2015 IEEE 7th International Conference on Cloud Computing Technology and Science

An Efficient Framework and Access control scheme for cloud health care

Saravana kumar N
School of Information Technology and Engineering
VIT University,Vellore,India

Rajya Lakshmi G.V
Northwestern Polytechnic university
Fremont,California,USA

Annappa B
National Institute of Technology
karnataka,India

***Abstract*—Cloud computing is being a potential role in providing services for utilizing a huge data in various application, as it is ubiquitous. In emerging growth of Cloud services been focused on security issues and optimal data storage used by consumers.Eventually, the Cloud storage is the best way to keep essential business data secure and accessible. Along with that, there are few important feature been considered. i.e(file versioning, automatic sync,collaboration tools, security File Encryption). In our research article, the framework is designed for real-time Healthcare business application to be achieved all the essential features with Inter-Cloud data storage.To do additionally, has been implemented and tested by an efficient CP-ABE (Cipher Policy-Attribute Based Encryption) algorithm for secure data transmission. Outcomes were powerful in a such way that can be promised in a designed framework developed in Python 3 in Charm-Cryptography.**

Keywords: cloud computing, CP-ABE,Health care,security,privacy.

I. Introduction

Cloud computing is a paradigm shift from traditional computing system. Albeit, the revenue of the cloud service providers increases exponentially the cloud critical application are limited. The security and privacy concerns inhibits the growth of cloud. By tradition, Encryption is the way used to secure data. The cloud servers are considered to be untrusted as the user data are stored in replication. As a result, the data theft by malicious attackers is comparatively high. Unlike traditional servers the encryption technique and access control schemes cannot be applicable to the cloud based servers. Role based access control (RBAC) and Identity based Encryption (IBE) seems to be promising but its suffers from user revocation problem. In RBAC, the access is being granted to the person of same position irrespective of the departments and fields. This again leads to security and privacy of the data. In case of Identity based encryption by means of knowing anyone of the identity of the user it is easy to revoke. To address the above stated problem the Attribute based encryption are proposed by sahai and waters. Attribute based encryption due to its properties it suites well for the cloud computing. Key-policy attribute based Encryption and the Cipher text attribute based policy are different types of ABE schemes. The private key of the user are being associated with attributes of the users. Once the user attributes satisfies the access structure the user able to encrypt the data. The generated cipher-text act as policy to decrypt the data by the user.KP-ABE is the reverse of CP-ABE and the key needs to satisfy to decrypt the data. In this paper we have proposed privacy-preserving preserving ABE algorithm for the health system. As there is exponential growth of medical data in recent years and traditional servers are not capable of storing large data sets of the users and maintaining and sharing it. The cloud has the advantage of being highly scalable,it requires secure sharing of Electronic Health Record (EHR) of the patients. As a result, the EHR can be accessed by patient at anyplace using internet at reduced cost. From the emergence of electronic health record the health care undergone various changes. Still people spending a huge amount for creating and maintaining the Personal Health Records(PHR). As the cloud uses pay as per use model it will be highly beneficial for the health industry. Its always right to move with latest technology as a result better services to the customer will be made at reduced cost. Albeit, the application of cloud in health care is highly appealing there is security, Privacy and legal issues. The recent changes in HIPAA will benefit the cloud service providers to start providing services to the customers. .

A. Motivation

The algorithm is proposed based on cipher text policy attribute based encryption. Though the CP-ABE is promising which was introduced by the waters there are certain issues. Generally we cannot follow the same encryption algorithm it depends on three factors application, size of the data and computational complexity. Considering the critical applications like health care, banking etc. the algorithm needs to change accordingly.In our algorithm, we consider, Cloud servers are considered to be semi-trusted. And multiple authority are involved throughout the process. The limitation of the CP-ABE Scheme as follows:

1) Cipher text complexity: The cipher text will act as an access policy to decrypt the message once it satisfies the user access structure. Generally, generation of cipher-text itself tedious process as it involves much complexity. As the user attributes and the data are gradually increasing and it requires a large amount of storage space for cipher-text itself and generated cipher text usually variable in size. As a result, it is much complex in terms of time and cost for generating cipher-text.

