Dynamic Access Control Scheme for Personal Health Record in Cloud Computing

E.V.N. Jyothi, V. Purna Chandra Rao

Abstract: ***Presently, usage of Cloud computing is increasing, due to internet availability most of Personal Health Record (PHR) owners outsourcing their records to the cloud, but it is untrusted, so a security mechanism needed in this paper proposing Dynamic Time-based encryption (DTBE), it derived from classic ABE. In the past, many researchers suggested different access controls for secure PHR. Still, most of the access control mechanisms introduce burden to the PHR owner while performing dynamic operations insertion, PHR user revocation, and when it updates, PHR users attribute list. Most of the ABE schemes have several limitations as it cannot efficiently handle adding or revoking users or identity attributes. It needs to keep multiple encrypted copies of the same key that incurs high computational costs. So, there is a need for a suitable access control mechanism that should support effective policies.***

Keywords: ABE, DTBE, PHR, Cloud Computing.

I. INTRODUCTION

Cloud Computing has become an integral part of our day to day life. We can see the applications of cloud used everywhere, either it could be web applications or mobile applications, IOT Applications or Data-based applications, the cloud has become a common term in the IT Industry.

Even a layman is also using the cloud with or without the knowledge of cloud. According to a report presented by Statista portal, the number of cloud-based consumers has increased from 2.4 billion in 2013 to 3.6 billion in the year 2018. The world’s total population is 7.6 billion people, and if

you see the previous statistics from Statista portal, half of the world’s population is directly or indirectly accessing/consuming the Cloud Services. When

such a vast number of people use cloud services by storing and accessing data, you can imagine the kind of problems like Storages, Processing Speed, Security, Privacy, etc..,. Somehow, Cloud Service providers have tackled the issues mentioned above, but Security remains the most crucial concern which makes the developers or IT professionals think twice before making use of the cloud services and due to the popularity and availability of cloud computing

now many organizations outsource their data to the remote server to prevent economic burden and share globally, cloud service providers are currently unreliable because of the many privacy challenges.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author

E.V.N. Jyothi*, Ph.D. Scholar, Department of Computer Science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University. E-mail: jyothiendluri@gmail.com

Dr.V. Purna Chandra Rao*, Professor, Department of Computer Science and Engineering, SVIT, Hyderabad, India.

Cloud as the computing or processing of remote resources or services and these services are IaaS, PaaS, SaaS and so on. Cloud can deploy in four ways, such as private, public, hybrid and community cloud. Every user connects to the Internet and uses the IT infrastructure to meet their daily needs as the demand for the Internet increases. Even service delivered as software, platform, database, storage services, etc. cloud offers "Pay as you go" to the user, maximum benefits can achieve by using these services at a lower cost.

Security issues in cloud computing

In Addition to Benefits for using cloud computing software and support, there are a few safety problems in computing. They comprise:

1. Lock-in: It's The issue of portability and Inter-operability. Lock-in difficulty could be to get vendors and data.

Data Lock-in: Information Saved at one cloud website cannot readily remove if an individual wants to alter a cloud supplier. It could attribute to the absence of standardized API. This leads to an issue of information lock-in. Cloud supplier gives services concerning APIs. API created for a single supplier of cloud might not be helpful for another supplier’s cloud. In case a change of supplier is necessary, then APIs also must be altered, resulting in partial re-development of this program. This matter termed as seller lock-in.

2. Service Availability: To get cloud client, service ought to be accessible at all times. Every time a user asks for cloud assistance, the supplier and consumer need to register SLA (Service Level Agreement). This defines the stipulations and specifications for cloud hosting support. Additionally, it has a percentage of time support is available. A cloud user anticipates a top available service with minimal or no downtime. A cloud supplier and its corresponding provider is chosen based on service accessibility and company requirements.

3. Bottleneck: Data transport bottleneck and support disruption are a few of the problems caused because of bandwidth restriction.

4. Information privacy: For a Variety of businesses, concerns about safety, privacy, compliance, and control over their information are challenges in moving towards embracing a cloud model.

