International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2013): 4.438

Key Aggregate Cryptosystem for Data Sharing in Cloud Computing

Rohit Tate[1], Jyoti Pingalkar[2]

[1, 2] Savitribai Phule Pune University, Siddhant College of Engineering, Sudumbare, Pune, India

Abstract: ***Now a days cloud computing is becoming the famous area for researchers. Because it is very important in data sharing methodologies. The data being shared inside the cloud must be secure, flexible and efficient. For this purpose we describe new algorithm which depends upon public key cryptography and produce constant size cipher text. These ciphers can be decrypt by using a secret key. This secret key can release the constant size aggregate key for selection of flexible choices of ciphers. The other encrypted files except these ciphers remain confidential. The obtained aggregate key can be sending to others or can save into a card in very secure manner.***

Keywords: Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.

1. Introduction

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data. Cloud storage services may be accessed through a co-located cloud compute service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service or deployed on-premises. Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage. The dada sharing is important application of cloud computing. One can upload or download the data inside cloud. We can store any type of data on cloud. That means data shared may be in the text format or may be in the multimedia format. This sharing of data should be in secure, efficient and flexible manner. Otherwise the data attacker may stole our personal information and may misuse it.

To achieve such type of security inside the cloud we have used the key aggregation technique. In this we are encrypting the data which user want share on the cloud. For this encryption we are using the secrete key. It will create ciphers of fixed data size. These cyphers can be decrypt by using the aggregate key. This aggregate key will decrypt only bunch of cyphers other remaining ciphers will be confidential.

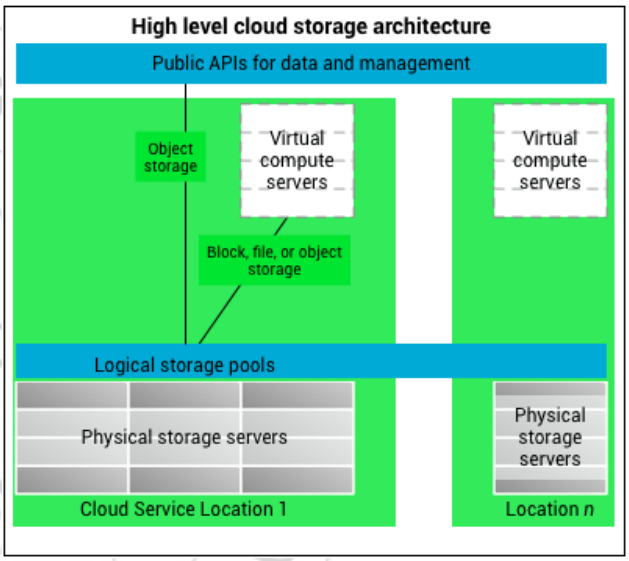

Figure: 1: Architecture of data sharing in cloud storage. (Font 9, Bold, Times new Roman)

2. Literature Survey

The importance of data sharing and the need to ensure privacy and security is discussed in a number of existing articles.

1. Security and Privacy in the Cloud
This paper outlines the requirements for achieving privacy and security in the Cloud and also briefly outlines the requirements for secure data sharing in the Cloud. It provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud. This explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud.

2. Dynamic Broadcast Encryption
This paper uses Broadcast encryption which enables a broadcaster to transmit encrypted data or information to a set of users so that only a targeted subset of users can decrypt the

Licensed Under Creative Commons Attribution CC BY

data. Other than above characteristics, dynamic broadcast encryption it also allows the group monitor to include new members by preserving previously computed information, and user decryption secret keys need not be computed again and again, the Aggregation logic and size of cipher texts are remain unchanged and the group encryption key requires no modification.

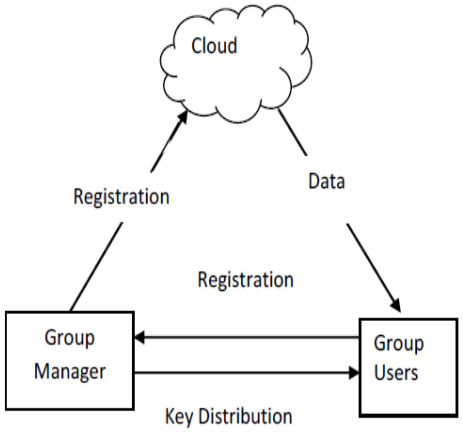

Figure 2: Dynamic Broadcast Encryption. (Font 9, Bold, Times new Roman)

3. Data Sharing in Cloud Using Hybrid Cryptosystem

This system uses the slice of data cloud to encrypt or decrypt the data. The original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. The data owner retrieve the signature from secure mediator and then it allows user to upload or download the data over the cloud.

Figure 3: Data Sharing in Cloud Using Hybrid Cryptosystem. (Font 9, Bold, Times new Roman)

4. Cryptographic Storage System

This system allows sharing of secure file on untrusted servers. It divides files into the group of file and encrypt each group of file with a unique file-key. The data owner can share the file groups with others by delivering the related lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-key needs to be updated and distributed again for a user revocation.

