABE combined with Cipher text Policy (CP-ABE) [11], [12]. In CP-ABE model, the attribute set given by the user defines a user key, while the cipher text is evaluated by encrypting the plain text combined with an access policy.

In [6], authors used the traditional key distribution mechanism for solving the computational overhead on data owner. The paper combines three encryption algorithms for getting appropriate results namely, Attribute Based Encryption (ABE), Proxy re-encryption and lazy re-encryption. It has been claimed that the accountability, that is achieved by the data owner's secret key that tends to the complex processing. The same ABE mechanism is used in another process for securing the health data over cloud [23]. In order to reduce the key management issues between data owner and the user, multi data owner criterion has been incorporated. Following that, the authors of [3] framing a mechanism for resolving the information leakage problem by enforcing indexing methods in cloud. This has been achieved by Specified data binding technique.

In [20], Identity Based Encryption (IBE) provided an optimal cryptographic method to the conventional public key cryptosystems. The main feature of IBE is that public keys are computed from the unique identity information of the registered user on cloud, instead of framing over the network. The three most important IBE based applications are as follows:

- Time released cryptography
- Time instant in the future
- Hierarchical IBE (HIBE), when there exits an organizational hierarchy

In an aspect, Role-based access to the encrypted cloud has been incorporated in cloud for enabling sensible data security [7]. The authors have framed a secure network architecture that comprises a Third Party Auditor (TPA). The major problem was about the dependability of the TPA. Further, the work in [13] had been processed with the novel method namely, bilinear aggregate signature to sustain multiple users at a moment along with the security issues in cloud. But, there is a requirement on the clear definitions on the reliability measures.

It is obvious that when the data is stored in the cloud server for long time, users will have security constraints. There may have some doubt that the information is actually stored in the cloud is still in the server or server, consequent in businesses and the future users are not able to access or restore the data files. For solving this crisis, a secure and proficient storage of proof protocol has been proposed in [10]. But, the overall logging methodology was not effectively described. Merkle Hash Tree (MHT), a novel approach has been developed in [2] for block authentication process that successfully tightens the certification process for secure usage of shared data over cloud. Prof. Asha has narrated a review paper [21] about the various security and privacy issues of cloud computing. Moreover, the paper highlighted the issues on cloud security to be concentrated more. There are several security parameters discussed in that paper such as Client side security, network security, data encryption, data recovery in cloud, access control on data, certification, auditing mechanisms, identity verification and access management. The security issues on SaaS have been discussed in [19]. The work focused on the constraints based on the following criteria:

- Data Security & Network Security
- Data Locality & Data Integrity
- Data Segregation & Data Access
- Authentication & Authorization
- Data Confidentiality
- Vulnerability in Virtualization
- Data Availability and Backup
- Data Breaches and Identity Management

There is another survey works in [16], [28] that help to understand more concepts on cloud in a better way. The complete focus of the paper was on privacy and security problems while storing data on cloud and solving techniques to overcome those issues. In [30], Subashini et al. provided another survey work on various security issues in IaaS, PaaS and SaaS respectively. It has been a great review work that portrayed some security models as well. In [32], clear descriptions about various methods involved in solving the security limitations on cloud were given. Moreover, the authors classified the works of research people under the related criteria which helps to the scholars effectively. Zissis and Lekkas [18] presented a paper work on various security issues on cloud and also described the security requirements to prevail those issues. Several proficient resolving methods have also been demonstrated in the paper for avoiding those security risks on cloud.

In [4], a framework for flexible distributed storage and auditing mechanism has been proposed. The main focus of that framework is about to handle integrity analysis using TPA called Third Party Authentication. Though it resolves problems based on Byzantine failure, colluding attacks and malicious data modification attacks, there is a limitation on reliability of the TPA. HASBE (Hybrid Attribute-set Based Encryption) is another technique enforced in [9]. This encryption process is an improvement of cipher text-policy attribute-set-based encryption (ASBE). It is given in the paper that the scalability can be effectively achieved with this technique. In [24], the authors have discussed about Attribute Based Encryption for maintaining Personal Health Records in Cloud. ABE process has been used to attain a fine-grained data access and storage over cloud. Also, this paper stated that, data confidentiality is guaranteed by the affirmed work. The same method in a distinct way has been given in [27]. The process was named as MAABE (Multi Authority Attribute Based Encryption) and the paper has given some valuable ideas about the advantages and disadvantage of various security related researches done by proficient research scholars. Furthermore, the paper [14] proposed a pairing-based provable multi-copy data possession (PB-PMDP) scheme for integrity verification. It provides confirmation to the data owners that all outsourced data are remaining intact. It permits authorized users to effortlessly access the data stored on to the CSP, and allows public verifiability. In [31], a new framework called Cloud Information Accountability (CIA) framework is developed and effectually concentrated on Data Accountability. The methodology has made the usage of shared data, transparent and traceable to the data owners.

In a distinct way, the method for secure data sharing in cloud based on data manipulation combined with data encryption is given in [25]. The authors have incorporated hybrid encryption and revocable decryption standards for attaining better results. An efficient secure framework has been proposed in [26]. The paper has described accountability and integrity part of issues in could and given a method for solving that. The encryption technique used in this paper could be enhanced with more cryptographic measures. MONA is a new technique developed by Liu et.al, in [16]. The technique uses multi owner data sharing for privacy preserving dynamic broadcast encryption. The overall process describes the ways to deal with multi owners when switching the product to larger applications. In [17], another work called RS-IBE (Revocable-Storage Identity Based Encryption) has been proposed. The authors have mainly concentrated on revoking the unauthorized user from the cloud network. Further, the security goals are framed on the basis of data secrecy, forward and backward confidentiality. But, it is also stated that the concept is little complex during the real time implementation. Maintaining Personal Health Record (PHR) in cloud has become an emerging trend and the work in [22] described that clearly. Using the cryptographic based data access control techniques, the process induced an encryption process called R-MA-ASBE (Revocable Multi Authority Attribute Set Based Encryption). It has given a method for attribute revocation problem in multi authority in data access.