2) Decryption overhead: When there is match between user attributes associated with cipher-text by satisfying the access structure, the user is allowed to decrypt the data. The decryption takes much time and it is costly as it requires large amount of server utilization. One way to reduce the decryption overhead is by means of using search able encryption scheme as the cloud server knows the user attributes. Consequently, its

978-1-4673-9560-1/15 $31.00 © 2015 IEEE
DOI 10.1109/CloudCom.2015.98

not preferred as it lead to privacy threat particularly for critical applications like health system.

3) Trusted authority and secure sharing of data: The CP-ABE schemes is widely adopted in cloud because it has efficient access control mechanism irrespective of the some overheads like storage and complexity compared to RBAC and IBE.Albeit, the sole owner of data is the owner (patient in case of health system).As the cloud server is untrusted/semi-trusted, its unsafe to have single control authority. Multi-authority is evident to over issue but it might leads to collision (update, delete and delegate) and there might be many multi-authority under the control of single control authority. And privacy of user should be preserved as it is critical health data and adhere to latest regulations of HIPAA. For sharing of data by the owner, the proxy re-encryption scheme is used with verifiability of the data.

B. *Our Contribution*

To overcome above listed, We have proposed a patient centric framework for health system. Our framework consist of hybrid CP-ABE with efficient sharing secret sharing scheme. Firstly, we propose patient centric efficient framework which involves multiple authorities with delegation and user revocation. Secondly,we proposed user perspective access control algorithm. Finally, analysis of the security has been made and implementation of algorithm is carried out.

1) To reduce the complexity of the cloud server, the constant size cipher text is being used in the algorithm [1]. Firstly, the user are subscribed to the cloud service. The Trusted authority provides the private key to the user and depends upon the attributes, Access structure will be created. The user needs to satisfy access structure to proceed to next step. And thus overcomes the limitation of cipher text complexity by limiting cipher-text size and bi-linear pairing.

2) Outsourcing the decryption process is the way to reduce the decryption overhead. The message decrypt needs to verify. Our proposed algorithm is enhanced and lightweight algorithm that reduces the cost of the decryption significantly.

3) Proxy re-encryption is the way for linear secret sharing of the data. The proxy servers is similar to original server it re-encrypts the cipher-text and the user can decrypt the message using her attributes provided it is shared.

II. Related Work

Encryption and access control are hot topic in cloud. There are various access control schemes proposed by various researches. The various access control schemes includes the DAC, MAC, RBAC, IBE to provide maximum security to the data and sharing. The limitation of these access control techniques leads to adoption of Attribute Based Encryption [2]. The author balamurugan et al proposed the framework for efficient data sharing for health system [3]. They have used framework is based on concept of community cloud and sharing of data is being limited. The paper doesnt describes about encryption techniques for data storage in cloud. The cost of implementation of the framework is high comparatively as they cloud environment uses building private cloud infrastructure in own premises. The paper titled Layered storage architecture for health system using cloud describes a detailed framework for data storage in cloud based on multi-cloud concept [4]. The paper uses three way data storage based on criticality of data and data encryption using RC5 algorithm. Though the framework seems to be efficient, the access control is again a critical issue. The paper proposes the efficient data sharing using Message passing Interface by creating clusters of cloud. Though the results seems to be promising the sharing of data limited to the clusters associated. The system model is not ubiquitous. [5] To overcome the above limitation the author proposed efficient framework to resolve the inter-operability issues in clouds [6]. Again the access control is an issue. Cipher text-Attribute based encryption was proposed by sahai and waters [7]. The authors proposed algorithm to overcome the limitation of IBE. They have proposed a collision free algorithm for efficient delegation of authorities. Moreover the algorithm uses threshold method and complex construction and decryption phases. In CP-ABE Scheme the concept of single trusted authority is used. Later Hierarchical attribute based encryption were introduced for fine grained access control [8]. Albeit, it provides solution for fine-grained access control its difficult to implement in practical. Moreover it doesnt support the compound attributes.Multi-authority attribute based encryption were proposed by Melissa chase by considering the cloud server to be untrusted and its always high risk of believing the single authority for credentials. The limitation of the model includes the user attribute revocation and decryption issues. In order to overcome the decryption overhead of cipher text, the green et al proposes the access control by means of outsourcing to another server.Though, the model seems to be efficient in terms of the cost and time yet it suffers from serious disadvantages of data verifiability. To overcome issues Junzuo Loi proposed algorithm for verification of the outsourced data [9]. Ming Li, proposes a framework for data sharing the paper describes the various types of attribute based encryption available and matches with the application and author proposes the light weight access control algorithm for the cloud critical applications. The new access control model (AC3) for the cloud computing by younis et al [10]. The author believed that the proposed scheme will solve the limitation of the existing access control scheme. All these enhanced attribute based encryption has its own pros and limitation. None of the access control schemes provides solution to the cloud critical application like health care where it need to satisfy the various factors like efficient fine grained access, prevent unauthorized access, highly scalable, dynamic user revocation, decrease in server complexity by reducing the storage , decryption time and efficient secret sharing.