Security in cloud environment

In cloud computing Paradigm, a cloud hosting supplier creates, deploys, and manages the tools, services, applications based on the supplier being IaaS, SaaS, or even PaaS. Multi-tenancy and virtualization are the crucial characteristics to produce efficient use of existing tools and software. A single host, computing center, information center and functioning system hosts lots of consumers by using virtualization. A high number of customers are becoming served by a cloud supplier at this idea of sharing.

Information security, communication, resource management for solitude, and virtualization are a few of the security problems arising because of multi-tenancy and virtualization from the cloud atmosphere. Essential Kinds of security threats from the context of cloud program are recorded in figure 1.1 and briefly explained below

1. Data User information is processed and stored in a shared environment that is under supplier’s controller. Deficiency of transparency concerning the data storage place in the cloud environment, regulatory dilemma because of cross border storage, etc., makes the necessity of information privacy and security in cloud surroundings much more notable. Thus data security problems, including information confidentiality, integrity and accessibility, are crucial security problems in computing.

2. Application Safety: Application software working on or designed for cloud computing systems presents distinct security challenges. An application that's running from the distant should be from real provider and with no malware. Flexibility, openness and public access to cloud infrastructure are risks for program security. Maintaining the integrity of software implemented from remote machines can also be among those concerns.

3. Network Safety: A cloud computing system could be of type private or public, depending on the installation model. Service and software obtained from remote places in a cloud atmosphere. Constant access to cloud support with no disturbance because of network security issues like a refusal of service, and other strikes are significant security challenges.

4. Virtualization Safety: Virtualization technology introduces potential of fresh attacks throughout the hypervisor and other management elements. There are not any reliable ways to evaluate safety of Virtual servers and software. VMs made and revert as and if needed from the cloud atmosphere. Since VMs can quickly be returned to previous cases, and readily transferred between physical servers, so it isn't simple to accomplish and maintain consistent safety. Therefore, virtualization safety is a concern while utilizing cloud tools.

5. Identity Cloud solutions to get it. Every user uses his individuality to obtain a cloud service. Unauthorized access to cloud tools and software is a significant issue. Cloud support. Many such malicious entities get the cloud tools leading into the un-availability of an agency for a valid user. Also, This may be in terms of access to secure place in memory or doing any surgery which not kept in Access Control List for a particular source and application. Therefore, Identity Management method for supplying authentication and Authorization is a problem for both suppliers in addition to a consumer in a cloud computing environment.

Access Control Mechanism

It's a step of assessing whether information is in the right hands. The information which is put host by the data operator shared with several information sharers. Each info sharer has different controls over information. The information can't supplied to the information sharer with no authentication and control data. Traditional access control steps assume that the proprietor in precisely the same place, therefore data owner has complete control of information. In tech, information owner trusts service supplier for cautious distribution of information. Precisely the same way CSP does not know information which put. Some external authentication and authorization measures are required to validate the information sharers. Typically, the access control mechanism accomplished by storing information locally that is preserved by the host. The server will assess the user's authentication before permitting user to get the source.

Nonetheless, in cloud solutions information is stored in various servers to offer high availability and higher performance. The problem arises when in specific areas, data could be mishandled. To be able to protect the vital information, encryption of the report highly demanded. Mere encryption is only going to safeguard information but there's not any provision for information sharing. The secret key needs to pass to distinct sharers. Even then, the secret can't shared as such. Every sharer will have separate control on information.

The service supplier, because of encrypted temperament can't undermine the information. If any sharer should access the information, with appropriate authentication service supplier will pass the encoded information. To get access to information the information sharer has toget that the decryption key from the proprietor. The amount works is completed within this region and every one of these has suggested different steps in supplying control.

II. RESEARCH LIMITATIONS

In above all Access control schemes the problems identified as

In every program, the data owner depends on a key generator (Third-party) to generate a public key and a private key.

Sometimes maybe third-party might be compromised, and then identities will be disclosed.

If any dynamic operations are done on the PHR [1], then the data should be re-encrypting and new keys should be re-issue to the corresponding PHR users.

