Achieving secure and scalable DAC in cloud computing using DLE with load balancing

[1]A.SYED ISMAIL
Department of computer science and engineering
PERI institute of technology, Anna University
Chennai, India
ismail_syed14@yahoo.com

[2]A.REVATHI
Department of computer science and engineering
PERI institute of technology, Anna University
Chennai, India
arevathi@gmail.com

***Abstract*— It is the style of computing as the different user can access the resource over the internet throughout the world .It can be used for both small and large organization. In cloud computing, security is a key issue. In cloud environment the data owners are having the responsibility of encrypting the data before upload into the cloud & re-encrypting the data whenever the authentication policies change. Data owner is highly affected for communication & computation cost. So based on double layer encryption we can limit the communication & computation cost. In this method we are going to decompose the access control policies ACP's into two ways. They are single ACP's and sub ACP's,the first way is one part of the encryption will be done by the owner and the other part of sub ACP's encryption will be done by the cloud. Here the main thing those who want to access the data the attribute will be checked then only it allows to access the data and here we are going to introduce the load balancing method by this method the data will be stored in the bucket, here bucket is nothing but the storage medium in the cloud. By using this method we can easily store and retrieve the datas quickly and it saves the time consumption.**

***Index Terms*—cloud, security, double layer encryption, ACP's, load balancing**

1 INTRODUCTION

Privacy and security are the two major concerns in the adaption of cloud computing for data storage .In current system the ACP's are encrypted by different symmetric keys and it is distributed to users. In this method we are facing a several problems.

The owner does not keep a copy of data. If the ACP's change the owner needs to download & decrypt the data. The owner again distributes the key to the user for encrypting the data to upload in the cloud. The owner needs to establish the private communication to the user for the purpose of issuing a new key. Hence we proposed an approach based on broadcast key management schemes (BKM) by this method we introduce the double layer encryption method, in this method whenever the user credential change the data will not be send to the owner the cloud it encrypt the data again but only the inner layer, the other layer (i.e.) the outer layer will be encrypted by the owner only. So there is no private communication among the user and owner. The cost will be reduced for computation cost.

1.1 Single layer Encryption & Double Layer Encryption

Single layer encryption approach, the data owners control the access through the encryption But it is having some limitations (i.e.) the data owner should be enforce all the ACP's after the users are added or removed.

All the encryption work will be done by the owner that incurs high communication & computation cost *(ex)* if the ACP's change, the owner must download the data from the cloud, generate a new encryption key and re-encrypt the downloaded data with the new key and then upload the re encrypted data to the cloud. Now we are going to proposed an approach called DLE (double layer encryption).In this DLE method is how to decompose the ACP's.So that ABAC enforcement can be delegated to the cloud.

In order to delegate as more access control enforcement as possible to the cloud. In this approach all ACP's are decomposed to two sub ACP's .The double layer encryption should be performed such that the data owner should be encrypt the first ACP's the cloud re-encrypts the encrypted data using the remaining set ACP's.

1.2 In this double layer encryption there are several advantages

When the policies or the user credential changes the inner layer encryption will be performed in the cloud. Here there is no transmission required between data owner & cloud. In this cloud service we are using a broadcast key management scheme. In this scheme the actual keys are not distributed to the user.

2 BROADCAST ENCRYPTION

It is used to make a message efficiently encrypted. There are two users are to be mentioned as follows:-

(i)Authorized users (privileged users)
(ii)Revoked (non- authorized users)

2.1 Authorized users *(privileged users)*: The privileged users only decrypt the encrypted message. They only having all the rights to decrypt the messages which have been retrieved from the cloud.

2.2 Revoked *(non- authorized users)*: The non authorized users cannot be able to decrypt. There are two approaches

stateful users and stateless users. In the stateful users approach the new user or the existing user change the keys are updated. In the stateless approach the key given to the users cannot change but it will be omitted.

