International Journal of Engineering & Technology, 7 (3.8) (2018) 141-146

International Journal of Engineering & Technology

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

Research paper

An Efficient Scheme to Support Direct Revocation in Cloud Computing Using CPABE :the Approach with Less Time Constraints

Miss. Rupali G. Dande[1], Prof. Dr. Amol D. Potgantwar[2]

[1]*Student, M.E.(Computer), SITRC, Nashik*
[2]*Head of Department, Computer Department, SITRC, Nashik*

**Corresponding author E-mail:[1]rupali.sury@gmail.com , amol.potgantwar@sitrc.org*

Abstract

Secure Data sharing is a major issue of concern in cloud computing. CPABE is well known encryption technique for dealing with the problem of data security over the network. Most of the files have multilevel access hierarchy especially in health care and military domain. The hierarchy structure and revocation of shared files is not scrutinized in CP-ABE. In this paper, experts proposed the enhanced method of encryption to support the direct revocation, in which sender specifies the revocation list during encryption of cipher text so that the problem of releasing periodic key update information in indirect revocation is vanished. Here the direct revocation mechanism and file access based hierarchy are merged to get enhanced CPABE. The multilevel access structure is integrated and merged with encrypted files with the current access structure. Along with revocation, aim is also to improve the overall system performance with respect to encryption time and decryption time. Experimental result shows the enhanced performance of the proposed system as compared to existing system with respect to time and security constraints. Moreover the scheme is secure under the standard security assumption. Finally, based on the research, it gives forthcoming research direction to expand and implement the scheme in any practical application where security is main concern by proper coalition of the proposed technologies.

Keywords: *Cloud Computing, Cloud security, access structure, ABE, CPABE, revocation, File hierarchy*.

1. Introduction

Scalable, flexible and ubiquitous nature of cloud computing is a real boon for individual and all fields. It offers remote access and data storage. Moreover one need not have own infrastructure for his business. Switch the data over the cloud and let the cloud handle of the rest. Various cloud service models and several deployment models play a crucial role in making cloud successful and useful at each level. Software as a Service (SaaS), reduction in purchasing of costly software and its updating cost is promising feature. Platform as a Services (PaaS) gives the platform to extend establish and extend the applications provided by the CSPs. Google App, Azure are the PaaS providers. Infrastructure as a Service (IaaS) provides the facility to control the hardware and software devices like disk storage, operating system, databases, etc over the internet. It is the accountability of the CSPs to take care all of the resources [30]. Cloud Deployment models aid in deploying above mentioned solutions Personal Cloud, Community

Cloud and hybrid cloud in line with the user’s requirements. But many hesitate to trust the cloud due to its security. CSPs gives best to ensure security to the user’s data but still some breaches are present which hurdles in cloud acceptance. The recognized seven security risks essential to consider before deploying data on the cloud which are listed below [10] [11]:

- Authorized user access.
- Data processing by third party ,outside the organization
- Storage space/location
- Data separation
- Data recovery in case of failures
- Investigation of breaches and attacks
- Long term viability

Along with these risks other risks related to confidentiality, integrity, collusion attacks, etc. The main objective of the system is to provide multilevel systems a direct revocation mechanism using file access hierarchy structure. This system can be used for the applications where multilevel data access and security is essential as in Health care and Military Services, Business Organizations, Banks [17].

2. Literature Survey

Huge amount of work is done to provide high level security to the cloud by researchers. Variations and updating in current technology is the key to unlock the sky-scraping level security in future. Primary methods were not much suitable and efficient and steadfast to secure immeasurable and remote data security. As in traditional public key cryptography there is no necessity of encrypting the cipher text with one particular user. Sahai in ABE enhanced changed the concept and introduced ABE in 2005.Which is enhanced Role Based Access Control. In this private key and cipher text must get matched is the primary condition for the user to get the access to data [2], [3].If conditions proved true between his private key and cipher text, only then user can decrypt the cipher text. The set of attributes are used to encrypt and decrypt the data by creating the access structure. Particular threshold attributes were defined for decryption.