If any user policies changes or due to progressive policies, the user must revoke, so to reverse PHR owner must be re-encrypt the PHR and re-generate the new keys.

Due to the above limitations, a new access control model should implemented and the new model should effectively handle the progressive policies and dynamic operations.

Research Gaps

In above all access control schemes the problem identified as

In every system, the data owner depends on key generator (Third-party) to generate public key and private key.

Sometimes maybe third-party might be comprised, and then identities will be disclosing.

If any dynamic operations done on file, then data should be re-encrypting, and new keys should be re-issue to the corresponding users.

If any user policies changes or due to progressive policies, the user must revoke, so to withdraw owner must be re-encrypt the file and re-generate the new keys.

Due to the above limitations, a new access control model should implement and new model should effectively handle the progressive policies and dynamic operations.

III.RESEARCH MOTIVATION

In a conventional cloud version, PHR operator can outsource his health record into the cloud but as a result of privacy problems, before outsourcing the private health record has to be encrypted and then it is going to upload into the cloud server. PHR user will get into the private health information (PHI) in the cloud however because of secure data he can not open the information, so then he must find secrete key from corresponding PHR proprietor, so to problems that the secrete keys to PHR users that the PHR proprietor has to maintain online, But it's not feasible to PHR proprietor to remain always on the internet, so the remedy is fundamental authority (CA). Though central administration isn't wholly trusted and essential management is a significant challenge in this model.

Data access control is a practical approach to guarantee the PHR confidentiality and PHR privileges from the cloud surroundings. Access control is defined as a policy or process and set of constraints that allow, denies, or confine access over the cloud to access private health information (PHI). A variety of techniques suggested safeguarding the PHR contents solitude via access management.

From the literature review, it understood that most of the access control mechanisms introduce burden to the data owner while performing dynamic operations insertion, user revocation, and when it updates users' attribute list. Most of the ABE schemes have several limitations as it cannot efficiently handle adding or revoking users or identity attributes. It needs to keep multiple encrypted copies of the same key that incurs high computational costs. So there is the need for a suitable access control mechanism that should support progressive policies.

IV.PROPOSED METHODOLOGY

This methodology explained with seven different phases and five algorithms, GCA for group creation where different users are classified into different groups, subgroup creation in this Doctor group is again subgrouped into Gynacolygist, derma, diabetic etc, after policies applied into groups, if any user policies need to update then policie update will work, finally revoke if any user polices need to remove then revoke should apply.

Personal Health Record (PHR) users grouped their responsibility by raising GCA Group creation Algorithm.

$GF\ (S) => \{\ X\ 1,\ X\ 2....\ Xn\}$

Additional PHR user decaying support on roles into number of subgroups formulated a SF:

$SF(X_{1,}X_{2,}.....X_n) => \{\ X_1/p_{1,}X_2/p_{2,}.....X_i/p_i\ \}$

Every subgroup is connected with token produced SA (System Authority).

$$SG_{i,i} \Leftrightarrow TK_{i,i}$$

SA maintained a set of strategies and connected it with PHR tokens.

$$SA => \quad \{P1,\ P\ 2....Pn\}$$

Every time PHR owner needs to move a file into cloud, it applies the exponentiation with R for file and group signature and submits its subgroup and level to CSP.

DO -----$^{(F,\ Grsign}$)^{R}--$^{SG}{}_{i}$--------------->CSP

Parallel, PHR owner generates $R^{-\ q}$ ACP's to SA System Authority.

DO --------------------> SA

CSP computes encryption then supplies to cloud server along with key information using RSA in a protected way.

$Enc_{sk}((File\ F,Grsign)^{R}),L_i,SG_i,S_i(sk),S_i^{ei}$

The user requests the CSP to access the file with unique $R_{id.}$

User $\leftarrow$------$^{R}{}_{id}$--------$\rightarrow$ CSP

Cloud service provider decides the access grant as per the PHR user level and the subgroup they belong to as mentioned in the token.

CSP => fetch L_i in security token TK.