3. Proposed Methodology

As everybody moving towards digitalization in everything, it creates a wide research space in storing and accessing the heath log through cloud in secure way for various reasons. With that note, the proposed methodology defines a model for efficient Health Log Management (HLM) in cloud by exploiting Enhanced Hierarchical-Attribute Based Encryption (EH-ABE) technique. That includes providing efficient key management and data confidentiality to the patients or the data owners to the overall system. It is explicit that the overall encryption process is completely dependent on various attributes on the users involved in HLM.

3.1 Health Log Management (HLM) Model

Based on the valuable survey work, it is noted that the process becomes apparent when the user attributes of the system is categorized into two security domains. Here, the user attributes involved in HLM are categorized into two namely: Private domain and Public domain. Figure 3 deliberates it evidently, there the private domain consist an individual and their attributes, wherein the public domain contains further classifications such as professionals, organizations, pharmacy, insurance sectors etc,. In HLM, the users may be associated with the patient or data owner side and also from the side of public domain comprises some skilled persons such as nurses, doctors, research peoples, etc,.

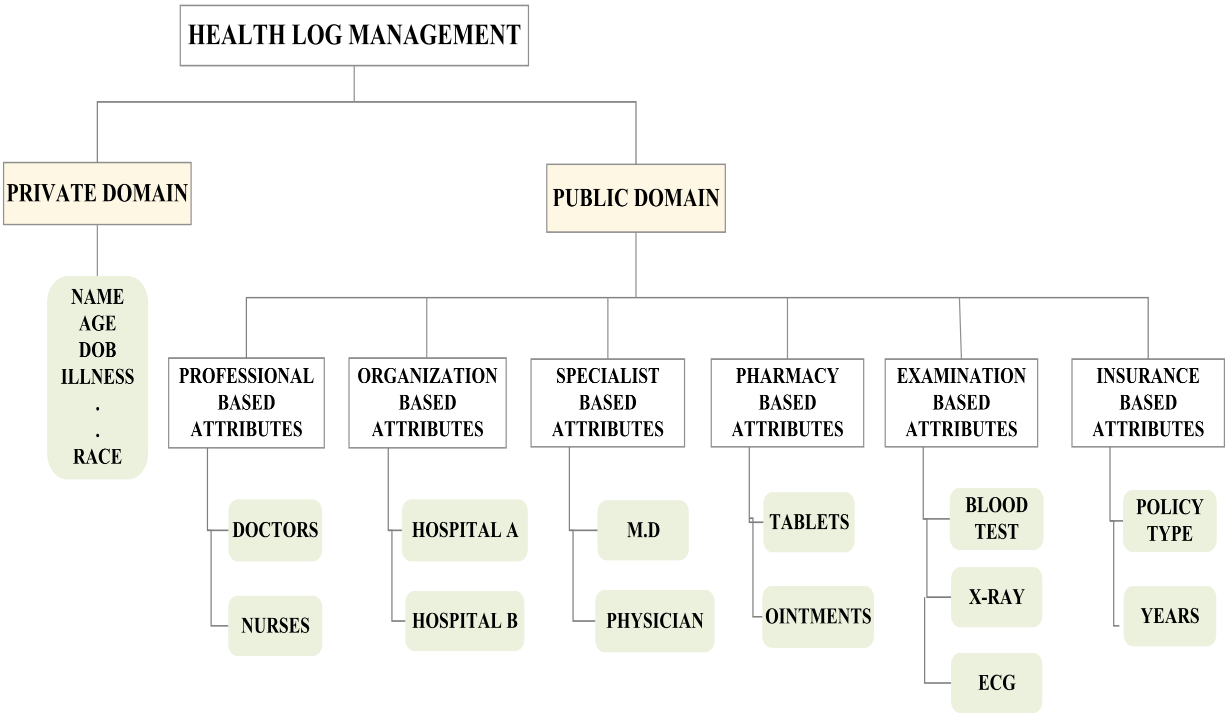

Fig. 3: Categories of user attributes involved in HLM

Particularly, the majority professional users are handled in a distributed manner by the defined attribute authorities in the earlier, though each owner is expected to manage the keys of a less number of users in their own personal domains respectively. In this way, the proposed model also concurrently handles diverse types of health records with reduced key management, manages dynamic policy modifications and dynamic access controls under some emergency conditions.

For achieving fine-grained access control on outsourced data, a unique method to be created with efficient encryption technique that handles both the multi authority access control and hierarchical based access control strategies. Moreover, the ultimate aim is to afford scalable patient centric HLM access and proficient key management at an instant. The affirmed model effectively works on that basis to attain the aforementioned goal. Moreover, the HLM is managed in cloud computing environment based on Multi authority settings.

