Trends in Engineering and Technology (NCTET-2K17)
International Journal of Advanced Engineering Research and Science (IJAERS) *Special Issue-3*
https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

A Secure and scalable data access control using Hierarchical CPABE in the Cloud

[1]C Sailaja, [2]B.Balakonda Reddy, M.Tech.,

[1]PG Scholar, Department of CSE, S.V. College of Engineering, sailajait1262@gmail.Com
[2] Assistant Professor, Department of CSE, S.V. College of Engineering,balakondareddyb@gmail.com

ABSTRACT:-- *Ciphertext-policy Attribute based encryption (CPABE) has been a favored encryption progression to illuminate the testing issue of secure information partaking in disseminated registering. The fundamental information reports all around have the common for multilevel hierarchy of leadership of noteworthiness, especially in the zone of helpful organizations and the military. Regardless, the levels of leadership of criticalness structure of shared records hasn't been analyzed in CP-ABE. In this paper, a compelling record chain of significance property based encryption plan is proposed in appropriated registering. The layered access to structures are encouraged into a singular get the opportunity to structure, and after that the hierarchial records are encoded with the joined get the chance to structure. The ciphertext partitions identified with qualities could be shared by the records. In this way, both ciphertext stockpiling and time cost of encryption are spared. Also, the proposed plan is wound up being secure under the standard supposition. Test reenactment makes the feeling that the proposed plan is altogether skilled with respect to encryption and unscrambling . With the amount of the records broadening, the motivations behind excitement of our course of action wind up being dynamically plainly obvious.*

Keywords—Cloud computing, Data sharing, File Hierarchy, Ciphertext-policy, Attribute-based encryption

1. INTRODUCTION

With the succeeding of framework development and flexible terminal, online data sharing has transformed into another "pet, for instance, Facebook, MySpace, and Badoo. In the meantime, circulated figuring is a champion among the most reassuring application stages to handle the shaky stretching out of data sharing. In appropriated figuring, to shield data from spilling, customers need to encode their data before being shared. Get the opportunity to control is focal as it is the principle line of resistance that thwarts unapproved access to the basic data. Starting late, attribute based encryption (ABE) has been pulled in significantly more contemplations since it can keep data security and recognize fine-grained, one-to-various, and non-instinctive get the chance to control. Ciphertext-methodology quality based encryption (CP-ABE) is one of possible arrangements which has significantly more prominent versatility and is more sensible for general applications In disseminated processing, as appeared. Master recognizes the customer selection and makes a couple of parameters. Cloud expert center (CSP) is the head of cloud servers and gives various organizations to client. Data proprietor encodes and exchanges the delivered ciphertext to CSP. Customer downloads and deciphers the charmed ciphertext from CSP. The common records generally have different leveled structure. That is, a social affair of records are disengaged into different hierarchy of leadership subgroups found at different get to levels. If the records in the same different leveled structure could be encoded by a coordinated get to structure, the capacity cost of ciphertext and time cost of encryption could be spared.

To safely share the PHR data in distributed computing, a patient partitions his PHR data M into two sections: individual data m1 that may contain the patient's name, government managed savings number, phone number, place of residence, and so on. The medicinal record m2 which does not contain touchy individual data, for example, restorative test outcomes, treatment conventions, and operation notes. At that point the patient receives CP-ABE plan to scramble the data m1 and m2 by various get to arrangements in view of the real need. For instance, a going to doctor needs to get to both the patient's name and his restorative record with a specific end goal to make an analysis, and therapeutic specialist just needs to get to some medicinal test comes about for scholastic reason in the related territory, where a specialist must be a therapeutic scientist, and the opposite

https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

is not really genuine. Assume that the patient sets the get to structure of m1 as: T1 {("Cardiology" AND "Specialist") AND "Going to Physician"}. Likewise, m2 is named as: T2 {"Cardiology" AND "Researcher"}.Apparently, the data should be scrambled twice if m1 and m2 are encoded with get to structures T1 and T2, separately. Two ciphertexts CT1 = {T1; ˜ C1;C1; ∀y ∈ Y1 : Cy;C ′y} where Y1={"Cardiology", "Scientist", "Going to Physician"} and CT2 = {T2; ˜ C2;C2; ∀y ∈ Y2 : Cy;C ′ y} where Y2={"Cardiology", "Researcher"} will be delivered.