CSP transmits the decrypted file to PHR User

CSP--- (file,*Grsign*)^{R}-----------$\rightarrow U_i$

User request for un-blind value from SA

U_i ----------^{req}-----------$\rightarrow$SA

SA sends the un-blind value to User in a secure way.

SA -----$^{E}{}_{R}{}^{(R-1)}$ -------------$\rightarrow$

The user applies un-blind value and verifies group signature and finally, it retrieves the file.

Ui-------((*file*,*Grsign*))-------------------------------> *file*

Phase 1: Dynamic PHR Group creation

The complete information clustered to task of clients they can achieve; Algorithm 5.2 signifies group construction based on the fundamental role of users. Assume representation space described as, Sg= (GCA, A=c, U{d}), where U is general set A is set of qualities, a whole set of specific secondary characteristics. Let e definite as a component in set S and N be sum of aspects collection.

Algorithm 1 GCA

```
Process GCA($S_g$)
I/0:  users $u_{1,}\ u_{2,}\ u_{3......}\ u_n$
Output: subsets of groups $X\ _1,\ X\ _2......X_n$
Initiate
For every Subsets = $X_{i,}$ i = 1….n
Start
$X\ _{i=\emptyset}$
RB=$\sum_{i=1}^{n} R_i$
Stop;
Calculate subsets $X_{i,}$ i = 1….n
Start
Prove elements 'role' $\approx\{R_s\}$ =>
$\forall R_j \exists\ R_s$,i = 0…. $n_i$
$\forall$Component $e_j \approx$ S, j=1 to n, d=1
Start:
If ($R_i$) GCAj,k$_,$= $R_i$ then
Start:
$A_i$: =$A_i$, $Be_j$
Else
Continue
}:
Continue
}:
End;
```

Originally, every subset {X1, X 2... Xi} negative, users shifted to either untidiness of subsections conferring to their parts, which belong part bundle. This returned all users continuously record relocated to some of the subgroups. The procedure ought to perform while fresh user appended to database.

Phase 2: Subgroup creation policies

Summary of algorithm 5.3 illustrated below. It gets information as subset X produced in algorithm 5.3 output of subgroups based on various admittance control policies. Concerning every subset, dependent property outlined with systems being in bundle users classified supporting system.

Algorithm 2 Creating policies for subgroups

```
Creation of SF ($S_1, S_2 \ldots S_n$)
I: $X \in SF$,  described as $S= (g_1,g_2,g_3 \ldots g_n)$
O: set $X_j/Y_i$, build on the group
Initiate
$\forall X_i \in X_1, X_2 \ldots X_n$ , n =0……n-1;
Start:
$\forall SF_i \exists PB$;
Start:
Choose division $GCA_i$: = $\{SF_{1\ldots n} \| X (GCA_{i\ldots n})\}$
Stop all starts:
```

Phase 3: Group Token creation:

The sign made for a respective policy controlled SA and est linked with policy records. The token contains of token_ID, algorithm_ID, subgroup file ID list, hash integrity digital signature DS.

SI D	*S_g D*	*$\{funid_1, \ldots funid_i\}$*	*TEx p*	*HMA C*	*D S*

Tokens stored in a cuckoo hash table are assigned to respective subgroups to produce a universal symbol for all members of the subset. If there remain unusual users in the database, algorithm 2 and algorithm 3 can use. The removal of consumers based on the identification of subclass to which fit following and unloading the data from the database.

Phase 4: Group User adding & Removing

The client adding performed via data arrangement retrieved cuckoo filter. The Algorithm 5.4 Fan et al., (2014) demonstrate how innovative client SF_1 added into subdivision centered on policies.