III. proposed work

A. *Framework*

Cloud based Health system is much needed in todays world. Exponential growth of medical data and difficulty in managing the data are some of the reasons associated with conventional system. At present most of currently available framework are related to private/hybrid/community cloud due to security and privacy concerns. Our framework is based on public cloud scenario. The electronic health record of the patient is uploaded by the physician. Primarily, the actors in the role are Physicians, nurse, pharmacist, patients, researcher, Insurance, emergency care are given access by the trusted

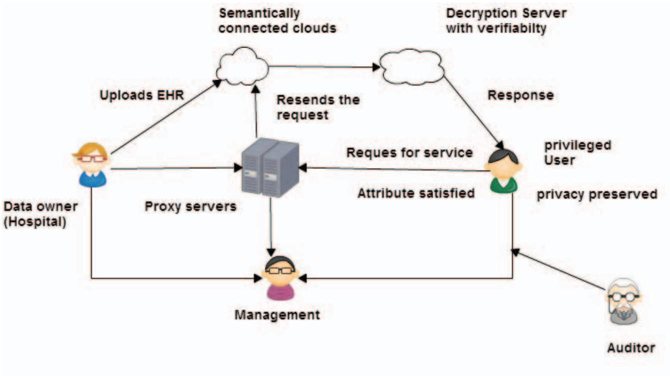

Fig. 1. Novel Framework for Health system using cloud.

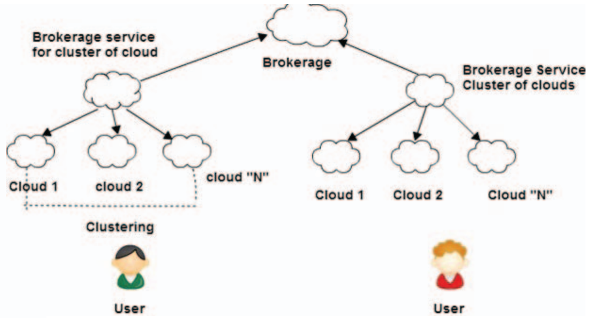
Brokerage service for cluster of cloud
Brokerage
Brokerage Service Cluster of clouds
Cloud 1
cloud 2
cloud "N"
Cloud 1
Cloud 2
Cloud "N"
Clustering
User
User

Fig. 2. Semantically connected cloud.

authorities (CSP). All the Hospitals in the region are connected to the cloud. Everything from storing the data to accessing the data are takes place in the cloud itself.