2. RELATED WORK

Hierarchial Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services Cloud figuring, as a making get ready viewpoint, draws in clients to remotely store their information into a cloud to recognize flexible associations on-request. Particularly for little and medium-sized endeavors with obliged spending masterminds, they can satisfy cost wander resources and capability redesigns by utilizing cloud-based associations to oversee errands, to attempt joint attempts, and so forth. In any case, permitting cloud master affiliations (CSPs), which are not in an indistinct set stock in extents from tremendous business clients, to oversee private information, may raise potential security and affirmation issues. To keep the delicate client information portrayed against untrusted CSPs, a trademark course is to apply cryptographic methods of insight, by unveiling unraveling keys just to avowed clients. Regardless, when meander clients outsource described information for sharing on cloud servers, the got encryption framework ought to strengthen fine-grained get the chance to control, and moreover give tip best, full course of action, and adaptability, to best serve the necessities of getting to information at whatever point and wherever, allotting inside attempts, and accomplishing a dynamic approach of clients. In this paper, we propose a course of action to help attempts to productively share puzzle information on cloud servers. We accomplish this objective by first joining the distinctive leveled character based encryption (HIBE) structure and the ciphertext-procedure quality based encryption (CP-ABE) framework, and in this way making an execution expressivity tradeoff, at last applying center individual re-encryption and lethargic re-encryption to our course of action.

Trademark Based Encryption With Verifiable Outsourced Decryption Attribute-based encryption (ABE) is an open key based one-to-various encryption that empowers customers to encode and translate data in light of customer characteristics. A promising utilization of ABE is versatile get the opportunity to control of mixed data set away in the cloud, using access polices and acknowledged attributes related for private keys and figure compositions. One of the major capability detriments of the current ABE arrangements is that unscrambling incorporates expensive mixing operations and the amount of such operations creates with the multifaceted way of the get the opportunity to approach. Starting late, Green et al. proposed an ABE system with outsourced unscrambling that, all things considered, gets rid of the deciphering overhead for customers. In such a structure, a customer gives an untrusted server, say a cloud authority association, with a change key that empowers the cloud to decipher any ABE ciphertext satisfied by that customer's attributes or get to plan into a fundamental ciphertext, and it just gains somewhat computational overhead for the customer to recover the plaintext from the changed ciphertext. Security of an ABE structure with outsourced translating ensures that an adversary (checking a noxious cloud) won't have the ability to get the hang of anything about the encoded message; regardless, it doesn't guarantee the precision of the change done by the cloud. In this paper, we consider another need of ABE with outsourced deciphering: obviousness. Coolly, undeniable status guarantees that a customer can viably check if the change is done precisely. We give the formal model of ABE with certain outsourced unraveling and propose a strong arrangement. We exhibit that our new arrangement is both secure and self-evident, without relying upon self-assertive prophets. Finally, we exhibit an execution of our arrangement and result of execution estimations, which demonstrates a significant lessening on figuring resources constrained on customers.

Ciphertext-course of action dynamic quality based encryption with short figure works Attribute-based encryption (ABE) structures allow scrambling to vague recipients by techniques for a get to procedure showing the properties that the proposed authorities should have. ABE certifications to pass on fine-grained get the chance to control of encoded data. Regardless, when data are encoded using an ABE plot, key organization is troublesome if there is innumerable from various establishments. In this paper, we develop ABE and propose another adaptable cryptosystem implied as ciphertext-approach different leveled ABE (CP-HABE). In a CP-HABE plot, the properties are dealt with in a matrix and the customers having higherlevel qualities can

https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

name their get to rights to the customers at a lower level. These components enable a CP-HABE structure to have endless from different relationship by assigning keys, e.g., engaging profitable data sharing among logically created far reaching social affairs. We manufacture a CP-HABE plot with short ciphertexts. The arrangement is exhibited secure in the standard model under non-savvy suppositions.