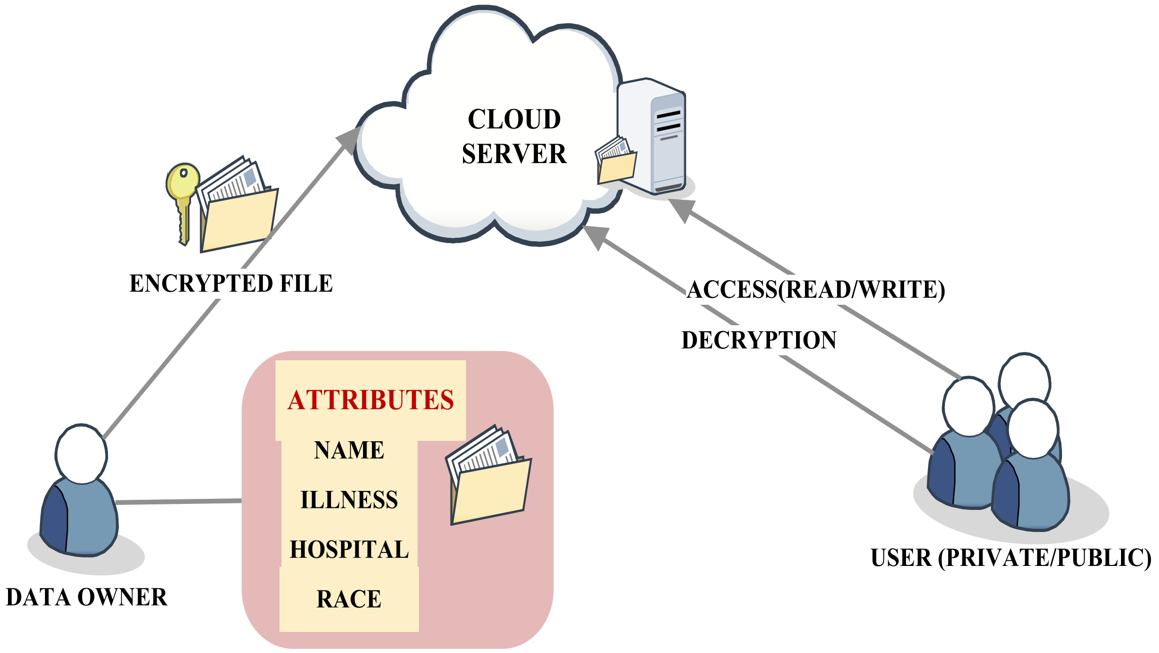

Fig. 4: Simplified Architecture of the Proposed HLM Model

In this system, multi authority based hierarchy ABE is processed for solving the key escrow problem. Each authority attribute of every single user directs a disjoint subset of the respective user attribute, it is not been allowed to control the security of the overall system. The CSP manages the cloud to afford data storage as a service over here, where as the data owners encrypt their health log before uploading on to the cloud by exploiting EH-ABE. The HLM has been processed in cloud and shared with the data user from the public domain of HLM whoever needs it. As illustrated in figure 4, the HLM using cloud comprises five significant tasks namely:

1. Heath log creation based on the attributes of data owner
2. File encryption using EH-ABE process and storing that on to the cloud
3. File decryption at the user side

While the whole process is working on the hierarchical combined access structure, the higher trusted authority is the root authority which is responsible for managing the attributes involved in high levels. On the other side, the lower level authorities are considered to be the owner based single users.

3.2 Hierarchical-Combined Access Structure for HLM

As is given earlier, the shared health logs basically have a hierarchical structure. In detail, a group of logs are categorized into number of hierarchical subgroups considered at different level of access. Moreover, the files in the same level are encrypted by an combined access structure. Moreover, it provides cost, time and storage efficiency for the overall process. Figure 5 portrays a HLM based hierarchical-combined access structure. For sharing the patient data securely on to the cloud, as per the previous explanations, the system divides the log into two parts: personal domain p_1 that contains the attributes such as name of the data owner, illness, age, etc. On the other side, the public domain $p_2$does not comprised with any personal sensitive information, rather contains information about the medical history such as test reports, specialists, treatment protocols, etc. Then, EH-ABE is adopted to encrypt the data of p_1 and p_2 depending on its own access policy requirements. From the sample figure (Figure 5), it is shown that the attending person needs to be a general doctor or specialist who knows about the patient's health record and personal information during the emergency scenario. For an assumption, the patient has the access structure of p_1 as AT_1 {("Hospital X", "Hospital Y") AND "First Aid"}. Similarly, p_2 is termed as AT_2 {("Specialist", "Doctor") AND "First Aid"}. These two access structures $AT_1$and AT_2 are in hierarchical relationship respectively, so that it can be integrated in to AT and that is called as the hierarchical combined access structure.

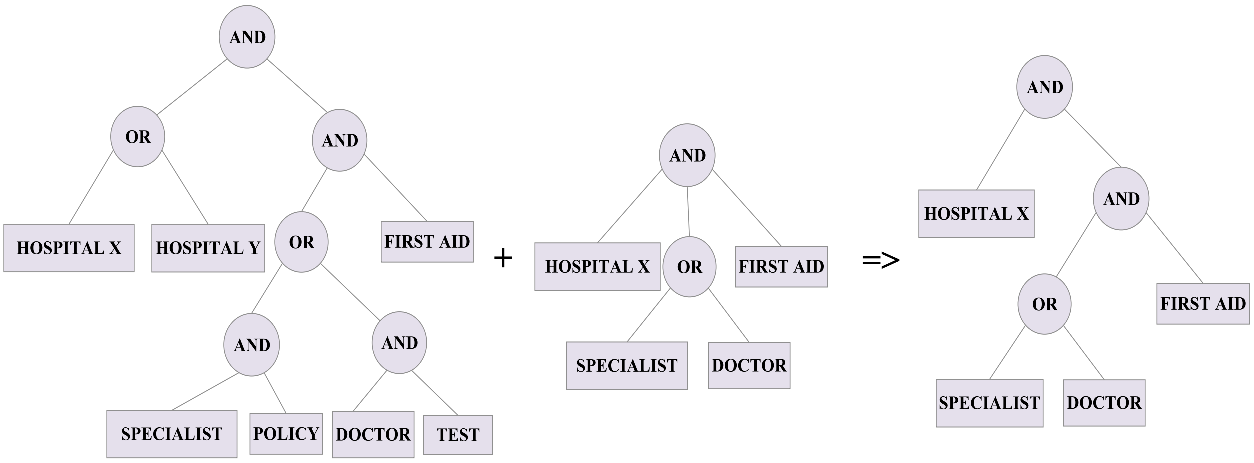

Fig. 5: Sample Hierarchical Based Combined Access Structure for HLM

When the combined access structure is encrypted using the proposed encryption technique, the cipher text will be produced as

$$CPT = \{AT;\ \neg COM; COM; \forall x \in X; COM_{x}, COM'_{x}\} \quad (1)$$

From the equation 1, *X*= {“Hospital X”,”First Aid”, “Doctor”}, the components of the cipher text is given as {AT;} are dependent to the respective policies. In the interim, this combined access structure is shared by two individual files. Hence, the computation complexities of storage overhead and encryption overhead of the cipher text generation can be minimized considerably.