1) Data Owner: Data owner generally own the credible data. The credible data (PHR) of the patient are uploaded to the CSP associated with. Though the data belongs to patient, in this scenario, data owner is generally the hospital. The framework maintains the common account for the user. If the user visiting hospital for first time in his life time its the responsibility of the hospital to create a new account for the user otherwise the user data are uploaded to the existing account of the user. The responsibility of hospital includes creation of account and data storage. Firstly, the data are created with conditionally satisfied access structure the hospitals assigns the tag and uploads the data to the cloud directly or by using proxy servers. The data owner who uploads the data must follow multilevel biometric secure authentication using smart cards. Figure 1. explains the novel framework for health system and the way the data are being stored and shared among various users.

2) Semantically connected clouds: In order to utilize the resources effectively and provide better services the clouds are being connected. Its similar to Networks of Networks sometimes called as clouds of clouds or simply termed as Inter-cloud. Though it needs to maintain the common Service level agreements between the CSP it has many benefits. There are many cloud service vendors and the user are associated with any of the cloud. Using the concept of ontology the clouds are being grouped geographically and there will be an autonomic cloud brokerage service to facilitate information sharing among the clouds to users. The main objective of using semantic cloud is effective data sharing and resource allocation. By means of maintaining the single health records for the patients (user), the entire process takes place in cloud from registration to sharing and auditing. The common medical profile personal Health Record (PHR) of the patients is highly useful while making decision of treatments for patients by keep tracking various medication patient had underwent earlier. Moreover it will be highly benefited for PHR sharing to various organization by the patient. Its easier to track the details of the patient affected from the different disease and it will aid the researchers for future medications process. It also immensely helpful for disease prediction. As everything is stored in cloud and the data shared to Insurance companies it will reduce the fraudulent insurance agencies by means of monitorization by health sector and PHR acts as an evident. Motivation of proposed framework is from the paper, and it follows the architecture for cloud identification and data communication [6]. The figure.2 represents the structure of semantically connected cloud.

3) Privileged user: Once the hospital has created the account for the patients, the user provided with the access grants for accessing EHR. The access grants are provided to the user based on the attributes. The Privileged user request for the data in the cloud to view or share the content. Firstly, the user request to proxy server and it sends the request back to the cloud server and returns back the original data. Basically, cipher text are stored in the cloud, unless the attribute are satisfied access are not granted. The proxy server (decryption) takes in charge and decrypt the cipher-text to the user.

4) Proxy server: Proxy server are similar to original cloud server. Every time the user cannot use the original cloud server. The proxy server takes the responsibility. The proxy servers are used to verify the user attributes in the access structure and the transfers the request to the semantically connected cloud. It also used in decryption process and data sharing by the user. Proxy servers are also used by the management people (authorities) and for efficient user revocation and delegation.

5) Decryption server: The decryption of the data is being outsourced to another server by means of using proxy. The proxy server simply re-encrypt the data and once the user attributes are matched the user/data owner can decrypt the message. The size of the re-encrypted cipher-text is very less comparatively and it aids in lesser storage space and efficient sharing. The decryption message is being verified with the original cipher-text for the accuracy of data. The privacy of the user is being achieved as the cloud server doesnt know about the user needs and it simply re-encrypt and provide the response to the user.The diagram represents sharing of data using proxy servers.

6) Management: The people responsible for generating keys for storage and sharing up of data. There will be multiple authorities as they have multiple CSPs. Once again auditor is another third party. The auditor monitors and keep track the functionality are being operated as per the guidelines.Figure.3 represents the generic framework describes the various users and data owners associated with health systems.

IV. Preliminaries

The background of cryptography is necessary for attribute based access control techniques.

Bi-linearity: Let G be the independent group and G_T be the cyclic group.Then G$\times G \rightarrow G_T, \forall a, b \in G,\ and\ e, f \in G, e(a^e, b^f) = e(a, b)^{ef}$.Z$_p$ is the cyclic group of prime order P. Z$_p = \{0, 1, 2.....n-1\}$.