Key Policy Attribute Based Encryption(KPABE) [7] by Goyal et al in 2006 joined access policy to user's private key Owner should be smart to choose attributes in such a way that promptly describes the authoritative users. In CPABE private key is united with set of attributes and cipher text is united with access policy [4]. A user can get original file if and only if associated attributes with the private key matches the access policy.

In the contrast KP-ABE, private key is united with the access policy and cipher text is united with the attributes [7], [9]. A user can get the original text if cipher text attributes match access policy in the private key. Both the schemes has their pros and cons but among the two CPABE is proved to be more efficient for future use as it has more scope and reliability [9]. Further researchers are trying to add variations to increase the efficiency of the CPABE.[11]

All above theories make use of monotonic access structure, Otrovsky presented the one with non monotonic access structure in 2007[19].Private Key was allowed to append negative attributes was the innovation. This is the first scheme which allows adding negative constraints to describe attributes. The scheme is detrimental for reasons like, at the preliminary stage it is hard portray the entire negative attributes correctly. Adding negative word in front of attribute can let the person who posses this attribute be inaccessible to the data. There are various organizations like companies, health care, military services where multiple authority schemes found productive and secure than single authority scheme. Take an example of manufacturing company where employees from various departments are having access to the data on cloud. In this scenario, employee from an account section should not have access to data which belongs to the admin or HR section and vice versa. For the scenarios like this, the model proposed by Wang et.al known as Hierarchical ABE is beneficial [14]. Hierarchical structure is developed in the current scheme is used to mention and save the access rights according to the designation level is the main objective.

Chun-I et al proposed ABE form IBE [28]. Identity based encryption is used to generate the keys. Root authority generates and manages system parameters and keys. Data owner, cloud storage server, domain authority and data users are the roles in the scheme. Advantages of this, it achieves the granularity as far as access control is considered. It merges the HIBE and CPABE achieves full delegation to the cloud. For confidentiality ,anonymity and CCA security ChunIYan et al proposed ABE from IBE.In this they have inherit some of the qualities from IBE to inherit into ABE for better enhancements like constant size cipher text ,anonymity and vice versa. They have used hidden access policy and introduced another access structure named and gate with wild card. Along with the encryption policies CSPs also has to consider about the decryption techniques. So that it should not impact on the system performance. Encryption and decryption time affects the system performances as they utilize the resources like memory size, battery, etc. So for the resource limited users, less decryption computations are required for better results. The secret access structure with decentralized CPABE is proposed by Huiling Quian et al [20], which is used in personal health record. By hiding and decentralizing the access structure the access security is made possible. Alongside with the access structure many focused on the length of the cipher text and associated keys with respect to data. The cipher text size will increase with access structure and accordingly results in increasing decryption overhead. Many times it affects the system performance where the resources are limited so research on this problem is important. Many of the proposed models suggest outsource decryption. But again there should be accurate security measures so that third party should not affect or harm the data. In ABE, it requires pairing based groups for encryption so every decryption will also require pair which satisfies the formula. Regular desktop can handle large operations but this could be significant problem in the devices with limited processors and inadequate battery life. The solution to this is, Green, Waters and Hohenberger [29] scheme. In which they outsourced the computation for decryption. Green suggested outsourcing the larger cipher text to the third party which cannot get the original message but its work is to generate the small size cipher text and give it to the user who by small exponentiation operation can get the original message. With the steps in ABE additional step generates the transformation key to share with the proxy which uses top shorten the cipher text. The scheme gains very much popularity as it reduces the cipher text size, but in this though the data is CCA secure and RCCA secure, there is no guarantee of the misbehaving the third party/proxy server[26]. So, Full reliability based techniques designed to achieve data confidentiality on the un-trusted server.

Lai et al proposed the concept [4] of decrypt then verify here user first decrypts the cipher text then verifies for its correctness. Recently in 2016, Jiguo Li et al proposed ABE which verifies the outsourced decryption in which their focus is mainly on verity then decrypt where user first verifies the cipher text only then decrypts after verification. The scheme is proved to be CPA Chosen Plaintext Attack secure. They proposed the delegation feature to the scheme by which several users can confirm the correctness of the cipher text but cannot access the original file Qi Li et al, concentrated their attention to multi-authority accessibility control program for storage. Secure, effective and revocable multiple authority accessibility control program in cloud storage is the result of this.

