Journal of Education for Pure Science- University of Thi-Qar
Vol.12, No2 (December, 2022)
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

DOI: http://doi.org/10.32792/utq.jceps.12.02.09

Improve Cloud Security By using Multi-Signature

Rana H. Hussain[1] Rasha B. Yousif[2] Abrar K. Sabah[3]

[1,2,3] Department of Computer Science, College of Computer Science and Mathematics, University of Thi-Qar, Iraq,

Received 18/05/2022 Accepted 21/8/2022 Published 01/12/2022

Abstract:

The problem of security in cloud computing is notorious. Several see data as safe only when it is managed in an internal network; others consider the cloud computing can provide the security necessary to ensure the preservation and integrity of information. Security problems in cloud computing come from two sides: the customer and the service provider, but the biggest load is always on the service provider. The purpose of the proposed system is to protect distributed data beyond to multi user on the cloud. Proposed system combination between Active broadcast encryption and multi-signature, so any user of cloud can distribute data among other secretly. After the practical application of the proposed algorithm, the results showed that it is more efficient and safer compared to the algorithms mentioned in the research and also helped reduce storage after canceling the unused accounts.

Keyword: broadcast encryption, cloud computing, multi-signature, security, healthcare.

1. Introduction:

The ancient was say “the need for is mother of invention”, the personal attention to cloud computing came after thinking of a safe solution to save important data, so that it is safe and easy to access from any device. The simplest way to achieve a basic understanding of cloud computing is to look at it as an application on the Internet and you can use it without having to know any technical details about it. In order to benefit from the services of cloud is to know your username and password. The cloud here is the same as the Internet itself. You will use the application with the same features as if it were loaded on your own computer. An additional advantage that makes this type of computing and its applications more attractive is that you can now use the application from all your mobile and non-mobile devices including smartphones, if you change it through one of these devices, you will find that it has been synchronized across all other devices [1].

Cloud computing means that computing is used as a service that is subscribed over the Internet and not as a product purchased and installed on a user's machine. Because it is a subscription service there are a large number of companies that provide this service and all its different conditions and types. There are companies that allow individuals or companies, for example, free storage space specified in the electronic cloud and in the case of the desire to increase them, they have several options, either monthly or annual subscription, or a one-time subscription as a license use, and there is a payment service according to use, Devices or programs and storage spaces are not fully activated [2].

These digital clouds can be public, so that any customer can access them through his subscription data, and may also be for a company and its employees, or it may be a hybrid between the two clouds (public and private), known as the Hybrid. A fourth type is the community cloud, which is used by groups with specific common characteristics and wants to communicate with each other and share resources across the network, such as educational, research or security communities[3,4].

2. **Healthcare and cloud computing**:

E-health technologies are expanding, and the future has many possibilities in this area. The virtual interest in the health sector is not a transient concern but it is serious and has the sole objective of facilitating the provision of health services, for example adopting electronic identity, A citizen in accordance with the law, which has been widely accepted, where patients are given so-called electronic identity cards, which alleviates and facilitates many of the issues and issues prevalent in the provision of health services [5]. The research cloud enables the doctor to come up with treatments that are appropriate for each patient individually after success with other patients complaining of similar conditions. To serve the "cancer research cloud", the Intel program, Trusted Trust Technology, in the first quarter of 2016, this allows servers to exchange encrypted data to maintain patient privacy. Medical records will be stored in a private and secure cloud service, allowing doctors to know full details of any medical condition of any condition, from anywhere [6,7].

On the other hand, a doctor's search for health information within a private electronic cloud will be like searching for a hotel on the Internet - transparency will help the doctor get the best information and treatments and thus speed and accuracy in treating patients[8].

Today clouds and networks are becoming the electronic walls on which scientific research projects are built, especially in the field of health, so that cloud computing provides a place for remote storage and access to huge sets of experimental data. Such collaborating, will create a global infrastructure for medical scientists studying how to treat some serious and intractable diseases by using networks. "These technologies can provide researchers around the world with free access to a large amount of data." Researchers are already able to exchange and share data and conduct large experiments on the development of various diseases that are difficult to diagnose, and know how to be and finally how to prevent them. The cost of maintaining electronic health technologies may also be beyond the reach of low-income countries [9,10,11]. So we suggest a system that reduces the cost and helps to share data through clouds and in a safe way.