Characteristic Based Encryption with Dynamic Membership Attribute-based encryption (ABE) is a prompted encryption advancement where the security of beneficiaries is ensured by a strategy of characteristics. An encryptor can guarantee that prohibitive the recipients who sort out the constrainments on predefined trademark respects

related with the ciphertext can unravel the ciphertext. In any case, keeping up the rightness of every one of clients' qualities will take enormous cost since it is basic to restore the clients' private keys at whatever point a client joins, leaves the party, or updates the estimation of any of her/his properties. Since client joining, leaving, and characteristic strengthening may happen an awesome piece of the time in true blue conditions, collaboration association will change into a to a great degree crucial issue in an ABE structure. In this paper, we will introduce an ABE plot which is the essential ABE arrange for that goes for dynamic selection association with self-confident states, not coordinated states just, for each quality. Our work likewise keeps high adaptability of the goals on qualities and makes clients can legitimately join, leave, and animate their properties. It is senseless for those clients who don't change their credit statuses to reestablish their private keys when some client resuscitates the estimations of her/his properties. At last, we in like way formally demonstrate the security of the proposed plot without utilizing optional prophets.

3. EXISTING SYSTEM

Sahai and Waters proposed fluffy Identity-Based Encryption (IBE) in 2005, which was the model of ABE. Starting late, an assortment of ABE named CP-ABE was proposed.

Since Gentry and Silverberg proposed the major idea of various leveled encryption create, different dynamic CP-ABE organizes have been proposed. For instance, Wang et al. proposed a dynamic ABE plot by joining the diverse leveled IBE and CP-ABE.

Wan et al. proposed distinctive leveled ABE plot. From that point, Zou gave an alternate leveled ABE plot, while the length of astound key is straightforward with the request of the trademark set. A ciphertext game-plan diverse leveled ABE plot with short ciphertext is likewise considered.

In these game plans, the parent support space addresses its tyke underwriting districts and a top-level support domain makes conundrum key of the going with level range. The work of key creation is scattered on various underwriting zones and the greatness of key ace focus is had any kind of effect.

DISADVANTAGES OF EXISTING SYSTEM

- Time and cost for encryption is high.
- No any special multiple hierarchical files are used.
- Decryption system time and computation cost are very high.

4. PROPOSED SYSTEM

- In this survey, a capable encryption plan in perspective of layered model of the get the chance to structure is proposed in disseminated registering, which is named report pecking request CP-ABE plot (or FH-CP-ABE, for short). FH-CP-ABE enhances regular CP-ABE with a different leveled structure of get to technique, to finish essential, versatile and fine-grained get the opportunity to control.
- The responsibilities of our arrangement are three perspectives. Firstly, we propose the layered model of get the chance to structure to handle the issue of various dynamic reports sharing. The records are mixed with one composed get the chance to structure.
- Secondly, we moreover formally exhibit the security of FH-CP-ABE plot that can adequately contradict picked plaintext ambushes (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.
- Thirdly, we lead and complete sweeping test for FH-CP-ABE plot, and the generation comes to fruition exhibit that FH-CP-ABE has low stockpiling cost and count multifaceted nature in regards to encryption and translating.

ADVANTAGES OF PROPOSED SYSTEM

https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

- CP-ABE feasible schemes which has much more flexibility and is more suitable for general applications
- Multiple hierarchical files sharing are resolved using layered model of access structure.
- In proposed system both ciphertext storage and time cost of encryption are saved.
- The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files.
- The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.

5. SYSTEM ARCHITECTURE

The system appear in conveyed figuring is given, which includes four one of a kind components: master, CSP, data proprietor and customer. In this work, we expect that data proprietor has k records with k get to levels and M = {m1; : ;mk} is shared in appropriated figuring. Here, m1 is the most vital hierarchy of leadership and mk is the slightest

pecking request. In case a customer can unscramble m1, the customer can similarly translate m2; : ;mk.

Authority. It is a completely trusted substance and recognizes the customer enrollment in appropriated registering. Moreover, it can similarly execute Setup and KeyGen operations of the proposed plan.

Cloud Service Provider (CSP). It is a semi-trusted in component in cloud system. It can really play out the doled out endeavors and return revise happens. Regardless, it might need to find however much delicate substance as could be normal. In the proposed structure, it gives ciphertext limit and transmission organizations.

Data Owner. It has enormous data ought to have been secured and shared in cloud system. In our arrangement, the substance is responsible for portraying access structure and executing Encrypt operation. In addition, it exchanges ciphertext to CSP.

User. It needs to get to a broad number of data in cloud system. The substance at first downloads the contrasting ciphertext Then it executes Decrypt operation of the proposed plan.