Vasily Sidorov [13] offered the different clear data security for data used and data at rest. He enhanced the TDE Transparent Data Encryption which originally has confined range of approaching solitude and protection issues. Hui Yin, Zheng Qin [16] designed secure, easily incorporated and fine grained question result confirmation scheme. A small signature strategy is used to assure credibility of authentication object. Yibin Li et al [18] given the intelligent cryptography based strategy for secure distributed huge data storage in cloud computing to accomplish the privacy. It stores the data in distributed documents so your cloud provider doesn't get the partial data. Knowledge packages are separate to reduce the operation time. Palivela Hemant [12] tried to solve the issues related to security and backup by providing governance body which handles the communication from user to server and again to the requesting user. The database of the user to server connectivity is given by the routing table which is attached to the end and middle server.

Recently Jiang Schuci and Gou Weibin, Fan Guisheng [18] in IEEE 2017 proposed the Hierarchy ABE for supporting direct revocation in cloud storage. They have discovered that, during practical implementation of ABE there is no provision for encrypting the data according to access level which is not suitable for practical purpose. So they implement the direct revocation support algorithm in ABE.

3. Related Work

ABE is widely known method for data security but is not suitable for the practical applications [18].One of the flaws in CP-ABE is it does not support direct revocation. Numerous evolutions have been implemented to enhance the security. But the main flaw by which it is still limiting the practical implementation is its lack of revocation mechanism. Though ABE is very efficient and reliable encryption method but it doesn't support the revocation based on access levels. In this study the main focus will be on the direct revocation along with file access.

4. Preliminaries

4.1. Access Structure

It’s an accumulation of the set of qualities or parties which are valuable in defining the licensed and non licensed attributes. Using monotone accessibility framework is more accepted than non monotonic access structure. It is the collection of non empty subsets of P.
Let P = P1, P2, P3, P4 be the set of parties, attributes plays a role of parties. A collection $A \subseteq 2^{P}$ is monotone if $\forall B, C\ \ B \in A\ and\ \ B\ \subseteq C\ then\ C\ \in A$
The sets in ‘A’ are referred to as authorized sets and sets not in ‘A’ are regarded as non authorized sets.

4.2. Access Tree

The symbol x represents the node’s row in T (from top to bottom), and y represents the nodes column in T (from left to right).Nodes can be denoted as,
P= (1,1), Q = (2,1), R = (2,2), X =(3,1), Y = (3,2), A = (4,1), B = (4,2), C = (4,3).
To facilitate the description of access tree, several functions and terms are defined as follows.
(x,y) represents nodes of the tree, if (x,y) is a leaf node to denote attribute, If (x,y) is a non- leaf node to denote threshold gate ,AND, OR , etc. num(x,y) number of (x,y) nodes children in Tree T, K(x;y) is threshold value of node , 0 < K(x;y) K(x;y).

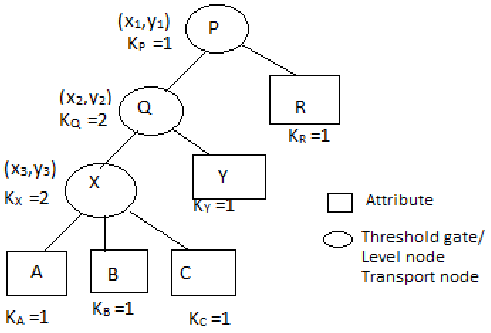

Fig. 1: An example of three levels Hierarchical Access Tree

When K(x,y) = 1 and (x,y) is a non leaf node, then (x,y) is OR gate. When K(x;y)= num(x;y) and (x,y) is a non leaf node, (x,y) is AND gate. In above figure 1, $(x_1; y_1)$ is highest hierarchy and $(x_k; y_K)$ is lowest hierarchy. Node (x,y) is a transport node when if one of the children of (x,y) contains at least one threshold gate. Index(x,y) returns a unique value associated with the node(x,y), where the value is assigned to (x,y) for a given key in an arbitrary manner. Attr(x,y) It denotes an attribute associated with the leaf node(x,y)in T.