3. Related works:

There are many studies to enhance the security in the cloud. Most of the previous studies have been devoted to building the Provable Data Possession (PDP). In [12] Focused on proving the ownership of the data for the client and also highlighting the weaknesses and strengths of this system. While [13] built an experimental model for (PDP) technology to store data in a collaborative manner in a multi-cloud environment. According to the results they obtained, an effective system at that time. Some of researchers depended on (KP-ABE) key-policy attribute-based encryption system, [14] propose a user crash prevention pattern which reserves the user's privacy when they work together with multiple establishments to obtain decryption identifications. [15] Improve system of [14] to avoid the linear attacks at present and achieves the user collision avoidance and reduce decisional bilinear Diffie-Hellman(DBDH) theory.in[16] try to overcome drawback of KP-ABE by proposed scheme(hybrid KC-ABE) which achieve fewer encryption and key generation time to increase an productivity of (KP-ABE).

While [17] Try to integrate (ODBE) technology with a group of signatures so that the user can anonymously share his data in the cloud and also reduce costs and increase security relatively.

4. Proposed Method:

This paper, combine the active broadcast encryption methods and group signature to arrive at secure distribution data especially to the new members in the cloud, give the data vendors to securely distribute data files among members that use the cloud resources. In order to avoid the problem of canceling the confidentiality of accounts from the canceled accounts in the active broadcast encryption method of transmission. This process will block the members with limited capacity and also constitute a load on the encryption method. To avoid this large problem, the Administrator group calculates the cancellation factor and transfers it to the cloud and makes it available. It is also the responsibility of the group to cancel or join the clients. The figure1 illustrates the proposed system design.

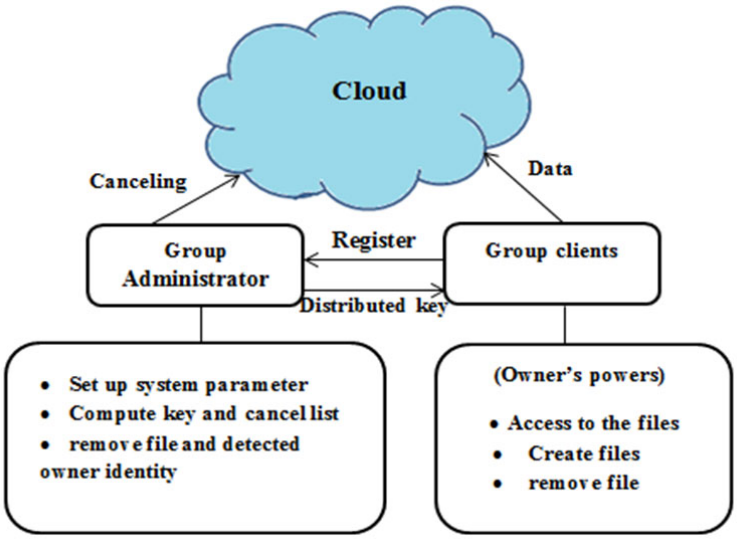

Fig.1. the proposed system architecture

At the beginning initialization the computer group administrators as following:

1. Construct bilinear map system K=(P, Q_a, Q_k,e)

1- Choose two qualitative element P, P_0 Є Qa with two qualitative numbers €1, €2 Є Z, then calculate the value of C= $€1^{-1}$ and D =$€2^{-1}$ PЄ Qa like €1.C = €2.M = P. Also, set of administrator P1= € 1 P0 and P2=€2P0є Qa.

2- Select two qualitative numbers J, O Є Qa and a amount of γ Є Z, then compute N= γ.J, D=γ. O and X=e(O,J),

3- Distributing the system factors: including (K, J, P, P0, P1, P2, C, D, N, M, X, f, f1, Enc()), where Enc(), f1 respectively are symmetric encryption algorithm and hash function {0, 1}*→Qa .

Note: group Administrator master key(F, $€1$, $€2$, γ)will be kept secret and f is a one way hash function {0, 1}*→Z.

4- Registration: selected a number xi ϵ Z and compute Ii, Ji via the following two equations to all member i in group Administrator :

$$I_i = \left[\frac{1}{(\gamma + x_i)}\right] J \in Q_a \qquad (1)$$

$$J_i = \left[\frac{x_i}{(\gamma + x_i)}\right] O \in Q_a \qquad (2)$$

After this process the set of Administrator will put these values into user list, then the user will own private key.

5- Cancelling operation occur through the set of Administrator complete a freely available canceling list , Table 1 shows the shape of cancelling list.