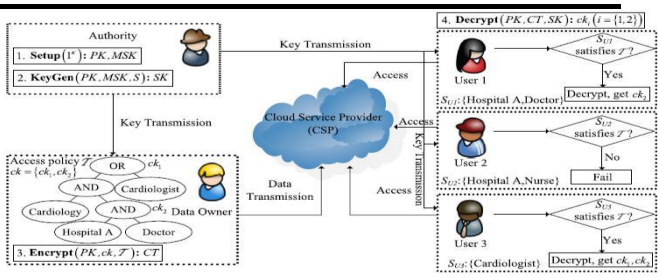

Figure 1: System Architecture

The detailed construction of FH-CP-ABE scheme is first presented. Then, based on the scheme, an improved encryption process about FH-CP-ABE scheme is proposed in order to reduce computational complexity. In addition, a brief discussion about FH-CP-ABE scheme's features is also provided.

Scheme Construction

Let $e : G0 \times G0 \rightarrow GT$ be a bilinear map, and G0 be bilinear group of prime order p with generator g. For any $k \in Zp$ and an attribute set $S = \{S1; S2; : : : ; Sm \in Zp\}$, the

Lagrange coefficient $k;S = \Pi\ l \in S; = k(x - l) = (k - l)$. Two hash functions $H1 : \{0; 1\} \rightarrow G0$ and $H2 : \{0; 1\}$ ( )

$$\sum \quad (\quad --- \quad ---) \quad \rightarrow GT$$

are used in the proposed scheme. An universe of attribute set is defined as $A\tilde{} = \{a1; : : : ; an\}$.

1) **Setup**( ) The authority runs the operation which inputs a security parameter _ and chooses random numbers $\in Zp$. It outputs *PK* and *MSK* as the formulas (2) and (3), respectively.

$PK = \{G0; g; h = g\_; e(g; g)\_\}$ (2) $MSK = \{ \quad \_; \_\}$ (3)

2) **KeyGen**(*PK;MSK; S*). The authority executes the algorithm which inputs a set of attributes $S(S\ A\tilde{})$ and creates a secret key *SK* about the set as the formula (4), where $r \in Zp$ and $rj \in Zp$ are randomly chosen for each user and each attribute $j \in S$.

$SK = \{ D = \cdot hr; \forall j \in S : Dj = gr \cdot H1(j)rj ; D\ j = hrj \}$ (4)

3) Assume that a data owner shares *k* files, i.e., $M = \{m1; : : : ;mk\}$, with *k* access levels. Then, the corresponding content keys $ck = \{ck1; : : : ; ckk\}$ are encrypted as the following **Encrypt** operation.**Encrypt**(*PK; ck; T*). The public key *PK*, content keys $ck = \{ck1; : : : ; ckk\}$, and a hierarchical access tree *T* are taken as input. The algorithm outputs an integrated ciphertext *CT*.

FH-CP-ABE Scheme With Improved Encryption

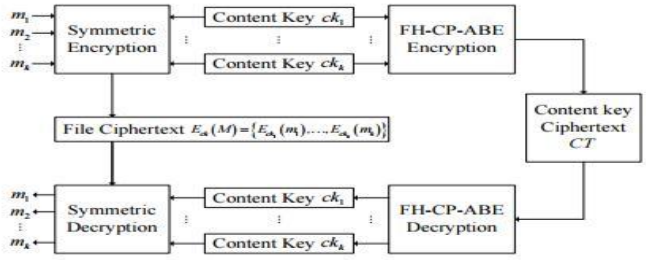

Figure2: The system framework of FH-CP-ABE scheme.

https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

To empower the presentation in the underneath, we demonstrate the above FH-CP-ABE plot as BasicFH-CP-ABE. We now show to change the encryption system of BasicFH-CPABE contrive remembering the ultimate objective to diminish computational diserse quality. In ciphertext CT, some vehicle center points are removed from CT in case they don't pass on any information about level center, where the information demonstrates leaf center, non-leaf center, level center, or transport center point in dynamic get the chance to tree. That is, these vehicle centers are ousted from CT if they don't particularly or roundaboutly contain level center. More unequivocally, we upgrade the part ˆ C(x;y);j about transport center in CT. Each and every other operation execute correctly as in BasicFH-CP-ABE. With a particular ultimate objective to make an unmistakable depiction, we use a case to furthermore speak to the upgraded encryption handle in the movement of ˆ C(x;y);j of ciphertext.