4.3. Bilinear Maps

It is the function which combines two vector spaces for producing the third result vector space. With the help of bilinear maps key generation and cryptography, IBE and short signature techniques get benefit a lot rather than other complex techniques.
Suppose P_0 and P_T be two groups of prime order p. P is the generator of P_0.
A bilinear mapping e: P_0 X P_0 → P_T proves following characteristics:

- Bilinearity: For all u; v $u, v \in G_0$ and $a, b \in Z_0$, it has $(u^a, v^b) = e(u,v)^{ab}$.
- Non degeneracy: It exists $\exists u, v \in G_0$ which makes $(u, v) \neq 1$.
- Computability: $\forall u, v \in P_0$; efficient computation is there e (u,v).

5. Proposed work

The proposed system is mainly focusing on the issue related to direct revocation in CPABE. Direct revocation list created by the owner will get merged in cipher text by which limited access will be sorted for different users according to various access levels. The proposed system consists of 4 modules each having performing separate tasks.

Key Authority:
Key Authority is the module who authenticates the user according to its identity and role. The key authority knows the owner and users information. Owner sends the metadata to the authority and then AA uses this Meta data to generate the keys for users. For every weighted attribute it posses n weighted it poses a weighted value by using which key authority computes the secret keys. Then CSP and Key Authority cooperate and generate secret key for the user. The hierarchical authorization structure of our scheme reduces the burden and risk of a single authority scenario.

CSP:
CSP’s task is to save and secure the data sent by owner and keeps the track of operations performed by users and owners. Then CSP and Key Authority cooperate and generate secret key for the user. Check the system performance.

Encryption:
The encrypt algorithm inputs the content keys, access Tree and public parameters to generate the cipher text. The encryption depends on the node information viz., level of the node, degree of the node and threshold value of the node. Form the root node the degree of polynomial is set to one less than threshold value. It starts from the root node that ‘i’ in top down approach. For each non-leaf node it sets the index of the parent and chooses d_x for defining the complete value. Meanwhile, each leaf node denotes an attribute with weight. In the access tree here contains leaf node with it minimum weight of each leaf node. The cipher text is then computed and sends the integrated cipher text to CSP.

Decryption:
When user requests CSP to access cipher text, CSP transmits the corresponding cipher text to user. The user can get the content key and then uses the content key to further decrypt the file. User requests CSP to access the cipher text, by improved algorithm, first he will get the content key only when he is authorized and then he can decrypt the cipher text to get the original message so that any other malicious intruder should not reach up to original data. In this improved decryption , there are two steps first is for obtaining the content key and second is for getting original data from respective content keys. Then it further has 2 different methods, one for users belonging to the leaf node and second for the users belonging to the non leaf node. We’ll discuss in detail in proposed approach. Simplified cipher text is the one with simplified access structure. Only authorized users will have privileges to query the owner’s data on the cloud. User has their ids and roles. After requesting data, user must satisfy the conditions present in the access structure. If user satisfies the conditions according to their access policy only the mentioned content keys will get decrypted and allows the limited conditions access to the file according to every level. User having higher level and satisfies the conditions present in the access structure with encrypted data, only those users can get the original data. The work flow of the proposed work in terms of medical system is shown in figure 2:

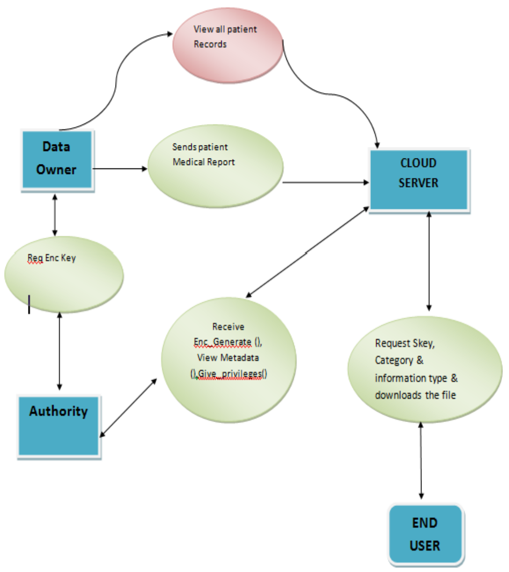
View all patient Records
Data Owner
Sends patient Medical Report
CLOUD SERVER
Reg Enc Key
Receive Enc. Generate (), View Metadata (),Give_privileges()
Request Skey, Category & information type & downloads the file
Authority
END USER