Table.1. Cancelling List

ID Group	I_1	X_1	T_1	J_1	Z_n	t_{RL}	Sign CL
	I_2	X_2	T_2	J_2			
	-	-	-	-			
	I_n	X_n	T_n	J_n			

Subsequently, the group Administrator puts (*Ii*, *xi*, IDi) into the user list. Then user *i* get a (*xi*, *Ii*, *Ji*) as a private key.

6- Generation data : set of user will perform the following steps to distributed its own data and store it in a cloud:

1- User sends the ID_{group} to the cloud. This will mean as request for cancelling list, so a cloud sends the cancelling list to user.

2- Check the validity of the sending cancelling list.

3- Select exclusive data identity ID_{data} , this can be done by two methods: find members are canceled or not. After this will encrypted the data, choose the qualitative number, compute hash function finally save all this in local storage and upload the data to the cloud after add the signature.

Algorithm 1: Generation the Signature:

Input: system parameter (J, C, D, P, N) Private Key (C, x) and data K.

Production: multi- signature on K.

Begin

Choose random numbers $\alpha,\beta,R\alpha,R\beta,Rx,R\delta1,R\delta2 \in Z$

Put $\delta1 = x\alpha$, $\delta2 = x\beta$

Computes the following values

$H1= \alpha*C$, $H_2 =\beta*D$, $H_3 = Ii + (\alpha + \beta)*P$

$L1= R_\alpha*C$, $L2= R_\beta*D$

$L3=e (L_3, J)tx\ e(P,N)-\gamma\alpha-\gamma\beta\ e (H,P)-\gamma\delta1-\gamma\ \delta$

$L4=Rx.H_1-R\ \delta_1.C$, $L_5=R.H_2-R\delta_2.D$

Put $c = f (K, H1, H2, H3, L1, L2, L3, L4, L5)$ *Then*

$S\alpha= C\alpha + R\alpha$, $S\beta= C\beta + R\beta$, $Sx= Cx + Rx$

$S\delta1 = R\ \delta1 + c$, $S\delta_2 = R\ \delta_2 + c$

Return $\sigma = (H_1,H_2,H_3,c,S\alpha,S\beta,Sx,S,S\delta_1,S\delta_2)$

End

Algorithm 2: signature confirmation.

Input: System factors (J, C, D, P, N, K) and

signature $\sigma = (H_1, H_2, H_3, c, S\alpha, S\beta, Sx, S, S\delta_1, S\delta_2)$

Output: True or False.

Begin

Compute the following values

$L1 = S\alpha * C - c * H_1$, $L_2 = S\beta * D - C * H_2$

$L3 = (e(H_3, N)/e(J, J))c\ e(H_3, P)Sx\ e(H, W)\text{-}S\alpha\text{-}S\beta$

$L4 = Sx.\ H_1\text{-}S\delta_1.\ C$, $L_5 = Sx.\ H_2\text{-}S\delta_2.\ D$

If $c = f(K, H1, H2, H3, L1, L2, L3, L4, L5)$

Return True

Else

Return False

End

Algorithm 3: Cancellation verification.

Input: System factor (P_0, P_1, P_2)*, a set of cancellation*

Keys $V_1 \ldots Vm$*, and a group signature* σ.

Output: allowed or Criminal.

Begin

Set temporary $= e(H_1, P_1)\ e(H_2, P_2)$

for $i = 1$ *to* m

If $e(H_3 - Ii, P_0) =$ *temporary*

Return allowed

End if

End for

Return Criminal

End

Algorithm 4: parameter computing.

Input: The canceled user factors $(U_1, x_1) \ldots (U_r, x_r)$,

And the private key of user partial (I, x).

Output: Or, r or Empty.

Begin

Set temporary = O

For $\mu = 1$ *to r*

If $x = x\,\mu$

Return Empty

Else

Set temporary $= O/(x - x\mu)\,(U\mu$ - *temporary)*

Return temporary

End

- **Data removing**: in case the owner of the Administrator group wants to delete a file from the cloud, they must get the (ID Data, C) from local storage. Then must compute the signature of the (ID Data, C) by using the Generation Signature algorithm .later send this Signature to the cloud to delete data requests. When the signature send to the cloud to check it and compute f(C). if the hash value is equal to the process of deletion will complete.
- **Data access**: access to the data that store in the cloud must perform these steps:
  · The user must be use the private key (,) and calculates the signature then sends it to the cloud to verify the authority of the signature.
  · The authority of data will check and calculate the key without interaction with the data owner. Which include three situations?
    1. If (T_{Data}< t1) this means no users are canceled before data was send to the cloud.
    2. If (Ti< T_{Data}< Ti+1) this means (i) users are canceled before the data was send to the cloud.
    3. If (T_R< Data) this means (R) users are canceled before the data was send to the cloud.