3.3 System Definition

The figure 6 depicts the complete working process of secure Enhanced Hierarchical-Attribute Based Encryption in cloud for a predominant Health Log Management. Moreover, the system level operation of the proposed EH-ABE mechanism evidently describes the overall computation process.

3.3.1. Initial Assumptions

Let *SK* be the security parameter, BG_0 be the bilinear group of prime order *PO* with generator *g*. For any instant and an attribute set. And also two hash functions namely, H_1:$\{0,1\}^* \rightarrow BG_0$ and H_2: $\{0,1\}^* \rightarrow BG_T$, where $BG_T \rightarrow BG_0 \times BG_0$. An universal attribute set is also been defined as λ= { λ_1,.... λ_k}.

3.3.2. Setup

The authority executes the operation with the security parameter *SK* and the randomly selected prime numbers α and β i.e α and β primenum. It produces the public key *PK* and the master secret key *MSK* from the following equations 2 and 3.

Pubic Key $PK = \{BG_0, bg, h = bg^{\beta}, e(bg, bg)^{\alpha}\}$ (2)

Master Secret Key $MSK = \{bg^{\alpha}, \beta\}$ (3)

3.3.3. Key Generation (PK, MSK, SK)

The proposed model operates the algorithm with a set of attributes as and generates a secret key *SK*, the set is framed by the following equation 4.

$$SK = \begin{cases} B = bg^{\alpha}, h^{r}, \\ \forall_{i} \in SK: B_j = bg^{r}.H_1(i)^{r_j}, B_i^1 = h^{r_i} \end{cases} \quad (4)$$

Where ‘r’ and ‘r_j’ belongs to the prime number set *primenum* i.e. are arbitrarily chosen for each user and attribute i.e. j.

3.3.4. Encryption

Consider that the data owner shares ‘n’ number of files with the cloud, therefore ‘M’ is the health log that carries M={m_1,m_2,...,m_n} with ‘n’ access levels. Then, the dependent content keys conk= {$conk_1$,$conk_2$,....$conk_n$}will be encrypted with the following operation.

The encryption process takes the public key PK, content keys conk= {$conk_1$, conk2 ...conkn} and the hierarchical combined access tree AT as inputs. The process gives the output as the cipher text for the hierarchical combined access and it is termed as CPT, as per the previous discussions (Section 3.2).

At initial level, the data owner fixes the level nodes as (x_i,y_j) for (i=1,2,..., n) for each AT and also selects ‘n’ number of random numbers as s_1,...s_n which is in *primenum* and ‘e(bg,bg)’ be the bilinear map. From these assumption, $C1_i$ and $C2_i$ for all i= 1 to n as in the formula 5.

$$C1_i = conk_i\ e(bg, bg)^{\alpha s_i}, C2_i = bg^{s_i} \quad (5)$$

Starting from the parent node PR, the data owner initializes QR=0=s_1. For each non-parent node (*x; y*), it sets QR(*x;y*)(0) = QR(x_i;y_i)(0) = $s_i$if the (*x; y*) is a level node, or else,QR(*x;y*)(0) = QR*parent*(*x;y*)(*index*(*x; y*)). Let X be the set of leaf nodes in AT and Y be the set of transport nodes, then the data owner evaluates and from the following equations 6 and 7.

$$C_{(x,y)} = h^{Q(x,y)(0)} \quad (6)$$

$$C1_{(x,y)} = H_1(attribute(x, y))^{Q(x,y)(0)} \quad (7)$$

Further, the data owner computes for every node (x,y) in the set of Y for all files 1 to n from the formula in 8.

$$C_{(x,y),j} = \begin{cases} e(hg,hg)^{\alpha.(Q(x,y)(o) + Q_{child_j}(o))} \\ .H_2\left(e(bg,bg)^{\alpha Q(x,y)(0)}\right) \end{cases} \quad (8)$$

Finally, the data owner computes the cipher text for the combined access structure by the equation 9 as follows.

$$CPT = \{AT, C1_i, C2_i, C_{(x,y)}, C_{(x,y),i}\} \quad (9)$$

3.3.5. Decryption

The decryption process takes place at the user side and it needs the public key *PK*, secret key *SK* as mentioned by the set of attributes S and probably the CPT. Initially, a recursive kind of operation should be clearly defined for *Decryptlog(CPT,SK,(x,y))*. Let *i=(x,y)*, when (x,y) is a leaf node, then the decryption process executes on the basis of the equation 10.

$$Decryptlog(CPT, SK, (x, y)) = \frac{e(D_i, C1_{(x,y)})}{e(D_i', C2_{(x,y)})} = e(bg, bg)^{r\beta Q(x,y)(0)} \quad (10)$$

In another case, if (x,y) is any non-leaf node, then *Decryptlog(CPT,SK,(x,y))* is computed as *Decryptlog(CPT,SK,v)* for all nodes *v*, that is considered as the children nodes of (x,y) and the output is taken as F_v. With the assumptions, $AS_{(x,y)}$ be the arbitrary notion for ‘n’ sized child nodes set *v* and also $F_v \neq$NULL. Therefore, $F_{(x,y)}$ is computed from the following equation 11.

$$F_{(x,y)} = \prod_{v \in AS_{(x,y)}} F_v^{\Delta_{i},AS'_{(x,y)}(0)} = \prod_{v \in AS_{(x,y)}} \left(e(bg, bg)^{r.\beta Q_v(0)}\right)^{\Delta_{i},AS'_{(x,y)}(0)} \quad (11)$$

With these computations, the decryption process initiates. When the set of attributes AS, satisfies AT then, is computed by the recursive process from the equation 12.