Fig. 2: The work flow of the architecture in terms of medical application defining main functionality of all modules

6. Proposed Approach

6.1 System Block Diagram

The proposed system architecture diagram is presented in figure 3. Following entities are responsible for performing the system operations.

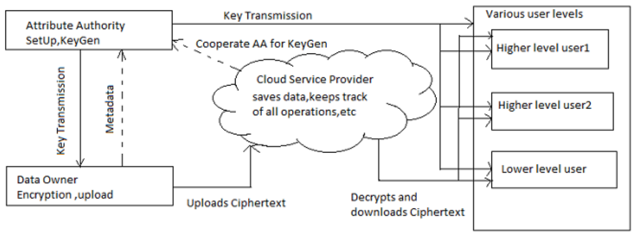

Fig. 3: The framework describing the workflow of the Proposed System with functionalities of each module.

CSP (Cloud Service Provider)

Responsible for performing assigned tasks related to storage and transmission of data. Keep records of the transactions, view owner and user record. Help the authority to generate the keys.

Data Owner

It should define the access structure and responsible for encryption operation in order to produce cipher text. Data owner uploads all the files, deletes the files and sends metadata to the authority.

Authority

The setup and key generation operations are performed by AA. The key distribution is also done by the AA. View all the authorized data owners and users. Provide the permissions to the users.

User

Downloads and decrypts the file if authorized.

6.2 Detailed Description Explaining R-CPABE

Initially setup and key generation actions are performed by Key Authority with the help of CSP. CSP selects a random number from the universe $\delta_1 \in Z_P$.

It calculates $K_1 = g^{k/\delta_1}$ (1)

Where, $k = (\alpha_1 + \alpha_2)\ \beta$.

CSP passes this information to KA.

KA chooses $\gamma \in Z_P$ and calculates

$$L_1 = K_1^{\gamma/\beta} = g^{(\alpha_1+\alpha_2)\gamma/\delta_1} \text{ And} \tag{2}$$

$$L_2 = h^{r\gamma} \tag{3}$$

KA sends (L1, L2 (γ, β, r)) to CSP.

Then CSP now computes,

$$K_2 = (L_1^{\delta_1}, L_2^{\delta_2}) \tag{4}$$

CSP transfers (L_2, δ_2) to KA.

Now KA calculates

$$L_3 = K_2^{1/\gamma} \text{ And send it to CSP.} \tag{5}$$

CSP calculates

$$D = L_3^{1/\delta_2} = g^{(\alpha_1+\alpha_2)}h^r \ = g^{\alpha}h^r. \tag{6}$$

And sends a personalized key components to respective users Say u.

KA performs the algorithm which inputs the MSK_1, and number m ∈ Z_p and set of weighted attribute S. Each weighted attribute posses a weighted value$\omega_j (\omega_j \in W)$.

Finally it computes SK_1 by the formula.

$$SK_1 = M = g^r, \forall j \in S :\ D_{j,} = H(j)^{r\omega_j}. \tag{7}$$

Now the encryption procedure it inputs public parameters PP, content keys ck and access tree τ , outputs CT cipher text. Initially the polynomial qx is selected for each node in top to bottom manner for each node x in τ. Remember, degree of the polynomial is set to 1 less than threshold value i.e. dx = kx – 1. Beginning from the root node $q_R(0)$ = s, where , s in Randomly selected from Zp, algorithm randomly selects d_R and other points of q_R. For each non root node it sets qx(0) = qparent(x)(index(x)) and randomly chooses dx to define qx. Each leaf node shows an attribute with weight. In access tree τ ,T be the set of leaf nodes with minimum weight of ω_i, algorithm computes the CT using these values. Sends integrated cipher text (ID,CT,ck(M)) to CSP. For all these operations, KA first accepts the enrollment, when a new user wants to join the system. KA authenticates and assigns a set of weighted attributes to the user according to user's role and identity. Then KA and CSP coordinate to generate the SK as discussed.