5. **Experiments and Performance Analysis:**

To test the proposed algorithms some setup steps are uses:

- The hardware side: hard disk 250 GB, RAM 4 GB and processor 4 GHz.
- The software side : windows and Ubuntu operating systems are used ,the programming language that used was Java with some libraries (miracle, GMP, PBC)
- The simulation consists of three factors (cloud, client and Administrator).

The user and Administrator do the operation on a laptop device. While cloud process is executed on a instrument that prepared with DDR3 RAM 8G, dual Core 4.3 GHz. Emulation process use, elliptic curve algorithm for 224 bit, which sends a feasible security scale with 2,048 bit RSA algorithm. To create a bilinear map to framework configuration use Pairing-based cryptography Library. Absolutely, utilize function pbc-demo and factors a.param with test header file in the sub-

directory of the Pbc Library to set group a pairing factors. Group A pairings obvious the symmetric bilinear pairings which are depended by the equation: $y^2 = x^3 + x$ through the domain F_p for several prime numbers q = 7 mod 11. The establish degree K is 4, and G_m is a sub-set of F_{p2}. The request p is specific prime component of q + 1. For secure employment, put q=1024 bit and p=224 bit, respectively. Moreover, the Enc() symmetric encryption done by using AES algorithm. For appropriateness, to save the other factors containing P, P0, P1 and U used distributing file.

Calculation Cost: Calculation cost of user and cloud is seeing acceptable, even if the totals of removal users are huge. Table 2 displays the totaling cost of multi- signature, ODBE and. ABE. Given the table show that totaling cost of multi- signature is actual acceptable than ODBE and ABE.

Table.2. Contrast is among and multi- signature, ABE and ODBE from calculation cost of client.

Technique	The Number of replaced users				
	0	20	40	60	80
	File Construction(200 MB)				
Multi-sign	1.52	1.502	1.504	1.507	1.503
ODBE	1.5	1.88	1.88	1.98	2.15
ABE	1.75	1.96	2.1	2	2.25
Multi-sign	**File Access (200 MB)**				
	1.2	1.15	1.15	1.15	1.25
ODBE	1.2	1.22	1.3	1.36	1.51
ABE	1.25	1.26	1.33	1.43	1.55
Multi-sign	**File Removal(200 MB)**				
	1.55	1.55	1.55	1.55	1.55
ODBE	2	2.11	2.3	2.4	2.5
ABE	2.75	2.86	3	3.03	3.15

The performance of the proposed system is evaluated by totaling cost and storage.

- **Storage**: Deprived of reduction of minimalism, configuration p = 224 and the components in Ga and Gm to be 163 and 2,024 bit, respectively. Also, assuming the size of the users, group and data will be fixed exclusivity 16 bits, which can returns about 216 records.

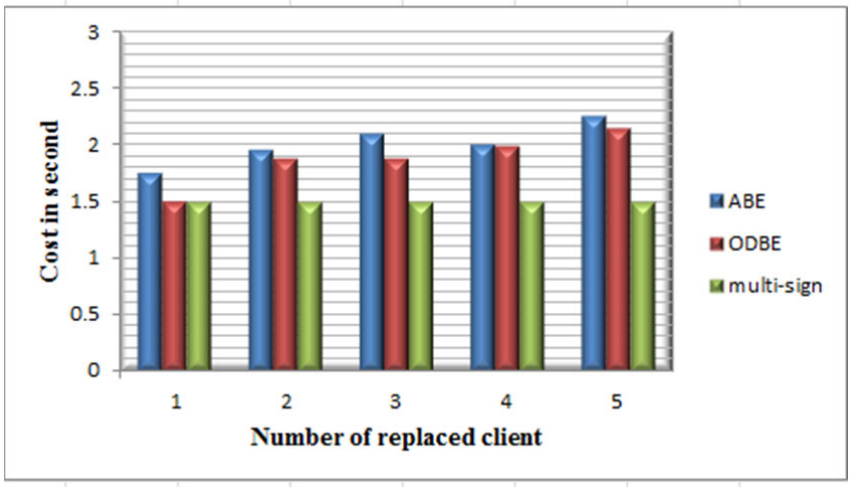

Fig.2. user calculation cost for file construction amongst multi- signature, ODBE and ABE.