We proposed an assortment of CP-ABE to reasonably share the distinctive leveled documents in appropriated handling. The dynamic reports are blended with a combined find the opportunity to structure and the ciphertext parts identified with properties could be shared by the records. Thusly, both ciphertext stockpiling and time cost of encryption are spared. The proposed plot has great position that clients can unscramble all support records by selecting mystery key once. Thusly, the time cost of deciphering is in addition spared if the client needs to unscramble distinctive chronicles. In addition, the proposed plan is wound up being secure under DBDH question.

6. MODULES

- Data owner Module
- User and Physician Module
- Cloud Service Provider (CSP)
- Authority Module
- File hierarchy System

MODULES DESCRIPTION

Data owner Module

In the main module, we build up the Data Owner Module. Proprietor Will Signup and Wait for the endorsement Key of administrator. In the wake of Getting key Owner can login utilizing the key, and transfer any records identified with clients restorative Information on the cloud. In this module, information proprietor will check the advance status of the record transfer by him/her. It has vast information should have been put away and partaken in cloud framework. In our plan, the element is responsible for characterizing access structure and executing Encrypt operation. Also, it transfers ciphertext to CSP. After the fruition, proprietor logout the session

User and Physician Module

In this module, we build up the User Module. Client Will registries and login on the client's page. We build up the module, with the end goal that, the User will scan for his/her therapeutic records by given client restorative record id on the page. Client will get query items of the medicinal records identified with the id and he/she will ask for administrator to get to the archive which is encoded one by the administrator. Subsequent to Getting unscramble key from the administrator, he/she can access to the therapeutic records. Client logouts the session. It needs to get to an extensive number of information in cloud framework. The element initially downloads the comparing ciphertext. At that point it executes Decrypt operation of the proposed conspire.

Cloud Service Provider (CSP)

It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides ciphertext storage and transmission services. In this module, we also develop admin module process. Admin Will Login on the admin's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt.

Authority Module

It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute **Setup** and **KeyGen** operations of the proposed scheme. The Researcher will registries and login on the researcher's page. Researcher will search for any medical records by the disease category (i.e Cancer, Hernia..etc..). Researcher will Request for decrypt key to the admin. After getting the key from admin, researcher will access to the medical records of patient without their personal details. After the process, Researcher logouts the session.

File hierarchy System

The large number of classes in the Java IO package is overwhelming and annoying. However, if we use Java, we still need to understand those classes. In fact, the classes in Java IO package is not very complex, but

https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

we need a good way to learn those. There are two important factors for understanding the classes:

1). Java io class hierarchy diagram
2). Decorator pattern

7. PERFORMANCE ANALYSIS AND RESULTS:

The FH-CP-ABE scheme's implementation adopts the improved encryption algorithm in encryption operation. in a CP-ABE scheme, the complexity of access policy associated with ciphertext impacts two aspects. The one is the time cost of encryption and decryption. The other is the storage cost of ciphertext.