Now comes the decryption part, valid user requests the CSP to access the cipher text (ID, CT, ck(M)).The user can get the content key ck by calling users. decrypt algorithm discussed below, then user uses this ck to further decrypt the file M using data. decrypt operation.

1) users.decrypt

As stated earlier user poses the set of attributes S, if S satisfies the access policy in τ , user can obtain the content key ck. It has two conditions one is for leaf node and another for non leaf node and depends on the weighted attribute of the node x.

If $K \in S\ or\ \notin S\ and\ \omega_i > \omega_k\ then$ decryptNode = ⊥.

If $K \in S\ and\ \omega_i = \omega_k\ then$ then we can compute the decryptNode as,

decryptNode (CT; SK; x)1 = $\widehat{e}(C_x, L).\hat{e}(C, D_k)$

$= \hat{e}(g,g)^{r\beta q_x(0)}.$

If $K \in S\ or\ \notin S\ and\ \omega_i < \omega_k\ \omega_i < \omega_k\ then$ then we compute decryptNode as

decryptNode = $\hat{e}(C_x.C_{x,j,}, L).\hat{e}(C, D_k)$

$= \hat{e}(g,g)^{r\beta q_x(0)}.$

If x is a non leaf node, decrypt node is defined ,∀nodes children nodes of x it input (CT,SK,z) and

Store output as $F_{z..}$ If no node exist Fz =⊥.

If not F_z is computed as below,

$$F_z = \pi_{z \in S_x} F_z\ \Delta_{k,S'(0)}$$

$$= \hat{e}(g,g)^{r\beta q_x(0)}.$$

$$F_z = \pi_{z \in S_x} F_z\ \Delta_{k,S'(0)}$$

$$= \hat{e}(g,g)^{r\beta q_x(0)}.$$

Where, k = index (z) and S’$_x$= index(z) : z ∈ Sx.
Then we define decryption algorithm for calling decryptNode$_1$ or decryptnode$_2$ on root node R of access tree τ.
If τ is satisfied by S then,

$$A = \text{decryptNode}_{1\text{or}2}(\text{CT, SK, R}) = \hat{e}(g,g)^{r\beta R(0)}.$$
$$= \hat{e}(g,g)^{r\beta S)}.$$

Then user can get ck,

$$\bar{C}/(e(\widehat{C,D})/A \;= \bar{C}\,/\hat{e}(g^s, g^\alpha.h^r)/\hat{e}(g,g)^{r\beta S} = ck \qquad (8)$$

2) data.decrypt :
Here user gets input as ck and cipher text file E$_{ck}$(M). File M can be obtained by using symmetric decryption algorithm either AES or DES as,

$$D_{ck}\,[E_{ck}(M)] = M. \qquad (9)$$

7. Performance Analysis

Here, the theoretical and practical simulation results are given. The results prove the proposed system is efficient with respect to time than the existing system. Various parameters are used for theoretical performance comparison, discussed in following table1:

Table 1: Comparison of system with performance parameters

Sr. No	Parameters	RCPABE	CPABE
1	Revocation	Present	Absent
2	Security	More secure than previous	Secure
3	Time Efficiency	Less	More
4	Overall Performance	Requires Less time	Requires more time

To perform the experimental analysis the algorithm is implemented in health care domain. The system used is having 1GB RAM, Pentium IV processor and the experiments are performed in java. The results are generated after implementing both the systems i.e. with ABE and with R-CPABE. The graphs are generated for both the systems. The data used for the system is the disease ontology files for the patient’s disease. The graphs are plotted against the files and the time required for encryption and decryption in milliseconds. From the above graphs, it is clear that the proposed system time delay in terms of encryption and decryption is much less than the existing system. The overall system performance of the system is improved as compared to existing system. Hence it is proved that this framework has improved the efficiency parameters like time, efficiency and performance parameter like direct revocation, security. We can also prove that the overall system performance is enhanced after using the R-CPABE with respect to time. The overall system performance time is much reduced by using the proposed algorithm as shown in figure 6.

