IJARES/October 2014/Volume-2/Issue-10/1686-1690 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

IMPLEMENTATION OF PROSPECTIVE ACCESS CONTROL IN CLOUD SYSTEM

Shaik Mahammad Sharief[1], Rambabu Pemula[2]

[1]**M.Tech Student, Dept of CSE, Nimra Institute of Engineering & Technology, Ongole, A.P, India**

[2]**Assistant Professor, Dept of CSE, Nimra Institute of Engineering & Technology, Ongole, A.P, India**

ABSTRACT:

Use of conventional encryption approaches is not satisfactory to maintain the enforcement of fine-grained organizational access control policies. Two layer of encryption was put forward reducing the overhead sustained by the owner all through initial encryption and subsequent re-encryptions. An essential concern in the approach of two layer of encryption is the way of handling out the encryptions among the cloud and the owner. The owner initially encrypts the information in the phase of data encryption and uploading, on the basis of owner's sub access control policies consecutively to conceal the content from the cloud. By usage of partial associations among access control policies, computing costs were planned to be reduced and substitute alternatives for two layers of encryption approach were planned. The time of running at the owner is inferior when compared to the approach of single layer encryption, in view of the fact that the approach of two layer of encryption divides the cost of enforcement among the owner and the cloud.

Keywords: Two layer of encryption, Access control policies, Owner, Data encryption, Cloud.

1. INTRODUCTION:

By employing of traditional encryption, data confidentiality against cloud was secured and is not satisfactory for managing of access control policies concerning fine-grained organizational enforcement. From cloud, in order to assure privacy, the owner decomposes each access control policy into at most two sub access control policy such that the owner put into effect the least

number of attributes [1]. Computing costs were planned to be reduced by making use of partial associations among access control policies and the substitute alternatives for the two layers of encryption approach were planned. Employing of cloud storage for selective allocation of data between the users is a vital requirement for high-assurance security and confidentiality of data and attribute based access control supports over encrypted data. Cloud performs delayed encryption all through convinced dynamic circumstances as the cloud manages the keys of outer encryption layer and encryptions. The owner and the cloud cooperatively enforce access control policies on the other hand, unlike the approach of single layer encryption, by means of performing two encryptions on every data item and this two layer enforcement permits one to decrease the load on the owner and delegates greatly duties of access control enforcement as probable to the cloud [2][3]. Two layer of encryption was put forward reducing the overhead sustained by the owner all through initial encryption and subsequent re-encryptions. The data owner performs a coarse grained encryption upon the data to facilitate the assurance of the data privacy from the cloud.

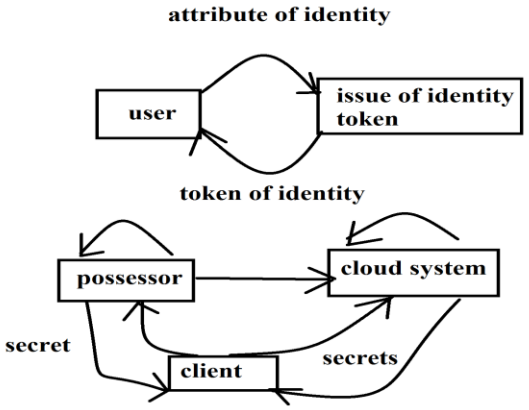

Fig1: Representation of two layer of encryption

2. METHODOLOGY:

In the direction of encrypting all data items by means of using a single symmetric key there are potential extremes for owner and allow the cloud to carry out the entire related encryption of access control. An option is based on decomposing access control policy with the intention that the risk of information disclosure and key management transparency are balanced. The difficulty is then how to go off the access control policy such that the owner has to administer the least amount of attributes although delegating as much enforcement of access control as possible towards the cloud devoid of permitting it to decrypt the information. By the user identity attributes, the confidential information has to be regularly