Alg: 3 Appending new user

```
Operation Append (U)
GL =  Group List ($u_1 \ldots u_n \in U$);
GL =  MD5_Hash∀U;
$GL_2 = GL_1$ ( MD5_Hash(GC));
if(  position[$GL_1$] Position [$GL_2$]) =>
(position [$GL_1$] position [$GL_2$]) = {MD5_Hash};
Return 1;
$GL_1$ = randomly pick $u_1, u_2 \ldots u_n$;
Do ( $L_i$ = 0…. N < $GL_2$; N++) execute randomly
If (position [GL]) == 0
Position [GL] == {GC};
Return completed;
Return stop.
```

Algorithm 4 User removing from group

```
Start-Process:
Process Remove (PR) (User ∈GL)
PR = remove ($u_1,u_2 \ldots u_n \forall$ GL);
$GL_1$ = MD5_Hash (GL);
$GL_2 = GL_1 \in$MD5_Hash ( PR );
If (position [$u_1$]$\in GL_1$,position [$u_1$]$\in GL_2$) ={ PR } =>
Delete $u_1 \in GL_1$
End process;
```

Algorithm 5 User search

```
Process start:
Process Search (PS) (u ∈ GL)
PS = identify_User ($u_1, u_2 \ldots u_n$);
$GL_1$ = Do_Hash ( $u \in GL_1$);
if ( PS                    (position     [$u_1$    ∈     GL]
                           position [$u_2 \in$ GL] ) ) =>
Search process end:
```

Phase 5: Outsourcing encrypted Data:

The owner asks the system administrator to concern keys and to produce RSA encryption on SK. The owner of data encodes the file (F, SK) of session key changed so that (Si) ei. All these coded sets Enc_{sk} (File, $Group_i$Sign), Enc_{sk}\{File, $U \in GL$\}, All information. Grobauer et al., (2011)

Phase 6: Ciphertext Update by owner

The revoked attributes, associated with the cipher text's are needed to be altered to their recent version so as to guarantee that the newly added user should adequate characteristic to decrypt above information that published before it added to the system. To enhance overall system, performance cloud server executes calculation for ciphertext update rather than carrying out at PHR owner surface. The advanced proxy re-encryption technique used for the cipher-text modernizes. In such a case cloud seems not require to decrypt cipher-text earlier perform an update. The cloud server executes the EncryptUpdate() algorithm to alter the ciphertext related canceled attribute X¬i. It uses inputs cipher text's connected with revoked attribute Xi and renew key UXi. It updates the ciphertext that is related to revoked attribute Xia.

$$CT^1=(C_i=c_i^{\,1}; € [I,1]$$

$$\text{If } p(i)= x^1_{attributeid}: C_i=(D_i)^{UK}{}_{Xattrid}$$

$$D\,i\ \ (\,Di)^{UK}{}_{attribid}$$

Phase 7: Re-encrypt to impose policies

The data items must be re-encrypted using a new symmetric key SK, in the case of user additions/revocations or access policy changes. This privacy-preserving method requires the owner to produce a new blind value R such that (file) $^{new\ R}$ to be generated and transmitted to the cloud. The encryption will be executed again with fresh symmetric key SK by the cloud server, to ensure the access control method is fine-grained.

Backward secrecy is imposed in re-encryption, in case a superset of old group users. Forward secrecy is imposed in re-encryption, in case a subset of old set of users.

V. RESULTS AND DISCUSSION

The proposed DTBE algorithm executed in Microsoft Azure environment where User interface created with ASP.NET, the proposed DTBE is compared with CP-ABE, it shown in Table 1 where the encryption, decryption for various files sizes of DTBE, and CP-ABE schemes are compared.

Table 1 Average computation time for various phases in HCP-ABE scheme with CP-ABE [9].

Operation Time (Sec)	**File Size (KB)**	**DTBE**	**CP-ABE**
File upload Total time (Encryption + Data Transmission)	10	0.036	0.0416
	50	0.041	0.0463
	100	0.057	0.058
	150	0.062	0.073

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

File Download Total time (Decryption + Data Transmission)	10	0.044	0.045
	50	0.066	0.067
	100	0.077	0.079
	150	0.081	0.084
User Insertion (In terms of Number of Users)	10	2.0	0.05
	20	2.6	0.07
	50	4.3	0.11
	100	6.2	0.12
User Revocation (Revocation + Re-Encryption) (In terms of Number of Users)	10	2.254	0.16
	20	2.35	0.23
	50	2.47	0.55
	100	2.66	0.71
RSA Key Management		0.0045	0.0045