Figure3:Home Page

Then we want to register the details before login in to page

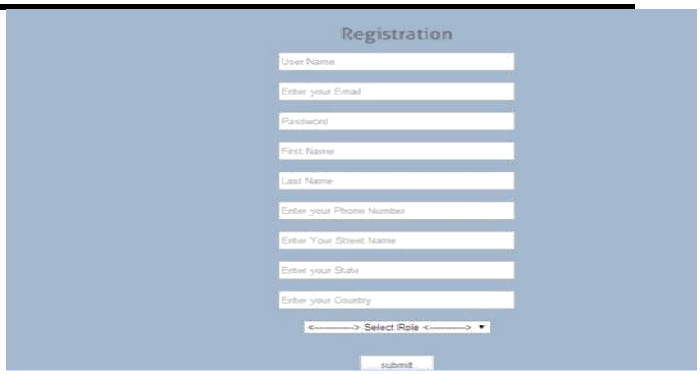

Figure4: Registration Page

Next admin want to login for checking details

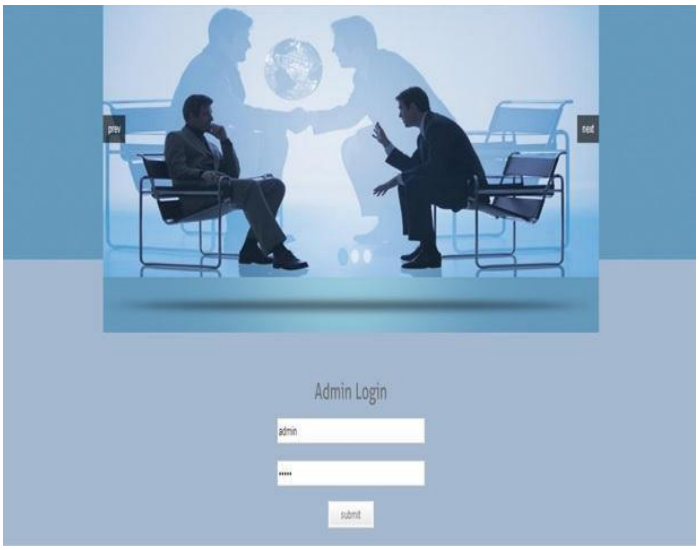

Figure 5:Admin Login

Here we can take the medical record

Figure 6:Example Of Medical Record

Figure7: Enter The Patient Details

After entering the details we want to upload files

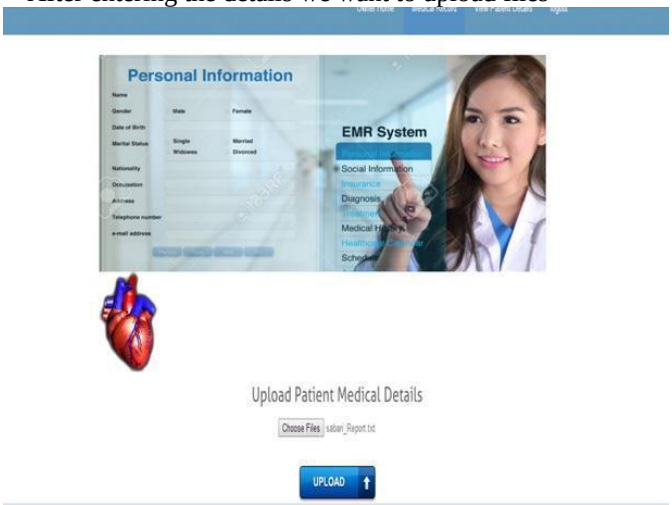

Figure8:Upload The File

Maintain the records of patient were upload file

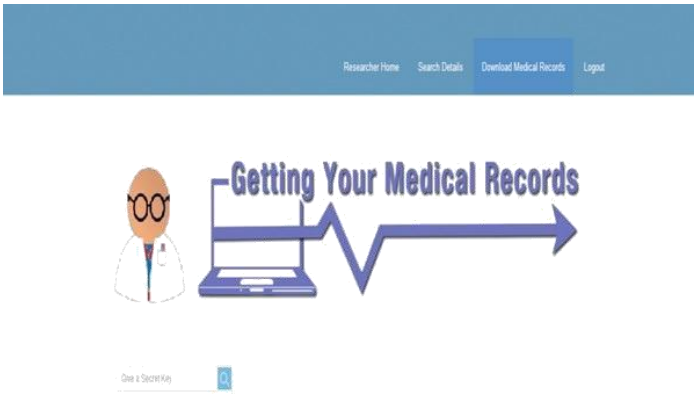

Figure9:Patient Medical Record

Receiving the medical record by using secrete key

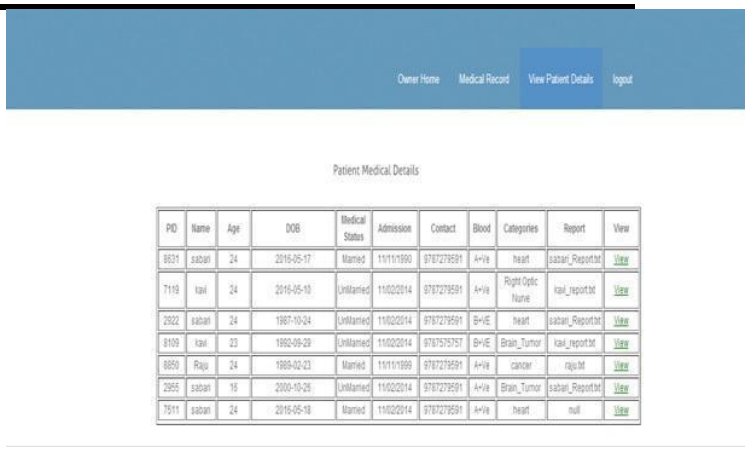

Figure 10:Getting Medical Records

The data which is uploaded by the owner will be stored in the cloud

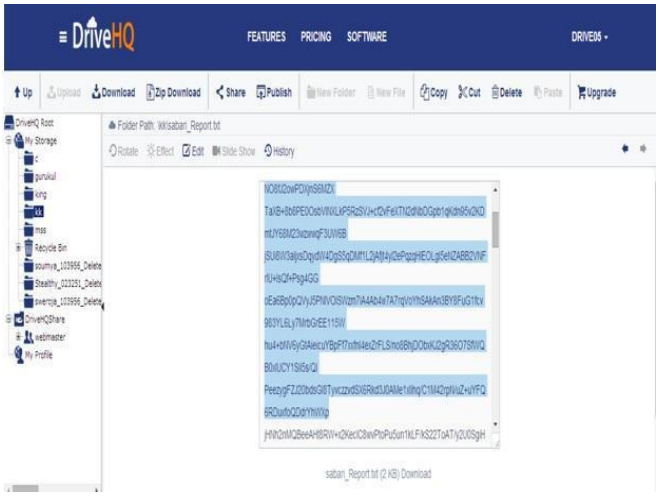

Figure 11:Public Cloud

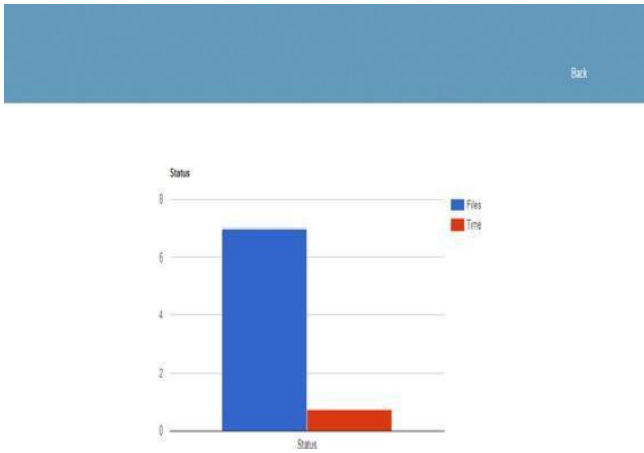

Figure12: Graph

https://dx.doi.org/10.22161/ijaers/nctet.2017.10 *ISSN: 2349-6495(P) | 2456-1908(O)*

8. CONCLUSION

An assortment of CP-ABE to effectively share the distinctive leveled chronicles in scattered figuring. The diverse leveled reports are blended with a sorted out get the chance to structure and the ciphertext parts identified with qualities could be shared by the records. In this way, both ciphertext stockpiling and time cost of encryption are spared. The proposed plot has slant that clients can unscramble all support records by taking care of mystery key once. Along these lines, the time cost of unraveling is additionally spared if the client needs to unscramble different records. In like manner, the proposed plan is ended up being secure under DBDH supposition.

REFERENCES

[1] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1667–1680, October 2014.