Non-degeneracy: e(a,b)$\neq 1$

Computability:$\forall\ a, b \in G, e(a, b)\ is\ computable.$

A. Access Structures:

Definition 1: Let P be the set of parties and ranges from $\{P_1, P_2, P_3.....P_n\}$ and by means of Bi-linear Diffie-Hellman Assumption(BDHA), $A \subseteq \left\{P_1, P_2, P_3.....P^{2n-1}\right\}$. The set $P \in A$ are called authorized sets, others are unauthorized.

Definition 2: The diffie-hellman is a bilinear decision algorithm used to check the symmetric parameters between the two groups G and G_T respectively. $e(a, b)^z$=$e(a, a)^{i,j,k}$ where i,j,k $\in$ Z$_p$ $\dot{\text{B}}$y assigning $\overrightarrow{y}_{a,\beta,h} = (a_1, a_2.....a_h, a_h +$ $2.....a_{2h})$ $\in$G^{2h-1} for random β $\in$Z$_p^*$ and an algorithm α outputs $\nu \in \{0, 1\}$.

$|\quad Pr[\alpha(a, b, \overrightarrow{y}_{a,\beta,h}, \widetilde{e}(g_{h+1}, b) = 1] - Pr[\beta(a, b, \overrightarrow{y}_{a,\beta,h}) = 1 \ |\geq \in$, simply we express it as $e(a, b)^z = e(a, a)^{\beta,h}$

B. Access policy

Definition 3:

Generally, access policy relates to granting the access to user. The value of data may be either 0 or 1.The values are in Boolean formula.ie. The access is granted or it not allowed. The access policy contains the additional privileges called wild card and denoted by w.$W = \{w^*, w^-, w^+......w^n\}$The wild card is used for classification of the departments. It might be denoted by considering the scenario where the access granted to hospital doctor.There might be n number of department. Firstly, it classifies departments based on the wild-card . Then, it follows to the access privilege tree. The access privilege tree for granting appropriate access depends upon the user attributes. For example:

$$p := (profession = docter)$$

$$\wedge(speciality = cardiology)$$

$$\wedge(designation = senior)$$

$$\wedge(organization = HospitalABC)$$

The access tree provides fine grained access to the data. The persons who have not satisfied the constraints cannot able to access data. Generally the access tree privileges has three main parts parent, child and leaf node. Every internal node acts as a threshold gate to the others. Usually the value of node =0 for OR Gate and 1 for AND Gate. As we discussed earlier, the access grants are Boolean values. The monotonic access structure needs to be converted.The value of the access privileges is calculated based on the attributes and converted to matrix form.

Definition 4: $\forall$P: $\{p_1, p_2......p_n\} \subseteq A, \exists\ matrix(V_i)$

with "i" columns and "r" rows.All the monotonic access can be converted to the linear secret sharing key.For all the elements in the universe there exist a secret key and the key is being transformed to user.

Initialization: There is a set U. $\forall\ elements \in U, \exists\ s \rightarrow U$. And there exists a functionality $f\left\{\gamma\right\}$, where "γ" is called security parameter.

[Setup:(γ, U)]The setup takes input from theU=p$_1, p_2.....p_i$, and outputs the Secret key and Master key.At first level there will be authorization by the trusted authorities.And the algorithm simply outputs the private key and Master key. The output of the $P_K = \left\{G_0, a, f_1 = a^{1/\alpha}, b = a^{\alpha_1}, f = a^{1/\beta_2}\right\}$ M$_k = \{\beta, a^\alpha\}$

Keygen:(PK,MK)

L$evel1\ :\ Authorization$: It is actually done by proxy servers.$A = \{a_1, a_2, a_3.....a_n\}$.The first level of authorization includes checking the security parameters and the attribute of the user.Once it is being verified it moves to the second level of authorization by the original cloud server.As the proxy server generates and verifies the attribute, the original cloud server work is being reduced.And the data being transferred by the proxy server makes easier for key sharing and delegation. The second level verification ensures the user are authorized person.Once the user are authorized , the cloud server randomly chooses the elements "r"$\in$Z$_p$. The polynomial interpretation between the two group takesplace and the secret key produced will be,