Therefore $G_i = e(bg, bg)^{r\beta.Q_{AS_i}} (i \in [1, n])$ (12)

Following this can be evaluated from 13.

$$F_i = \frac{e(C2_i, D)}{G_i} = e(bg.bg)^{\alpha.AS_i}\,(i \in [1,n]) \tag{13}$$

Then, the respective content keys conk= {conk$_1$, conk2 ...conkn} are computed by the equation 14 in repeated manner.

$$\frac{C1_i}{F_i} = \frac{conk_1 e(bg.bg)^{\alpha.AS_i}}{e(bg.bg)^{\alpha.AS_i}} = conk_1(i \in [1,n]) \tag{14}$$

Finally, the health log M= {m1,m2,...,m$_n$ }is decrypted with conk= {conk$_1$,conk$_2$,....conk$_n$} effectively by the symmetric decryption process. The secure HLM incorporates EH-ABE mechanism to strengthen the overall privacy and confidentiality of health log that is outsourced on to the cloud and it is attained evidently through the aforementioned computations.

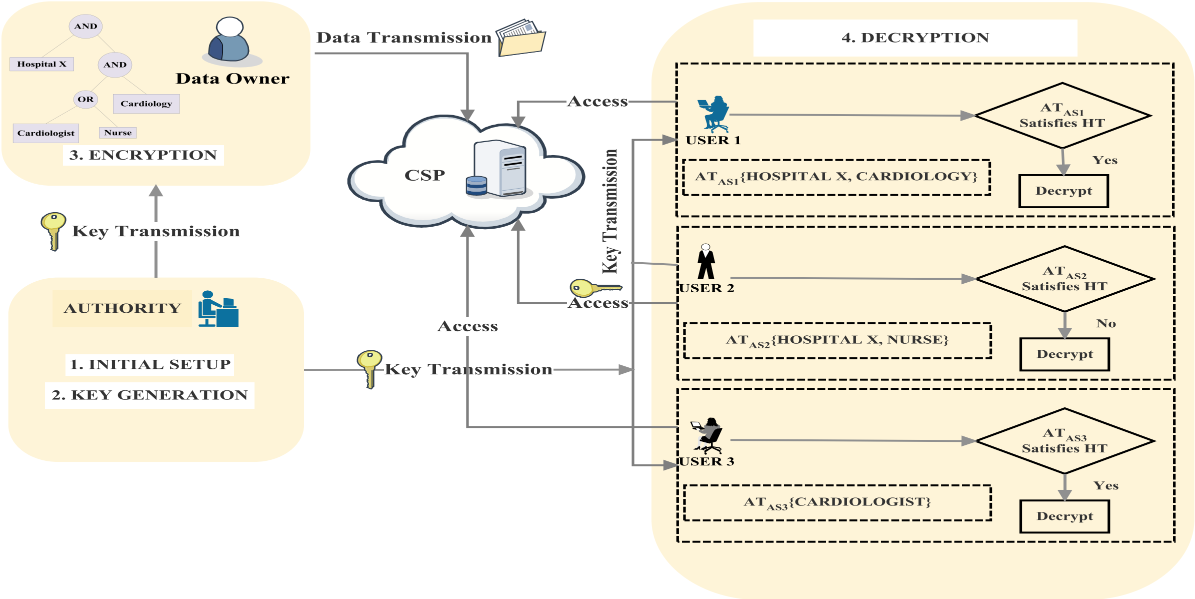

Fig. 6: Secure EH-ABE used in Cloud for HLM

4. Experimental Results and Discussions

In the experimental analysis, the proposed model for secure Health Log Management has been analyzed with respect to the factors such as time consumption, memory utilization, accountability and the computational overhead. Additionally, the results have been

compared with the previous methods such as CP-ABE and HIBE. As in basic way, comparisons are done for memory and time consumption for health log creation, execution, encryption and decryption respectively. With respect to time, the overhead occurs at the encryption of a health log and also at the incorporation of the logs. When storage overhead is concerned, the adduced method is very trivial, in that the only data to be shared are given by the actual files and the combined logs. The result shown in Figure 7 depicts that the time to create a log file increases proportionally with the size of the log file. For verifying whether the process is with bottleneck, the time required to create log files has been computed. Figure 8 shows the comparison chart on key generation time with respect to the number of attributes in each key.

The chart portrays that the proposed model accumulates lesser time than the existing process such as HIBE and CP-ABE. The next figure 9 depicts the comparative analysis made on storage overhead with respect to the memory utilized to store the log on CSP and the size of files in KB. It is obvious from the analysis that the proposed efficient model occupies lesser space that the existing CP-ABE and HIBE models.