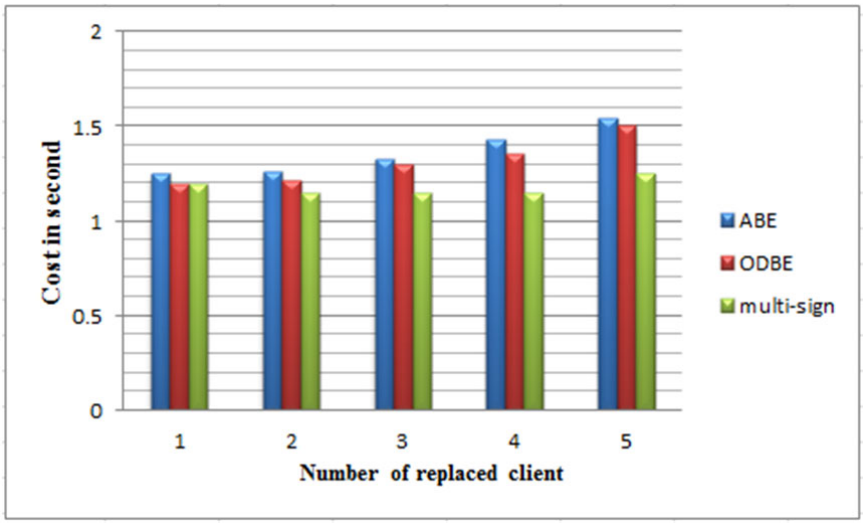

Fig.3. user calculation cost for file access among multi- signature, ODBE and ABE.

Fig.4. **user calculation cost for file cancelling among multi- signature, ODBE and ABE.**

- **Group Administrator:** the main private key of the group administrator in the proposed method, is (F, €1, €2, γ) Є Ga×Zq. Allowing for the proposed method with 300 users and

assuming that each user allocate normally 60 files. Note the distributed file and the user lists must be saved at the group administrator. The whole storage size of the group administrator is: $(88.125+44.125*200+2*10000)*10^{-3}$ =29.5 KB, this is acceptable.

- **Computation cost:** from the figures 2, 3, 4 observed valuations on cost of user's calculation for file construction process among the proposed method, ODBE, and ABE, the proposed method is irrelevant to the number of canceled users. While this cost growing with the number of canceled users in ABE and ODBE.
- **Group Memberships:** Eventually, in a proposed method each user needs more or less 60 bytes to save their private key (Ii, Ji, xi)Є Ga2×Zq. There be current a balance between the calculation and the storage overhead. e.g., when execute four pairing process the total storage of every user is nearly 572 bytes.

6. Conclusion:

The future has many necessary options in a cloud to use in the stock market and healthcare fields. This work concentrates on a secure and efficient distributing method to the data in a cloud. This can be done by using the proposed method which merges between two technologies (multi-signature and Attribute-Based Encryption). Besides, this will keep up the expert user removal and new user joining. In predominantly, user removal can be consummate a public cancellation list, without changing the pawned keys of the residual users and new users so the new user became truly coded the data's saved in the cloud earlier than their affiliation. Also, storing and encryption costs are stable. General examination displays that this suggested method justifies the desired protection and expertise as fully.

REFERENCES:

[1] Peter Mell, "What's Special about Cloud Security?," IT Professional , vol. 14, no. 4, pp. 6-8, July-Aug 2012.

[2] J. Grundy and A.S. Ibrahim M. Almorsy, "Collaboration-Based Cloud Computing Security Management Framework," in IEEE 4th International Conference on Cloud Computing, Washington, DC, USA, 2011, pp. 364-371.

[3] A.Gordon, "The Hybrid Cloud Security Professional," IEEE Cloud Computing , vol. 3, no. 1, pp. 82 - 86, Jan-Feb 2016.

[4] P.Dhamdhere and Y.Gajmal A.Markandey, "Data Access Security in Cloud Computing: A Review," in International Conference on Computing, Power and Communication Technologies (GUCON), Galgotias University, Greater Noida, UP, India, 2018, pp. 633-636.

[5] A.i Maulana and Asfiyan, "Design of Cloud-based and IPTV Digital Signage System System," TELKOMNIKA, vol. 16, no. 1, pp. 385-389, February 2018.