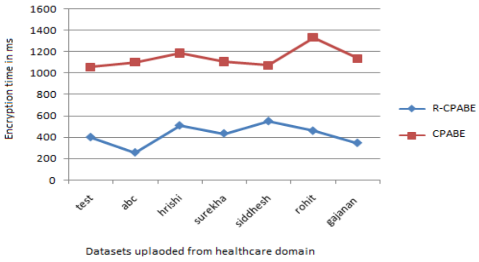

Fig. 4: Performance Comparison between ABE and R-CPABE for encryption of the files

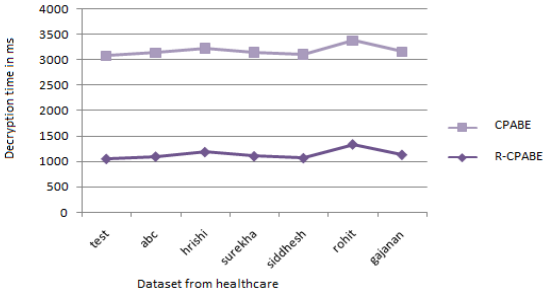

Fig.5: Performance Comparison between ABE and R-CPABE for decryption of the files

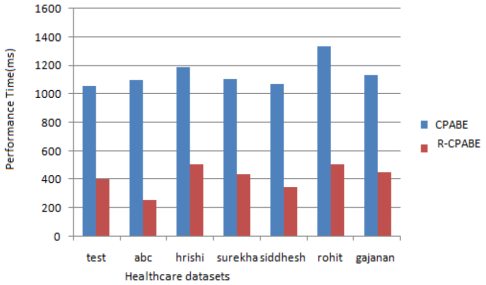

Fig.6: Comparison of the system with RCPABE and non RCPABE using real time heath care datasets

8. Conclusion

The proposed system provides direct revocation access with high data security. Support higher and lower access revocation beneficial for multilevel systems. The main advantage of the scheme is it gives support for direct revocation by encrypting the data or files by managing the revocation of people who can decrypt the whole data or not. Based on the file hierarchy access structure the user having higher level can decrypt the lower level files but reverse situation is not true. That is lower level user’s cannot decrypt the higher level files. The proposed system find implications in services like healthcare and military where employee access hierarchy is essential to keep system well maintained. There is a lot of scope in improving the security in cloud. The less user overhead algorithms must be proposed and implemented further. The issues related to virtualization, multi tenancy should be reduced in future. Lastly, using the ABE algorithms various data level security must be implemented. There should be widely acceptance of the proposed system for multi level file hierarchy based CPABE.

Acknowledgement

I would sincerely like to thank our H.O.D Dr. Amol D. Potgantwar, Department of Computer engineering, SITRC, Nashik for his guidance, encouragement and the involvement shown in this research. His expert suggestions and feedback had immensely enhanced the effectiveness of this work. The work is supported in part by the Thermax Global Company Ltd. Pune.

References

[1] Hashizume et al., “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications, 2013.

[2] J.Bethencourt, A. Sahai and B. Waters, Ciphertext - policy attribute based encryption, Proc. IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[3] A. Sahai, B. Waters, Fuzzy identity based encryption, Proc. EUROCRYPT 2005, LNCS 3494, Springer, pp. 457473, 2005.

[4] Jiguo Li, Yao Wang, Yichen Zhang and Jinguang Han, “Full Verifiability for Outsourced Decryption in Attribute Based Encryption”, February 2016, IEEE Transactions.

[5] Chun-I Fan, Yi-Fan Tseng, and Chih-Wen Lin, “Attribute-Based Encryption from Identity-Based Encryption”, SEPTEMBER 2016, JOURNAL OF LATEX CLASS FILES.

[6] Anand Tripathi and Gowtham Rajappan, “Scalable Transaction Management for Partially Replicated Data in Cloud Computing Environment”, 2016 IEEE 9th International Conference on Cloud Computing.