S$_k = \left\{a^{Ind}, A^r\right\}$

E$_u = a(a_u + r_u)/\beta$

E$_u = a^{ru^k} \cdot H\ (au^k_{i,j})^{ru^k}$

E$_{usr} = a^{\alpha + \sum_1^n au_(w) / \sum_1^n \beta_w, 1}$

Encryption(PK,MK,APT)

once the attribute are matched and next step is to encrypt the data.Firstly,our algorithm maintains constant cipher text and limited number of bi-linear pairing to reduce the complexity of the server.The lagranges co-efficient has used during this step.

$\triangle i, s = \prod j \in S, j \neq i\ x - j/i - j$ where i $\in$Z$_p$ and the element S $\in$Z$_p^*$

The output of this algorithm will be a Cipher= (APT, =M e(a,a)$^{\alpha s}, C = b^s$.

$\forall z^y \in z^y : \tilde{c}^y_z = h^{qx(0)_{y1,2}}$

Decryption(SK,CT,APT)

once the data are stored in cloud. Albeit, it is stored in the encrypted way the data are vulnerable to attacks and data leakages.Once the user request for the service, the proxy server authorizes the user.And it transfers the data to the semantic cloud.The customer request is handled by the single server and the request is being outsourced for decryption server.The storage size of the cipher text is less as we are partitioning the data into equal amount of size for maintaining the constant size of the data.Using proxy server, once again the cipher text is being re-encrypted to another cipher text without knowing the original data. The decryption server sends out the requested data to the user with verifiability.

C. Decryption steps include:

1) step1: compute the depth of the access tree and identify root and child nodes.

2) step2: Decryption of file K$_R = e(a,b)^{ru_i^w}.q_R(0) = e(a,b)^{ru_i^w}.\theta, i \neq 0$ by satisfying the access structure"W"

3) Step3: Compute: e(a,b)$^{au}X = \prod(e(C^w), E_u^k$

4) step4: compute=e(a,b)$^{a,\theta}$e(a,b)$^{a\theta}$ $= e(\prod_{w=1}^{w=n} C^w, E_{usr}/X$

The above steps will be performed by either owner of the data or the user who have privileges. In case, the data "M", needs to be transferred from one person to other either by the user nor by the data owner it needs to follow certain additional. The secret sharing of data. The data can be decrypted by the person who is not the owner nor user of the data.The ultimate objective of using semantic cloud and proxy is used here. The generated cipher-text is being transformed to another person by the owner, then

5) step 5: **Transformation key(PK,MK,CT)** It takes the input of the private key parameters, Master key for delegation of authorities of authorized sets.And the generated cipher text.The cipher-text is re-encrypts as follows,

$$T_k = e(C_1, Ke_1)/(\prod k \in A_i(e(C_1, k_0^1).e(k_{A_i}^1, E_1, i)).]$$

And finally it outputs

$$e(a,b)^{\alpha \in Z_P}$$

$$\forall\, C_T \in P, \exists\, T_k T_k = \sum_{T_1=1}^{T_n} e(a_1, a_2....a_n{-}1)^{\alpha}.e(b_1, b_2......b_n{-}1)$$

$$T_k = e(a,b)\prod_{\alpha_1}^{\alpha_n}$$

6) step 6: **verification of keys:**

$$\forall\ P \in A, \exists\, \{C_1, C_2.....C_n, E_{usr}\} \cdot \{T_1, T_2.....T_n, E_{usr}\}$$

The Ciphertext (C_1) has to be matched with the transformation key (T_1) for decryption of the data, otherwise it returns $\perp$.Thus the transformed key is being verified before it undergone decryption phase ie response to the user.

