International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Privacy Procuring Legitimate Key Switch Over Protocol In Public Clouds With Two Layer Encoding

Sasikala B[1] ,Mr. P. V. Ramesh [2]
[1] Department Of Computer Applications, Riims College, Afflicated To S.V University Tirupati, Andhra Pradesh, India
[2]Department Of Computer Applications, Riims College, Tirupati, Andhra Pradesh, India

ABSTRACT

Distributed computing is a rising figuring innovation. It grants clients, store their information, learning or data remotly. The motivation behind this paper is to secure access control conspire for open mists. We introduce a "Security Preserving Two Layer Encryption Access control in Public Clouds", Which gives greater security and protection as contrast with the custom approaches. Current ways to deal with authorize get to administration polices(ACPs) on outsourced information utilizing chose encryption expect associations to deals with all keys and encryptions and transfer scrambled information on the remote stockpiling. Such sort of methodologies acquire high correspondences and the calculation cost to oversee keys and encryptions at whatever point client roll out improvements. To taking care of this issue by assigning as a significant part of the Access Control requirement obligations as conceivable to the cloud while lessening the data presentation hazard because of intriguing clients and Cloud.

Keywords: Distributed computing, encryption, Security Preserving Two Layer

I. INTRODUCTION

Distributed computing is a data innovation (IT) worldview that empowers universal access to shared pools of configurable framework assets and larger amount benefits that can be quickly provisioned with insignificant administration exertion, frequently finished the Internet. Distributed computing depends on sharing of assets to accomplish rationality and economies of scale, like an open utility.

Outsider mists empower associations to center around their center organizations as opposed to using assets on PC framework and maintenance. Advocates take note of that distributed computing enables organizations to evade or limit in advance IT foundation costs. Advocates additionally guarantee that distributed computing enables undertakings to get their applications up and running quicker, with enhanced sensibility and less upkeep, and that it empowers IT groups to all the more quickly alter assets to meet fluctuating and flighty demand. Cloud suppliers ordinarily utilize a "pay-as-you-go" display, which can prompt surprising working costs if heads are not acclimated with cloud-estimating models.

Cloud contending share information through outsider cloud benefit supplier has never been more practical and simpler. Cloud figuring is more well known and assume imperative part in our life. Distributed computing brings clients with numerous advantages, for example, the help of the capacity and adaptable information get to. They can persuade clients to store their neighborhood information into the cloud and guard the security of clients. They can consolidate set of existing and new procedures from

inquire about region, for example, Service-Oriented Models (SOA) and virtualization. The greater part of the association perform get to administration polices. (ACPs) proposes what clients will get to that data or records. These entrance administration strategies communicated inside the terms of client property is known as character characteristic by exploitation get to administration dialect like XACML. Control is frequently in view of security-applicable properties of clients referrers the personality qualities, the part of client in association also, venture on which client are working. These entrance control process are called as the characteristic based access control (ABAC) frameworks. Trait based access control (ABAC), supports fine grained get to control for information security what's more, security.

Proposed system approach:

The TLE approach is how to decompose the ACPs so that fine-grained ABAC enforcement can be delegated to the cloud while at the same time the privacy of the identity attributes of the users and confidentiality of the data are assured The TLE approach has many advantages. When the policy or user dynamics changes, only the outer layer of the encryption needs to be updated. Since the outer layer encryption is performed at the cloud, no data transmission is required between the data owner and the cloud. Further, both the data owner and the cloud service utilize a broadcast key management scheme whereby the actual keys do not need to be distributed to the users. Instead, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data. This two layer enforcement allows one to reduce the load on the Owner and delegates as much access control enforcement duties as possible to the Cloud. Specifically, it provides a better way to handle data updates, user dynamics, and policy changes.

Modules:

The system is proposed to have the following modules along with functional requirements.

- ✓ Identity token issuance
- ✓ Identity token registration
- ✓ Data encryption and uploading
- ✓ Data downloading and decryption Encryption evolution management

Identity token issuance

IdPs are trusted third parties that issue identity tokens to Users based on their identity attributes. It should be noted that IdPs need not be online after they issue identity tokens. Identity token registration Users register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users register their tokens related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues them two sets of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. The Owner keeps one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data. Data encryption and uploading The Owner first encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the AB-GKM::KeyGen algorithm and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the data based on the keys generated using its own AB-GKM::KeyGen algorithm. Note that the AB-GKM::KeyGen at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys.

Data downloading and Decryption Users download encrypted data from the Cloud and decrypt twice to access the data. First, the Cloud generated public information tuple is used to derive the OLE key and then the Owner generated public information tuple is used to derive the ILE key using the AB-GKM::KeyDer algorithm. These two keys allow a

User to decrypt a data item only if the User satisfies the original ACP applied to the data item. Encryption Evolution Management Over time, either ACPs or user credentials may change. Further, already encrypted data may go through frequent updates. In such situations, data already encrypted must be re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re-encrypts the affected data without the intervention of the Owner.

II. CONCLUSION

we proposed a two layer encryption based approach to solve this problem by delegating as much of the access control enforcement responsibilities as possible to the Cloud while minimizing the information exposure risks due to colluding Users and Cloud. A key problem in this regard is how to decompose ACPs so that the Owner has to handle a minimum number of attribute conditions while hiding the content from the Cloud. We showed that the policy decomposition problem is NP Complete and provided approximation algorithms. Based on the decomposed ACPs, we proposed a novel approach to privacy preserving fine-grained delegated access control to data in public clouds.

III. REFERENCES

[1]. G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, "Deduplication in cloud storage using side channels in cloud services," Oct 2008.

[2]. D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[3]. K. D. Bowers, A. Juels, and A. Oprea, "Hail: A highavailability and integrity layer for cloud storage," in Proc. Of CCS'09, 2009, pp. 187-198.4A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[4]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Intl Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[5]. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131- 145, 2003.

[6]. A. Fiat and M. Naor, "Broadcast Encryption," Proc. IntlCryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[7]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[8]. X.Liu,B.Wang,Y.Zhang, and J.Yan,"Mona: Secure MultiOwner Data Sharing for Dynamic Groups in the Cloud,"IEEE Computer Society,vol. 24,no. 6,June. 2013.

[9]. 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.

[10]. E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," ACM Trans. Inf. Syst. Secur., vol. 5, no. 3, pp. 290-331, 2002.

[11]. 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.

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

[13]. 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. 172-180.15]M.Nabeel,N.Shang,andE.Bertino,"Privacypreservingpolic y based content sharing inpublic clouds," IEEE Transactions on Knowledge and Data Engineering, 2012. 14

[14]. 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 33rdInternationalConferenceonVeryLarge DataBases, ser.VLDB 07. VLDB Endowment, 2007, pp. 123-134.

[15]. 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.

[16]. A. Fiat and M. Naor, "Broadcast encryption," in Proceedings of the 13th Annual International Cryptology Conference on Advances inCryptology,ser.CRYPTO 93. London, UK:Springer-Verlag, 1994, pp. 480-491.19D. 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.