[2] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," *Computer Security in ESORICS 2014*, vol. 8712, pp. 257–272, September 2014.

[3] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1667–1680, October 2014.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, October 2006.

[5] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie,

"Efficient attribute-based encryption from R-LWE," *Chinese Journal of Electronics*, vol. 23, no. 4, pp. 778–782, October 2014.

[6 X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing," *Journal of Universal Computer Science*, vol. 19, no. 16, pp. 2349–2367, October 2013.

[7] Y. Yang, J. K. Liu, K. Liang, K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," *Computer Security in ESORICS 2015*, vol. 9327, pp. 146–166, September 2015.

[8] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing," *Future Generation Computer Systems*, vol. 52, no. C, pp. 95–108, November 2015.

[9] C. Fan, S. Huang, and H. Rung, "Arbitrary-state attribute-based encryption with dynamic membership," *IEEE Transactions on Computers*, vol. 63, no. 8, pp. 1951–1961, August 2014.

[10] H. Zheng, Q. Yuan, and J. Chen, "A framework for protecting personal information and privacy," *Security and Communication Networks*, vol. 8, no. 16, pp. 2867–2874, November 2015.

[11] X. Zou, "A hierarchical attribute-based encryption scheme," *Wuhan University Journal of Natural Sciences*, vol. 18, no. 3, pp. 259–264, June 2013.

[12] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption,"

Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques, vol. 6110, pp. 62–91, May 2010.

[13] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271–2282, August 2013.

[14] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," Proceedings of the 20th the system framework of

FH-CP-ABEscheme. USENIX Conference on Security, August 2011.