$$e(E_i, T_i)/e(E_i^1, T_x^1)$$

$$e(a,b)^{rq_x}0$$

User revocation: when the user has given the access to shared data which actually not own by him.ie sharing of data to another user like organization,relations etc.As soon as the data are viewed or accessed by the user his/her access grants has to be revoked.The revocation is done by proxy server by communicating with the semantically connected cloud. The user has no longer access to the service once the access grants are removed by the cloud server.These things are take care by the autonomic cloud so the data confidentiality is highly achieved. The user delegation were granted by cloud service authority for the limited time and particular data. article

V. Algorithm

Algorithm 1 explains the data sharing in our framework.The Data sharing is done by user.Here, jill shares the data to Ross which she doesn't have access.Firstly,jill shares the data.The CSP of the Jill , Domain authority generate the secret key to jill.The secret key needs to share with the ross.And the Rose is being authorized by the attributes.Jill and Rose has different CSP.The algorithm 2 explains about the decryption process.

Algorithm 1 Data sharing algorithm

```
procedure SEARCH FILES
    input
    output  ciphertext
                    $\tau \neq 0\ ie\ non-empty$
 $for\ each$ request $search\ Id$
     $for(i = 0; i < n; i++)$, then
    Output $Fid\ \ for\ each$ Fid $outputs\ respective\ ciphertext$
    Jill $generates\ the\ secret\ key\ for$ Rose
 $Domain\ authority\ generates\ the\ Access\ Grants$
 By respective CSP's
     $for(j = 0; i < n; j++)$,then
    Output  cloud server Transfer key to outsourced
 decryption server by step 6
    endfor
    endfor
end procedure=0
```

The **Algorithm 2** explains about the decryption process of our framework. Once the cipher-text are transferred, The proxy server will re-encrypt the data and finally by matching the transformation key the rose able to decrypt the data. The role of semantically connected cloud is to assign the proxy servers with nearest distance and assigning the sharing the cipher-text to freely available servers.As the semantic cloud are connected by means of geographic location, it easier to for brokerage service to delegate the service to the user. The single control authority like American health association will monitor the whole process by looking at the semantic cloud brokerage.

Algorithm 2 Decryption algorithm

```
procedure KEY MATCHING
    input  Access structures, key, ciphertext, transfer key.
    output  Message. $for\ each$ Ciphertext $there\ exist\ Id$
     $for(j = 0; j < n; j++)$, then
    Output  Re-rencrypt  Message
  $for\ each$ Fid $outputs\ respective\ ciphertext$
    Rose $utilize\ the\ secret\ key\ todecrypt$
 $DA\ of\ rose\ verifies\ the\ Access\ Grants$  By respective CSP's
    if  $the\ Tranfer\ key\ matches,\ then$
    Output  decryption server respnse with msg
```

```
        else Access Denied
        endfor
    endfor
end procedure=0
```

Our framework uses semantically connected because of following reasons. The two most important reasons are,

1) Every hospital has different cloud service providers and while sharing up of data either to another hospital or another organization or even to the insurance companies.As we discussed earlier there will be single account for the user and if the patient underwent the treatment in another hospital it records the all the data in both cloud storage. User might be subscribed to any other csp for data access.The user request are being transferred by connecting toe the nearest proxy server and the clouds are generally connected 2) Importantly, all the system are connected to Hadoop map-reduce for efficient clustering on cloud servers and it highly scalable and it reduces time and it finally reduces the complexity and power of datacenter.In order to obtain the all these above discussed benefits the semantically connected cloud with single control authority is needed.

VI. Experimental analysis

The experimental analysis of our proposed system were carried out in charm crypto system using python3.charm is a cryptographic library that integrates pairing based cryptography(pbc) and gcc libraries.These mathematical libraries are used for checking correctness of the policy or algorithm. By means of using python, coding were carried out in high level language and its easier to understand.we carried out experiment in laboratory of system having 2.1 Ghz intel processor with 8GB RAM and ubuntu 14.04.02 LTS.The results are seems to be fruitful.