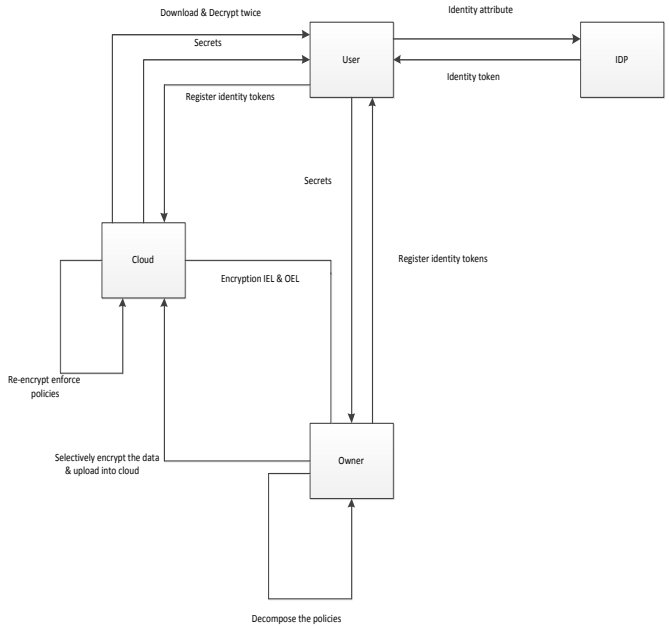

Fig.1: Architectural diagram

3 OVERVIEW

The overview of our solution to the problem in DAC is outsourced data in the cloud the detailed description is given in sec 1.1, the DLE encryption consists of the four blocks User, IDP, Owner and cloud. This Double layer enforcement allows to reduce the load on the owner, it provides a better way to handle the data updates, user dynamics and policy changes. Apart from that here load balancing is an additional one to host the data and retrieve the data from the cloud. Figure 1 shows the system diagram of the DLE approach.

3.1 Token issuance: The tokens are issued to the users by their identity attributes. By this identification the tokens are to be issued if there attribute was mismatch the tokens will be rejected.

3.2 Decomposition policies: Here all the ACP's are decomposes into sub ACP's to limit the number of attributes & for assure the confidentiality of the data from the cloud.

3.3 Token registration: The users are register their identity tokens to obtain the secrets to decrypt the data that they allowed to access .The users can register into the owners sub ACP's the balance identity tokens are with the cloud in privacy manner.

3.4 Encryption and uploading: The owner encrypt the data based on their sub ACP's and upload them with BKM algorithm & remaining ACP's into the cloud.BKM at the cloud takes the secret which they are issued to the user and sub ACP's which are given by the owner.

3.5 Data downloading & encryption: Users download the encrypted data from the cloud & decrypt the same by using keys. The users are decrypt the data twice (i.e.) one for remove encryption layer added by the cloud and another by the owner.

3.6 Encryption evolution management: The ACP's or user credentials may change, by this process the encrypted data may go for frequent updates. So that the data already encrypted must be re-encrypted with a new key. The cloud that performs the re-encrypts the affected data only without the intervention of the owner.

3.7 Policy decomposition: The policy decomposition has to manage all the authorizations when ACP's change. The cloud is not trusted for the confidentiality of the data. So the owner was initially encrypt the data into the cloud to avoid re-encryption by the owner the data may have to encrypted again by DLE.In this decomposition method the data have to be encrypted again with two encryption layers
(i)OEL-outer encryption layer
(ii)IEL- Inner encryption layer

3.7.1 IEL (Inner encryption layer): it assures the confidentiality of the data and it is respected to the cloud, which is generated by the cloud. For the user credential the security will be updated in the server for that purpose the whole system get encrypted but it will take lots of communication cost so the inner layer encryption will be done by cloud.

3.7.2 OEL (outer encryption layer): It is for authorization to controlling accesses to the data by the users & it is generated by the owner. for the user credential the security will be updated in the server for that purpose the whole system get encrypted but it will take lots of communication cost so the outer layer encryption will be done by the data owner.

4 LOAD BALANCING

It is the method to distribute workload across the computers, CPU, Network link & or other resources. It is to achieve the optimal utilization & maximize throughput .It minimize the response time & avoid the overload. In the load balancing there are two general algorithms:-
(i) How load are distributed & how the processes are allocated to the nodes (system load)
(ii)Status of the nodes (system topology)

4.1 In the system load: It is classified as *centralized and distributed load*

4.1.1 Centralized: Single node is responsible for managing the distributed system. In this system the single node will be distributed for whole system and simultaneously this node is responsible to control the system load.

4.1.2 Distributed system: Each node manages the single distribution system. Same here the whole distribution system load is controlled by each node. Here multiple nodes are present for each system.

4.2 System topology

4.2.1 Static approach *(design and implementation)*:This approach is related to design oriented once we develop a project it must be implemented by using a several test and only the successful project will be counted.

4.2.2 Dynamic approach *(current state of the system during load balancing)*:If we want to balancing the load the data must be separated in the sequential manner if the datas are overflow we can't able to balance, for that purpose we are going to balance the load whenever we are uploading the datas.