3. Proposed System

The proposed system is basically design on the basis of key aggregation encryption. Here we are using two keys to encrypt and decrypt the data which are secret key and its aggregate key. The data owner creates the public system parameter and generates a secrete key which is public key pair. Data can be encrypted by any user and he may decides ciphertext block associated with the plaintext file which want to be encrypted. The data owner have rights to use the secret key from which he can generate an aggregate key which is use for decryption of a set of ciphertext blocks. The both keys can be sent to end user in very secure manner. The authenticated user having an aggregate key can decrypt any block of ciphertext. This project consist of five algorithms which are used to perform the above operations. These algorithms are as follow:

Setup: the account is created on the untrusted server for sharing of data. This account is generated by data owner.

KeyGen: This algorithm is use for the generation of public key. The data owner generates a public secrete key to encrypt the data over cloud. He also create an aggregate key to access the block of ciphers of limited size.

Encrypt: This algorithm encrypts the data provided by the data owner by using the secrete key. This encrypted data is then share among the cloud.

Extract: The aggregate key is use for extracting the particular block of the ciphers from the cipher file. But other encrypted data remains secure.

Decrypt: The encrypted data is then decrypted by using the same secrete key which is use for encryption.

As the above figure shows, the key assignment is done in dynamic way. The aggregate key is use to decrypt only those cyphers which user wants. This key will not decrypt the other remaining ciphers. The main encryption and decryption is done by the secrete key. If any user enters the wrong secrete key or wrong aggregate key then the user contains will be blocked by the data owner. And the information which that user tries to retrieve is then added into non confidential storage. Only data owner can unblock that user contents and he may transfer the information from non-confidential storage to confidential storage. The user can only access the data on cloud if he has secrete key and the aggregate key, otherwise he will be block forever.

4. Results and Discussion

Figure 3: User Registration

Licensed Under Creative Commons Attribution CC BY

Figure 4: User Login

Figure 5: File Upload

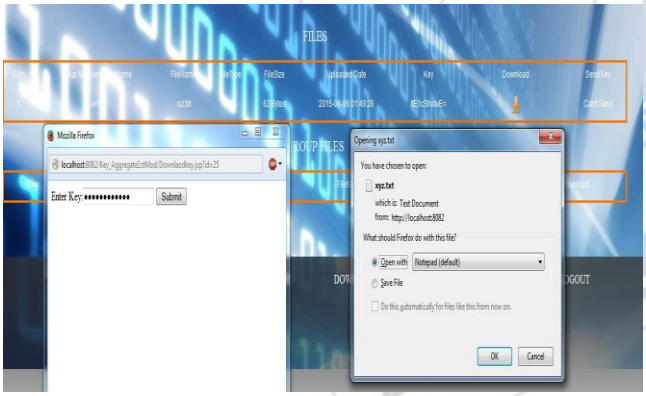

Figure 6: File Download

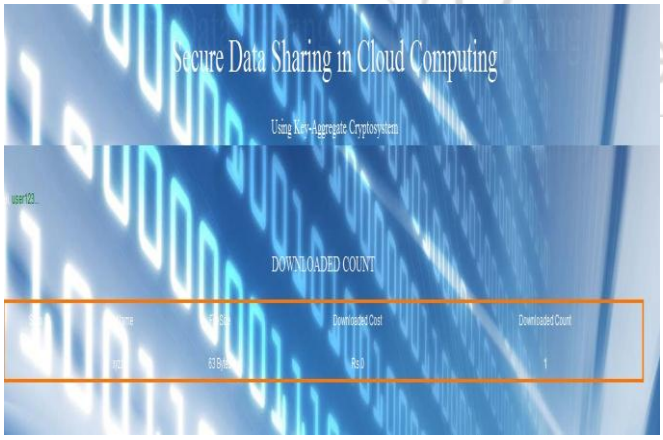

Figure 6: Download Count

Figure 7: History

Figure 8: Admin Login

Figure 9: User Details

Figure 10: Upload Details

Licensed Under Creative Commons Attribution CC BY

5. Conclusion

From above paper we conclude that the proposed system is found to be very efficient for sharing the data on cloud. This sharing is done in a secure and confidential manner. For this we have calculated KAE algorithm which means key aggregate encryption algorithm. In this paper we have maintain two public keys. First one is secrete key which is use for encryption and decryption of the data over cloud. And the second key is aggregate key which is use to decrypt limited block of cipher. Other data remain confidential. This system provides blocking mechanism for the user whose behavior is seems to be malicious.

References

[1] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[2] L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.

[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[5] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicatedto Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

[7] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.

[11] S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, pp. 239–248, 1983.

[12] G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in Proceedings of Advances in Cryptology – CRYPTO '89, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322.

[13] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188,2002.

[14] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryptology, vol. 25, no. 2, pp. 243–270, 2012.

[15] R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95–98, 1988.

[16] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.

[17] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '04). IEEE, 2004, pp. 2067–2071.

[18] J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," Microsoft Research, Tech. Rep., 2009.

[19] B. Alomair and R. Poovendran, "Information Theoretically Secure Encryption with Almost Free Authentication," J. UCS, vol. 15, no. 15, pp. 2937–2956, 2009.

[20] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology - CRYPTO'01, ser. LNCS, vol. 2139. Springer, 2001, pp. 13–229.

[21] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proceedings of Advances in Cryptology - EUROCRYPT '05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457–473.

[22] S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," in ACM Conference on Computer and Communications Security, 2010, pp. 152–161.

Licensed Under Creative Commons Attribution CC BY