[6] I.M.Murwantara, et al., "Towards Adaptive Sensor-cloud for Internet of Things," TELKOMNIKA, vol. 16, no. 6, pp. 2771-2781, December 2018.

[7] A. Bhawiyuga, et al., "Architectural design of IoT-cloud computing integration platform," TELKOMNIKA, vol. 17, no. 3, pp. 1399 -1408, June 2019.

[8] Arokia Paul Rajan R, "A review on serverless architectures - function as a service (FaaS) in cloud computing," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no. 1, pp. 530-537, February 2020.

[9] Iqbal Ahmed, "A brief review: security issues in cloud computing and their solutions," TELKOMNIKA, vol. 17, no. 6, pp. 2812-2817, December 2019.

[10] Iqbal Ahmed, "Technology organization environment framework in cloud computing," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no. 2, pp. 716-725, April 2020.

[11] B.Ayyoub, et al., "A proposed cloud-based billers hub using secured e-payments system," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 19, no. 1, pp. 339-348, February 2021.

[12] R. Ibrahim and N. A. Abu Bakar M. T. Amron, "Cloud computing acceptance among public sector employees," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 19, no. 1, p. 124~133, 2021 February.

[13] M.Bahrami and M. Singhal, "A Dynamic Cloud Computing Platform for eHealth Systems," in IEEE 17th International Conference on e-Health Networking, Applications and Services (Healthcom): Short and Demo Papers, Boston, MA, USA, 2015, pp. 435-438.

[14] Lo'ai A. Tawalbeh and S. Habeeb, "An Integrated Cloud Based Healthcare System," in Fifth International Conference on Internet of Things: Systems, Management and Security (IoTSMS), Valencia, Spain, 2015, pp. 268-273.

[15] G. Sirisha and A.M.Reddy Ch.Reddy T, "Smart Healthcare Analysis and Therapy for Voice Disorder using Cloud and Edge Computing," in 4th International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Mangalore, India, India, 2018, pp. 103-106.

[16] D. Kumar and S.K. Khatri I. Singh, "Improving The Efficiency of E-Healthcare System Based on Cloud," in 2019 Amity International Conference on Artificial Intelligence (AICAI), ubai, United Arab Emirates, United Arab Emirates, 2019, pp. 930-933.

[17] V.Casola, et al., "Healthcare Related Data in the Cloud:Challenges and Opportunities," IEEE Cloud Computing, vol. 3, no. 6, pp. 10-14, Nov.- Dec. 2016.

[18] H. Jemal, et al., "Cloud Computing and Mobile Devices Based System for Healthcare Application," in 2015 IEEE International Symposium on Technology and Society (ISTAS), Dublin, Ireland, 2015, pp. 1-5.

[19] Suguna.M, et al., "A Survey on Cloud and Internet of Things Based Healthcare Diagnosis," in 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, India, 2018, pp. 1-4.

[20] Pooja Natu et al, "A Comparative Analysis of Provable Data Possession Schemes in Cloud," (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, no. 6, pp. 7927-7931, November - December 2014.

[21] V.Kollaand P R. Rao H. Katta, "Scalable and Efficient Provable Data Possession," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 9, pp. 3374-3377, september 2013.

[22] P. Liang, and Y. Mu L.Zhang, "Improving Privacy-Preserving and Security for Decentralized Key-Policy Attributed-Based Encryption," JOURNAL OF LATEX CLASS FILES, vol. 14, no. 8, pp. 1-10, AUGUST 2015.

[23] You and L. Wang, "Hierarchical Authority Key-Policy Attribute-Based Encryption," in *IEEE 16th International Conference on Communication Technology (ICCT)*, Hangzhou, China, 2015, pp. 868-872.

[24] and P.VijayaKarthik Sangeetha.M, "To provide a secured access control using combined hybrid Key-Ciphertext Attribute based encryption (KC-ABE)," in *IEEE INTERNATIONAL CONFERENCE ON INTELLIGENT TECHNIQUES IN CONTROL, OPTIMIZATION AND SIGNAL PROCESSING*, Srivilliputhur, India, 2017, pp. 1-4.

[25] G.B.V.PADMANADH P.L.DEVI, "Dynamic Broadcast Encryption Techniques for Groups in the Cloud," *International Journal of Scientific Engineering and Technology Research*, vol. 3, no. 31, pp. 6257-6262, October,2014.