4.2.3 Scalability: The ability of an algorithm for performing load balancing, a system with any number of nodes. If the node was more we can't able to balance but accidentally the nodes will be overflow, to limit the overflow of data we must to be careful when uploading the datas.

4.2.4 Performance: It is used to check the efficiency of the system. If the system performance was poor the total system get fault. So whenever the system performance goes beyond the minimum level it should be maintained. Hence the performance ratio will be become higher.

4.2.5 Response time: The total amount of time should be taken for responding a particular load balancing algorithm in distributed computing. Because the time which has taken for searching the data must be important, if the data searching is delay means the total performance get poor, for this purpose the responding time will be an important.

5 ALGORITHMS

5.1 Round robin algorithm: In this algorithm all the processes are divided between all the processors each are assigned in a round robin order. In this the work load distribution is same but the times for different processes are not same. At any point of time some nodes may be heavily loaded and others remain idle. It is mostly used in web servers

5.2 Equally distributed data load balancing algorithm: It handles priorities against the request. It will check not only the balanced manner but also check the variable of each data centre occupy in cloud. So by this way the load is equally distributed even not only improves performance also reduce the time delay. We can easily store and retrieve the datas.

6 CONCLUSIONS

In current approaches the outsourced data is using selective encryption that require organizations to manage all the keys and to respect the load it will be exceed in any nodes so the time also take delay. Hence we introduce the double layer encryption method whenever the user credentials change the owner will encrypt the outer layer & cloud changes the inner layer encryptions. The computational cost will be less. Here there is no private communication between users and the owner, if the encryption changes in the cloud.

In this proposed system additionally we are introducing the load balancing method to distribute the work load across the *computers, CPU, Network link and other resources.* By using this method we can minimize the time delay and performance increasing. In future work we plan to encryption & decryption will be done by cloud itself. Once the owner uploads the data, the cloud encrypts the data and stored it in the system equally in their allocated buckets. If the user credentials change the encryption also change but the encryptions will be automatically update in the cloud itself.

REFERENCES

[1]M. Nabeel and E. Bertino, "Privacy preserving Delegated access control in public clouds," IEEE Transactions on Knowledge and Data Engineering, 2012.

[2] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEE International Conference on Information Reuse and Integration(IRI), 2012.

[3]G.Miklau and D. Suciu, "Controlling access to published data using cryptography," in VLDB '2003: Proceedings of the 29th international conference on Very large data bases.VLDB Endowment, 2003, pp. 898909.

[4]M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Transactions on Knowledge and Data Engineering, 2012

[5] D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases, ser. VLDB'07. VLDB Endowment, 2007, pp. 123-134.

[6] M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA,2011.

[7] D. Naor, M. Naor, and J. B. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO'01. London, UK: Springer-Verlag, 2001, pp. 41-62.

[8] M. Nabeel and E. Bertino, "Attribute based group key management," IEEE Transactions on Dependable and Secure Computing, 2012.

[9] A. Shamir, "How to share a secret," The Communication of ACM, vol. 22, pp. 612-613, November 1979.

[10] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09. New York, NY, USA: ACM, 2009, pp. 276-286.

[11] J.-M. Do, Y.-J. Song, and N. Park, "Attribute based proxy reencryption for data confidentiality in cloud computing environments," in Proceedings of the 1st International Conference on Computers, Networks, Systems and Industrial Engineering. LosAlamitos, CA, USA: IEEE Computer Society, 2011, pp. 248-251.

[12]Amandeep Kaur Sidhu, Supriya Kinger "Analysis of Load Balancing Techniques in Cloud Computing,"International Journal of Computers & Technology, Volume 4 No. 2, March-April, 2013, ISSN 22773061

[13] A. M. Alakeel, "A Guide to dynamic Load balancing in Distributed Computer Systems", International Journal of Computer Science and Network Security (IJCSNS), Vol. 10, No. 6, June 2010, pages 153-160.
[14] Y. Fang, F. Wang, and J. Ge, "A Task Scheduling Algorithm Based on Load Balancing in Cloud Computing", Web Information Systems and Mining, Lecture Notes in Computer Science, Vol. 6318, 2010, pages 271-277.
[15] Zenon Chaczko, Venkatesh Mahadevan, Shahrzad Aslanzadeh, Christopher Mcdermid (2011)"Availability and Load Balancing in Cloud Computing" International Conference on Computer and Software Modeling IPCSIT vol.14 IACSIT Press,Singapore 2011.