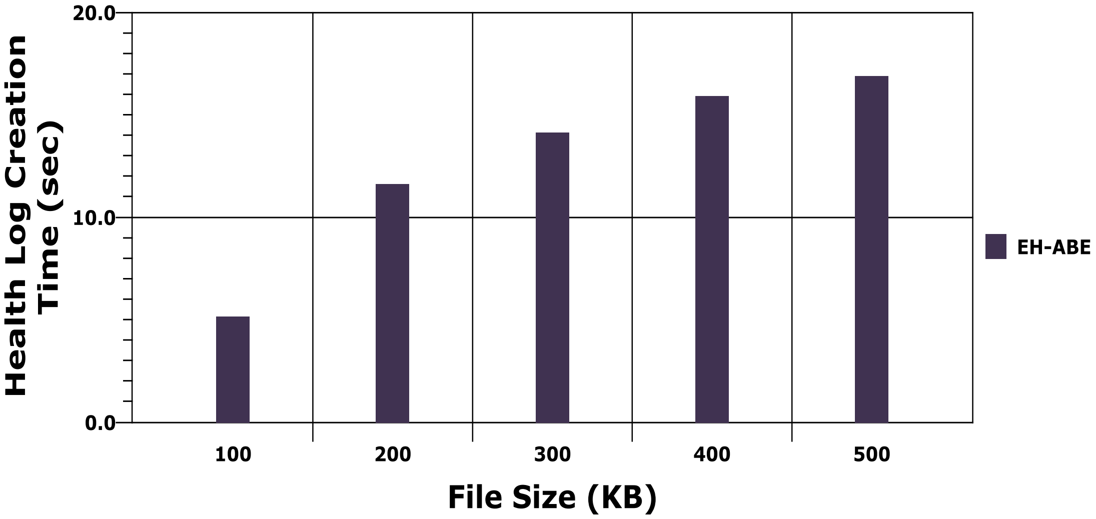

Fig. 7: Time Taken for Health Log Creation

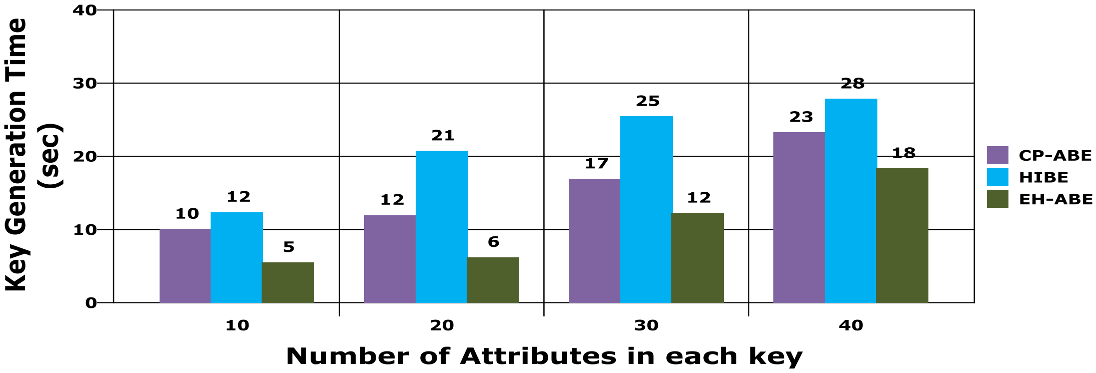

Fig. 8: Key Generation vs. Number of keys

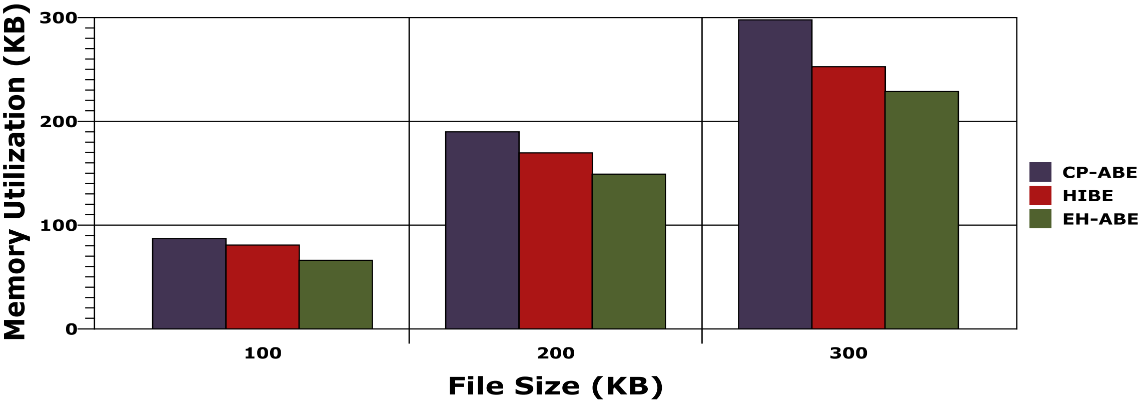

Fig. 9: Comparative Analysis on Storage Overhead

Because of the effective computation techniques in EH-ABE, the time taken for encryption and decryption has been considerably reduced. It is compared with the aforementioned existing methods and the results are given in the following figure 10. The results are given by separately analysing the computation process of encryption and decryption of EH-ABE.

