International Journal of Grid Distribution Computing
Vol.7, no.3 (2014), pp.163-166
http://dx.doi.org/10.14257/ijgdc.2014.7.3.16

Defending of Trusted Access Control in Cloud Computing

Venkata Naresh Mandhala[1], Siva Koteswara Rao Chinnam[2] and Tai-hoon Kim[3*]

[1]Information Technology Department, VFSTR University,Vadlamudi-522213, Guntur, India
[2]Information Technology Department, VFSTR University, Vadlamudi-522213, Guntur, India
[3]Department of Convergence Security, Sungshin Women's University, 249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea
[1]mvnaresh.mca@gmail.com, [2]csrvictory@gmail.com, [3]taihoonn@daum.net

Abstract

The privacy of the information against the cloud was assured by the technique of encryption and the usage of approaches of conventional encryption is not enough to hold up the access control policies of fine-grained organizational enforcement. Throughout the initial encryption and subsequent re-encryptions, scheme of two layer of encryption was developed that diminishes the overhead sustained by the owner. During the addition or removal of identity attributes the owner has no need to re-encrypt the data since the essential re-encryptions were performed by the cloud to implement the access control policies and consequently the two layer of encryption approach reduces the overhead of computation and communication at the owner. 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.

Keywords: *Encryption, Fine-grained access policy, Two Layer of Encryption, Identity Attributes*

1. Introduction

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 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 [4]. By the technique of encryption and the usage of approaches of conventional encryption, the privacy of the information against the cloud was assured and is not enough to hold up the access control policies of fine-grained organizational enforcement [8]. To have right to use the data, numerous organizations have nowadays access control policies modifying of users and these are frequently articulated in terms of the identity attributes, making use of languages of access control and they are referred to as attribute based access control that sustains access control of fine grained which is essential for high-assurance data protection and confidentiality [1]. 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

[*] Corresponding Author

ISSN: 2005-4262 IJGDC

the load on the owner and delegates greatly duties of access control enforcement as probable to the cloud [7, 12]. The fine-grained access control was maintained by the scheme of attribute based access control which supports over encrypted data and to make use of the cloud storage intended for selective allocation of data between the users is a vital requirement for high-assurance security and confidentiality of data [15]. Throughout the initial encryption and subsequent re-encryptions, scheme of two layer of encryption was developed that diminishes the overhead sustained by the owner. By means of utilizing partial associations among access control policies, the computing costs were further planned to be reduced and the substitute alternatives for the two layers of encryption approach were planned [2]. 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. As the cloud manages the keys of outer encryption layer and encryptions, the cloud has the prospect to carry out delayed encryption all through convinced dynamic circumstances [10]. 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. The owner of the data executes a coarse grained encryption upon the data to facilitate the assurance of the data privacy from the cloud under the scheme of two layer of encryption [14]. 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.

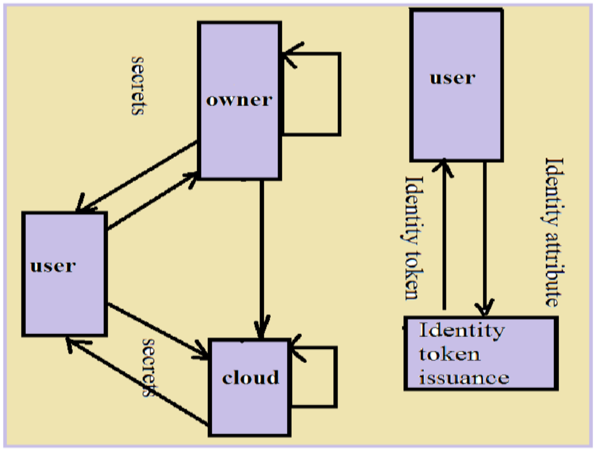

Figure 1. Representation of Two Layer of Encryption

2. Methodology

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. There are four entities in the system of the two layer of encryption such as: owner, user, identity token issuance and cloud [6]. 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. To guarantee privacy of data from the cloud in the phase of Policy decomposition, 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 [11]. The system of the two layer encryption approach was shown in fig1. On the basis of their identity elements in the phase of

Identity token issuance, the issue tokens of identity to users were issued. With the intention of getting hold of secrets to decrypt the information that they are approved to access in the Identity token registration phase, users record their tokens of identity. 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 [3]. Along with the public information produced by means of the algorithm of attribute based group key management subsequently uploads them all and the outstanding sub access control policies to the cloud. 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 [5, 13]. 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 [9]. 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. 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. There are two potential extremes such as the initial approach is intended for the owner towards encrypting all the items of data by means of using a single symmetric key and allow the Cloud to carry out the entire related encryption of access control. The subsequent approach is intended for the cloud and owner to carry out the entire access control related encryption double. The approach 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 updates of inner encryption layer necessitate re-encrypting all the items of data. The subsequent 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. 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.

3. Results

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 and. 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 defense and confidentiality, the developments in the performance arrive. 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. In view of the fact that 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. 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.

4. Conclusion

Performing of two encryptions on every data item permits one to decrease the load on the owner and delegates greatly duties of access control enforcement as probable to the cloud. 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. 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. The owner of the data executes a coarse grained encryption upon the data to facilitate the assurance of the data privacy from the cloud under the scheme of two layer of encryption.

References

[1] J. Camenisch, M. Dubovitskaya and G. Neven, "Oblivious transfer with access control", CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. NewYork, NY, USA: ACM, **(2009)**, pp. 131–140.

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

[3] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", CCS '06: Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, **(2006)**, pp. 89–98.

[4] 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. 898–909.

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

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

[7] 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.

[8] N. Shang, M. Nabeel, F. Paci and E. Bertino, "A privacypreserving approach to policy-based content dissemination", ICDE '10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, **(2010)**.

[9] J. Bethencourt, A. Sahai and B. Waters, "Cipher text - policy attribute-based encryption", SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, **(2007)**, pp. 321–334.

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

[11] C.-K. Chu, J. Weng, S. Chow, J. Zhou and R. Deng, "Conditional proxy broadcast re-encryption", Proceedings of the 14th Australasian Conference on Information Security and Privacy, **(2009)**, pp. 327–342.

[12] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing", CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, **(1992)**, pp. 129–140.