encoded and as a result be strongly defended from the cloud. The cloud carries out fine grained encryption over the encrypted data offered by data owner based on the access control policies granted by the data owner. By making use of the two layer of encryption can lessen the overhead of the owner and extensive simulation results show that the approach decomposes the access control policies. To implement the access control policies during the addition or removal of identity attributes and the owner has no need to re-encrypt the data because the essential re-encryptions were performed by the cloud and consequently the two layer of encryption approach reduces the overhead of computation and communication at the owner [4]. By the data owner, a broadcast key management scheme was utilized and the cloud service whereby the actual keys do not necessitate to be distributed to the users. Cloud merely re-encrypts the data that is affected lacking the interference of the owner; as the cloud carries out the access control implementing encryption. An essential concern in the approach of two layer of encryption is the way of handling out the encryptions among the cloud and the owner. The owner initially encrypts the information in the phase of data encryption and uploading, on the basis of owner's sub access control policies consecutively to conceal the content from the cloud [5]. In addition to subsequent re-encryptions, the approach of two layer of encryption lessens the transparency incurred by the owner for the duration of the initial encryption. The system of the two layer encryption approach was shown in fig1. There are four entities in the system of the two layer of encryption such as: owner, user, identity token issuance and cloud. In the approach of two layer of encryption, the time of running at the cloud is superior to that at the owner in view of the fact that the cloud performs encryption of fine grained while the owner only carries out coarse grained encryption. By means of the derived keys in the phase of data downloading and decryption, users download encrypted information from the cloud and decrypt the information. The privacy related sub access control policy were made compulsory by the owner and the cloud put into effect the enduring sub access control policies. The time of running at the owner is inferior when compared to the approach of single layer encryption, since the approach of two layer of encryption divides the cost of enforcement among the owner and the cloud. The

approach is intended for the cloud and owner to carry out the entire access control related encryption double has the slightest overhead for the owner as he does not supervise any attributes and carry out related encryption of fine grained access control and the approach has the uppermost information disclosure risk appropriate to collusions among the cloud and the users as one malicious user revealing the encryption key of reveals all sensitive information to the cloud. The approach has the smallest amount of information disclosure risk due to collusions since the fine grained access control is imposed in the initial encryption. It has the uppermost transparency on the owner as he has to carry out the similar job at the start as in the single layer of encryption approach and, additionally, desires to administer all attributes of identity. Based on identity elements in phase of Identity token issuance, the issue tokens of identity to users were issued [6].

3. RESULTS:

The time of running at the owner is inferior when compared to the approach of single layer encryption, in view of the fact that the approach of two layer of encryption divides the cost of enforcement among the owner and the cloud. In this approach, the cloud gain knowledge of access control policies. At the outlay of defence and confidentiality, the developments in the performance arrive. The owner does not encompass to re-encrypt the information since the cloud performs the essential re-encryptions to put into effect the access control policies, when identity attributes are added or disconnected or the owner modernizes the cloud's access control policies. The transparency incurred by the owner was lessened by the approach of two layer of encryption for the duration of the initial encryption besides following re-encryptions. For the most part of the tasks of key management are performed by means of the cloud and the owner holds only the conditions of negligible set of attribute. As the cloud performs encryption of fine grained while the owner only carries out coarse grained encryption, the time of running at the cloud in the approach of two layer of encryption is superior to that at the owner.

4. CONCLUSION:

In the direction of encrypting all data items by means of using a single symmetric key there are potential extremes for owner and allow the cloud to carry out the entire related encryption of access control. The privacy

related sub access control policy were made compulsory by the owner and the cloud put into effect the enduring sub access control policies. For the most part of the tasks of key management are performed by means of the cloud and the owner holds only the conditions of negligible set of attribute. An essential concern in the approach of two layer of encryption is the way of handling out the encryptions among the cloud and the owner. The owner initially encrypts the information in the phase of data encryption and uploading, on the basis of owner's sub access control policies consecutively to conceal the content from the cloud. Two layer of encryption was put forward reducing the overhead sustained by the owner all through initial encryption and subsequent re-encryptions. The owner and the cloud cooperatively enforce access control policies on the other hand, unlike the approach of single layer encryption, by means of performing two encryptions on every data item and this two layer enforcement permits one to decrease the load on the owner and delegates greatly duties of access control enforcement as probable to the cloud.

REFERENCES

[1] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, ser. CollaborateCom '11, 2011, pp. 172–180.

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

[3] S. 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.

[4] 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.

[5] A. Fiat and M. Naor, "Broadcast encryption," in Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '93. London, UK: Springer-Verlag, 1994, pp. 480–491.

[6] 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.