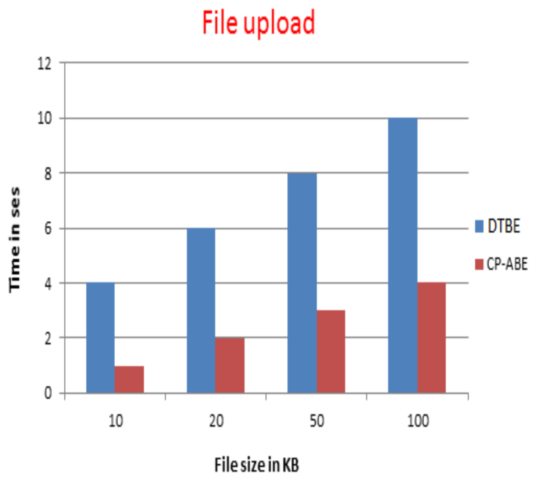

Fig: 1 Average computation time comparison for the file upload operation

Figure 1 shows the comparison of file upload for the DTBE and CP-ABE scheme. The encryption period of both schemes varies in respect to different file size.

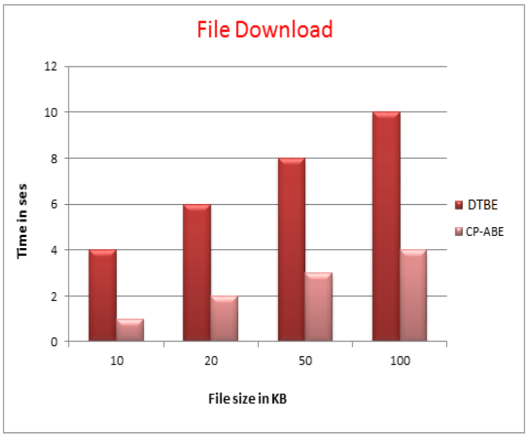

Fig: 2 Average computation time comparison for file download operation

The Figure 2 indications evaluation of file downloads operation for the HCP-ABE and CP-ABE. The decryption time also differs through reverence to the various file sizes for both the approach and time also spent nearly equal to both the schemes.