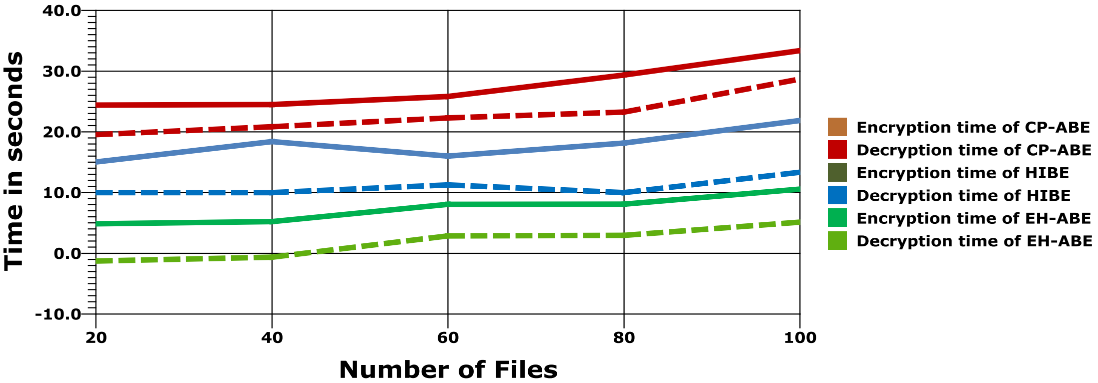

Fig. 10: Time Analysis for Encryption/ Decryption Process

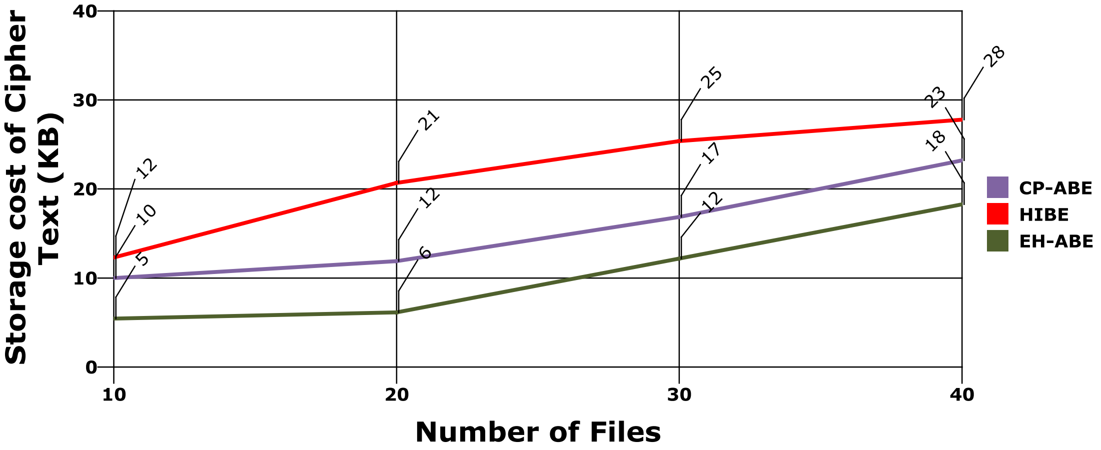

Fig. 11: Number of Files Vs Storage cost of Cipher Text

While considering about the memory utilization on cloud, it is vital to analyze about the storage cost for cipher text over the number of files to be outsourced on cloud. In figure 11, the results of the evaluation have been depicted with the comparison. It is more obvious from the figure that the storage cost is considerably reduced in the current work in this paper.

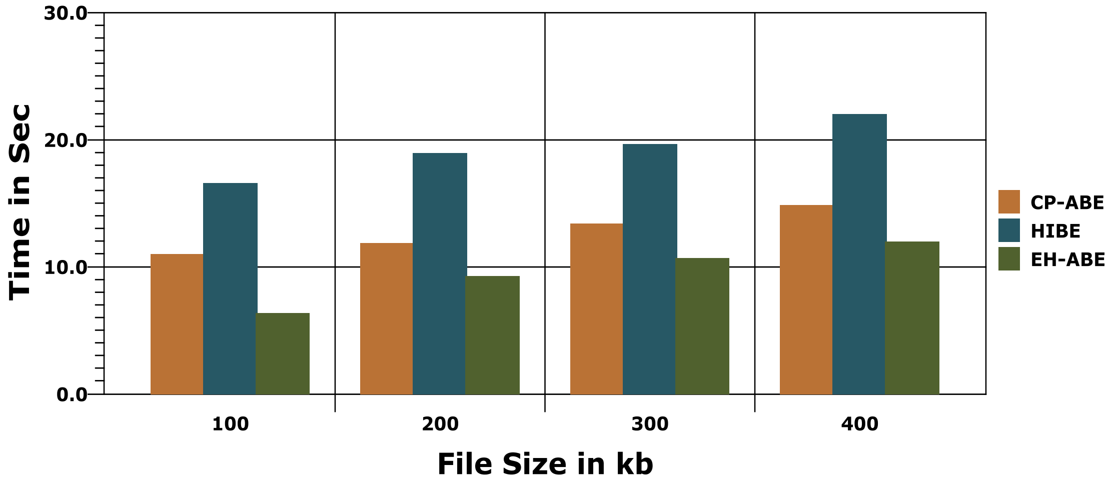

Fig. 12: Analysis on Overall Computation Time

Finally, it is significant to evaluate the overall processing of secure data storage for maintaining scalable HLM in cloud, by incorporating HE-ABE. In order to prove the effectiveness of the current work, it is compared with CP-ABE and HIBE. And, from the figure 12, it is evident that the proposed mechanism uses minimal time than the methods compared.

5. Conclusions and Future Work

This paper aims on achieving proficient data access control along with data confidentiality and data privacy while storing the data in cloud computing environment. As an application oriented process, the work evidently describes a mechanism for efficient Health Log Management (HLM) in cloud. In the proposed model, the attributes of the data files are framed as hierarchical files and then, the files formed a combined access structure. By exploiting Enhanced Hierarchical- Attribute based Encryption (EH-ABE), the cipher texts are framed with the combined access structure. Hence, memory and time cost efficiency of the encryption process has been achieved. Moreover, there is an advantage in the proposed mechanism that all outsourced can be decrypted by the users by evaluating the secret key for single time. Therefore, the execution time for decryption has also been effectively reduced when the user needs to decrypt several files at one instant. Thus, it is stated that the process enforces secure HLM on cloud. The previous section shows the performance of the affirmed work effectively. For further enhancements, hybrid cryptographic techniques could be used for key generation process and some other security attacks can be concentrated more and can also create a way to use various functionalities of cryptography for resolving those problems on cloud.

References

[1] Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin, “Ensuring Distributed Accountability for Data Sharing in the Cloud”, IEEE Transactions on Dependable and Secure Computing, VOL. 9, NO. 4, JULY/AUGUST 2012, pp. 556-562.

[2] Qian Wang, Cong Wang, Kui Ren and Wenjing Lou, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” In the Proceedings of IEEE Transactions on Parallel and Distributed Systems, May 2011, Volume: 22, Issue: 5, pp. 847-859.