[7] V. Goyal, O. Pandey, A. Sahai and B.Waters, Attribute-based encryption for fine-grained access control of encrypted data, Proc. 13th ACM conference on Computer and Communications Security, pp. 89-98, 2006.

[8] Yibin Li a, Keke Gaib, Long fei Qiu, Meikang Qiub ,Hui Zhao d, “Intelligent cryptography approach for secure distributed big data storage in cloud computing”, 2016, ELSEVIER..

[9] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, “A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments”, International Journal of Network Security, July 2013.

[10] S.Mahdiet.al, “Challenges and security issues in Cloud computing from two perspectives: Data Security and Privacy Protection”, 2015, KBEI.

[11] Dimitro Zissis, Dimitos Lekkas , ”Addressing CC security issues”,2010, ELSEVIER.

[12] palivelaHemant,NitinChawande,et al., ”Development of servers in CC to solve issues related to security and backup ”2011,IEEE.

[13] VasilySidorov,WeeKeong Ng, ”Transparent Data Encryption for Data-in-Use and Data-at-Rest in a Cloud-Based Database-as-a-Service Solution”, 2015, IEEE.

[14] G Wang et al,Hierarchical ABE for fine grained access control in cloud storage services,17th ACM conference on computer and communication security ,2010.

[15] Dong,Wang, ”Trust-but-Verify: Verifying Result Correctness of Outsourced Frequent Itemset Mining in Data-mining-as-a-service Paradigm”,2015,IEEE transactions on cloud.

[16] HuiYin,ZhengQin,et,al., ”Achieving secure ,universal,fine grained query results verification for secure search scheme over encrypted cloud data ”,2016,IEEE transactions on cloud.

[17] Naeem Ahmed, ”Cloud Computing: Technology, Security Issues and Solutions”,2017,IEEE

[18] Jiang Schuci,GuoWeibin et al,”Hierarchy Attribute -Based Encryption scheme to support direct revocation in cloud storage”,2017,IEEE.

[19] Cheng-Chi Lee et al, “A survey on attribute based encryption schemes of access control in cloud environment”, July 2013, International journal of network security.

[20] HuilingQianJiguoLiYichenZhang,et al.,”Privacy-Preserving DecentralizedCiphertext-Policy Attribute-Based Encryption with Fully HiddenAccess Structure”,2013,International Conference on Informationand Communications Security.

[21] SuhairAlshehri, Stanisaw P. Radziszowski, and Rajendra K. Ra “Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption”, 2012 IEEE 28th International Conference on Data Engineering Workshops.

[22] Cheng Guo1, Ruhan Zhuang1,2,Yingmo Jie1, YizhiRen, Ting Wu, Kim-Kwang Raymond Choo, “Fine-grained Database Field Search Using Attribute-Based Encryption for E-Healthcare Clouds”,2016 Cross- Mark.

[23] M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE cipher texts, Proc. The Usenix Security Symposium, pp. 34-34, 2011.

[24] J. Lai, R. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption”, IEEE Trans. Information Forensics and Security, vol. 8, no. 8, pp. 1343-1354, 2013, doi:10.1109/TIFS.2013.2271848.

[25] B. Qin, R.H. Deng, S. Liu and S. Ma, “Attribute-based encryption with efficient verifiable outsourced decryption”, IEEE Trans. Information Forensics and Security, vol. 10, no. 7, pp. 1384-1393, 2015, doi:10.1109/TIFS.2015.2410137.

[26] X. Mao, J. Lai, Q. Mei, K. Chen and J. Weng, Generic and efficient Constructions of attribute-based encryption with verifiable outsourced decryption, IEEE Trans. Dependable and Secure Computing, 2015, doi:10.1109/TDSC.2015.2423669.

[27] Edonardo Gaetani et al , Block chain based database to ensure data integrity in cloud environments.

[28] Chun-I Fan Attribute Based Encryption from Identity Based encryption, Journal of LATEX class files,September 2016.

[29] Matthew Green, Brent Waters, Susan Hohenberger, Outsourcing the decryption of ABE cipher texts, Proc. The usenix security symposium, pp.34-34, 2011.

[30] William Stallings Cryptography and Network Security Principles and Practices, Fourth Edition.