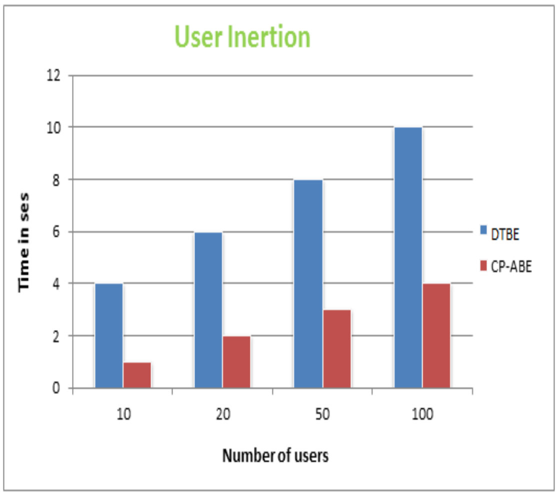

Fig: 3 Average computation time comparison for User Insertion

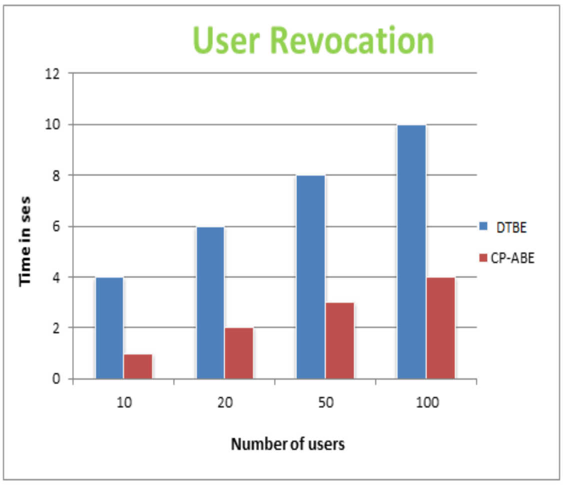

Fig: 4 Average computation time comparison for User Revocation

Figure 3 and Figure 4 show correlation of user insertion and revocation for HCP-ABE, CP-ABE scheme. The computation time varies concerning several users are inserted or removed from its database. Hence, the HCP-ABE scheme applies the clustering approach and uses the cuckoo filter techniques time it takes to perform user insertion of user revocation is very less compare to HCP-ABE. However, both the scheme takes similar key management time, which is nearly 0.0045 seconds. The same way clustering process in the CB-HPAC scheme takes approximately a few milliseconds which is negligible.

VI. CONCLUSION

In this paper, addressed the problem of dynamic policies and operations on cloud storage, generally in cloud storage to control outscored data, PHR owner enforces access control mechanism by using this he can grant the privileges to set of desired PHR users or revoke rights of particular PHR users so to achieve this many access control mechanisms are implemented, like Identity-based encryption (IBE), ABE and CP-ABE, etc. However, all these existing access control mechanisms are static means if once policy is defined on encrypted text if any user policies are changes why because users are dynamic, not static once polices updated privileges of user also get update or if any PHR user removed or want to take back the rights which are assigned previously for this these circumstances existing access control mechanisms not suitable. Sometimes once inserting data toward cloud, PHR owner could want to update Health records or remove so policies should be updated, so the objective of this work is if any PHR user policies are changes or if any dynamic operations done on a cloud server without changing any PHR user policies over encrypted data the cloud data should be updated. To achieve this new access control mechanism should require, this work proposing a new access control scheme called DTBE.

REFERENCES

1. Jingquan Li, (2013), “Electronic Personal Health Records and the Question of Privacy”, ISSN: 0018-9162, Volume: PP, Issue: 99, PP: 1-1.
2. K Liang & Willy (2015). “Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage”, ISSN: 1556-6013, Volume: 10, Issue: 9, PP: 1981-1992.
3. Lan et al. (2016), “A Secure Role-Based Cloud Storage System For Encrypted Patient-Centric Health Records”, ISSN: 1460-2067, Volume: 59, Issue: 11, PP: 1593-1611.
4. R. Manoj; et.al, (2017), “Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud”, PP: 185-190.
5. Shu-Di Bao; et.al, (2017), “A Method of Signal Scrambling to Secure Data Storage for Healthcare Applications”, ISSN: 2168-2194, Volume: 21, Issue: 6, PP: 1487-1494.
6. Sathishkumar et al. (2016), “An Efficient Key Management Infrastructure for Personal Health Records in cloud”, PP: 1651-1657.
7. Xin Yao et al. (2018), “Privacy-Preserving Search Over Encrypted Personal Health Record In Multi-Source Cloud”, ISSN: 2169-3536, PP: 3809-3823
8. Yang et al. (2017), “Lightweight Sharable and Traceable Secure Mobile Health System”, ISSN: 1545-5971, Volume: PP, Issue: 99, PP: 1-1.
9. E.V.N. Jyothi and Dr.V. Purna Chandra Rao (2019), “A Comparative Study on Access Controls and its Characteristics”, Vol 11, Issue 04, pp:799-803.
10. Jyothi E.V.N., Rajani B. (2019) Effective Handling Personal Electronic Health Records Using Metadata Over Cloud Computing. In: Bapi R., Rao K., Prasad M. (eds) First International Conference on Artificial Intelligence and Cognitive Computing. Advances in Intelligent Systems and Computing, vol 815.

AUTHORS PROFILE

E.V.N.Jyothi, working as an Assoc.Professor in CSE Dept. of Pace Institute of Technology & Sciences. I did M.Tech in CSE and currently doing Ph.D in CSE from JJT university. I have 13 years of experience in teaching for various Professional Institutions across India. So far I have published 17 papers in various Journals & Conferences. I was awarded Best Senior Faculty Award from DKIRF.