[3] Squicciarini, A, Sundareswaran. S and Dan Lin, “Preventing Information Leakage from Indexing in the Cloud” In the Proceedings of 2010 IEEE Transactions on Distributed Computing, July, 2010, pp. 188 - 195.

[4] Cong Wang, Qian Wang, Kui Ren, “Towards secure and dependable storage services in cloud computing,” IEEE Transactions on services computing, 2012, Volume: 2, Issue: 2.

[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” Advances in Cryptology EUROCRYPT, May 2005, pp. 457–473.

[6] Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou, “Achieving Secure and scalable, Fine-grained Data Access Control in Cloud Computing,” In the Proceedings of IEEE Conference- INFOCOM, March 2010, pp. 1-9.

[7] Cong Wang and Kui Ren, Jin Li, Wenjing Lou, “Toward publicly auditable secure cloud data storage services,” IEEE Transactions on Secure Computing, July /Aug-2010 ISBN:0890-8044/10.

[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[9] Zhigou Wan, Jun'e Liu, Deng, R.H.,“HASBE: A Hierarchical Attribute based Solution for flexible and Scalable access control in cloud computing,” IEEE transactions On Information and Forensics and Security, April-2012, Volume: 7, Issue: 2,pp. 743 – 754.

[10] Narn-Yih Lee and Yun-Kuan Chang , “Hybrid Provable Data Possession at Untrusted Stores in Cloud Computing,” In the Proceedings of IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS), December, 2011, pp. 638 - 645.

[11] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute Based Encryption,” IEEE Symposium on Security and Privacy, May 2007, pp. 321- 334.

[12] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” Proceedings of the 14th ACM conference on Computer and communication security, pp. 456–465, October 2007.

[13] Cong Wang, Qian Wang, Kui Ren nad Wenjing Lou, “Privacy-preserving Public Auditing for Data Storage Security in Cloud computing,” IEEE Transactions on Parallel and Distributed Systems, San Diego, March 2010. ISBN: 1063-6692.

[14] Ayad F. Barsoum and M. Anwar Hasan, “Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers,” In the Proceedings of 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID 2012), pp. 829-834.

[15] Dr. Ragesh G. K. , Dr. K. Baskaranb, “Cryptographically Enforced Data Access Control in Personal Health Record Systems”, in the proceedings of Science Direct- Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016), Procedia Technology 25 (2016), pp. 473 – 480.

[16] Selvamani K, Jayanthi S, “A Review on Cloud Data Security and Its Mitigation Techniques”, Science Direct-Elsevier, International Conference on Intelligent Computing, Communication &

Convergence (ICCC-2015), Procedia Computer Science, Vol. 48, 2015 pp. 347 – 352.

[17] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption, " IEEE transaction on cloud computing, Journal Of Latex Class Files, VOL. 14, NO. 8, August 2015, pp 1-13.

[18] Dimitrios Zissis, Dimitrios Lekkas, " Addressing cloud computing security issues" science direct-Elsevier, Future Generation Computer Systems, Vol. 28, 2012, pp. 583–592.

[19] S. Subashini n, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, 2011, pp. 1–11.

[20] Kihidis, A. , Chalkias, K. and Stephanides, G. , "Practical Implementation of Identity Based Encryption for Secure E-mail Communication," In the Proceedings of 14th Panhellenic Conference on Informatics (PCI), September, 2010, pp. 101 – 106.

[21] Prof. Asha Mathew, "Security and privacy Issues of Cloud Computing: Solutions and Secure Framework," International Journal of Multidisciplinary Research, April, 2012, Volume: 2, Issue: 4, pp. 182-193.

[22] Soumya Parvatikar, Puja Prakash, Richa Prakash, Pragati Dhawale, S.B. Jadhav," Secure Sharing Of Personal Health Records Using Multi Authority Attribute Based Encryption in Cloud Computing ", International Journal of Technical Research and Applications, Volume 1, Issue 5 (Nov-Dec 2013), pp. 50-52.

[23] Ming Li, Shucheng Yu,Yao Zheng, Kui Ren, Wenjing Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013, Pp. 131-143.

[24] Mr.Prasad P S, Dr. G F Ali Ahammed, "Attribute-Based Encryption for Scalable andSecure Sharing of Personal Health Records in Cloud Computing," (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, pp.5038-5040.

[25] Aakanksha Maliye1, Sarita Patil, "Scalable and Secure Sharing in Cloud Computing Using Data Manipulation & Encryption", International Journal of Science and Research (IJSR), Volume 4 Issue 7, July 2015, pp. 1877-1881.

[26] K.Senthil K.Prasanthi, "An Efficient Framework for Enhancing Security in the Cloud Environment" International Journal of Engineering Science and Technology, Vol. 5 No. 06S Jun 2013, pp. 76-80.

[27] Shaik Shahina, Guntapalli Minni And Sayeed Yasin, "Sharing Personal Health Records In Cloud With Scalable And Secure Using ABE," International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Volume 23, Issue 8 – NOVEMBER 2016, pp. 61-65.

[28] Selvamani K, Jayanthi S, "A Review On Cloud Data Security And Its Mitigation Techniques," Science Direct-International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015), Procedia Computer Science, Vol. 48, 2015, pp. 347 – 352.

[29] Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, June 2013 Pp.1182-1191.

[30] S. Subashini, V.Kavitha,"A survey on security issues in service delivery models of cloud computing" Journal of Network and Computer Applications, Vol- 34,2011, pp. 1–11.

[31] SmithaSundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data sharing in the Cloud," IEEE Transactions of Dependable and Secure Computing, August 2012, Volume: 8, Issue: 4, pp. 556- 568.

[32] Prof.Y.B.Gurav and Manjiri deshmukh, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pp. 617-625.