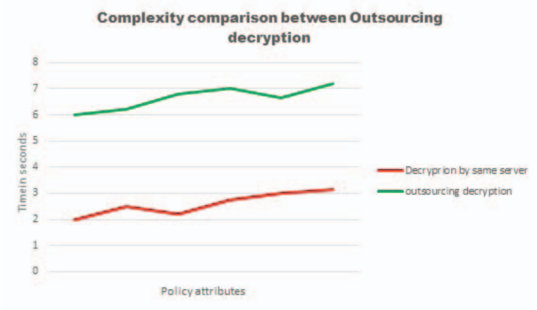

Fig. 3. Decryption by same server vs outsourced decryption in terms of complexity

The above figure illustrates time complexity between own server vs outsourcing decryption process to another server. Since it involves little bit overhead by means of transferring it to another server.The time complexity is higher when compared to decryption by own server.

VII. conclusion

Thus we have proposed a framework for cloud based health care.The enhancement of cipher text policy access control scheme has been made.The algorithm has been implemented using charmcryptosystem using python3.The experiment results shows it is efficient when compared to CP-ABE Scheme.

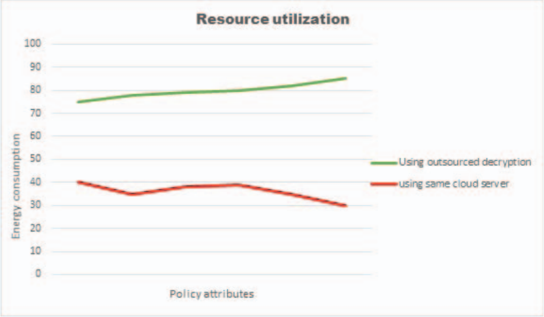

Fig. 4. Decryption by same server vs outsourced decryption in terms of resource utilization

References

[1] w. teng, G. Zhang, Y. Xiang, and D. Wang, “Attribute-based access control with constant-size ciphertext in cloud computing,” *Cloud Computing, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[2] N. S. Kumar, G. R. Lakshmi, and B. Balamurugan, “Enhanced attribute based encryption for cloud computing,” *Procedia Computer Science*, vol. 46, pp. 689 – 696, 2015, proceedings of the International Conference on Information and Communication Technologies, {ICICT} 2014, 3-5 December 2014 at Bolgatty Palace amp; Island Resort, Kochi, India. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S187705091500191X

[3] B. Balamurugan, P. Venkata Krishna, N. Kumar, and G. Rajyalakshmi, “An efficient framework for health system based on hybrid cloud with abe-outsourced decryption,” in *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, ser. Advances in Intelligent Systems and Computing, L. P. Suresh, S. S. Dash, and B. K. Panigrahi, Eds. Springer India, 2015, vol. 325, pp. 41–49. [Online]. Available: http://dx.doi.org/10.1007/978-81-322-2135

[4] B. Balamurugan, P. Venkata Krishna, L. Rajya, and N. Saravana Kumar, “Layered storage architecture for health system using cloud,” in *Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on*, May 2014, pp. 1795–1800.

[5] B. Balamurugan, P. Krishna, G. Rajya Lakshmi, and N. Kumar, “Cloud cluster communication for critical applications accessing c-mpich,” in *Embedded Systems (ICES), 2014 International Conference on*, July 2014, pp. 145–150.

[6] B. Balamurugan, N. S. Kumar, G. V. R. Lakshmi, and R. N. S. Shanmuga, “Common cloud architecture for cloud interoperability,” in *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, ser. ICTCS ’14. New York, NY, USA: ACM, 2014, pp. 10:1–10:6. [Online]. Available: http://doi.acm.org/10.1145/2677855.2677865

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *Security and Privacy, 2007. SP ’07. IEEE Symposium on*, May 2007, pp. 321–334.

[8] Z. Wan, J. Liu, and R. Deng, “Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 2, pp. 743–754, April 2012.

[9] J. Lai, R. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 8, pp. 1343–1354, Aug 2013.

[10] Y. A. Younis, K. Kifayat, and M. Merabti, “An access control model for cloud computing,” *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 45 – 60, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212614000222