SECURE DE-DUPLICATION OF ENCRYPTED DATA SHARING SCHEME IN CLOUD COMPUTING

B.V.Chowdary[1], T.Pandian[2], K. Rakesh Reddy[3], K.Bhavani[4]
[1]Associate Professor, Department of CSE, Vignan Institute of Technology & Science, Hyderabad
[2, 3, 4] Department of CSE, Vignan Institute of Technology & Science, Hyderabad

Abstract: Encrypted data has been now most commonly used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider, and can share the data with security. In this paper, we present a storage system by using hash function (SHA-1) secure data in a cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data duplication systems, our system has two advantages. Firstly, it can be used to infrastructure and share data with users by specifying access policies rather than sharing decryption keys. Secondlysecurity notion with shared data instances.

Index Terms—Secure data, cloud infrastructure.

I. INTRODUCTION

Cloud computing greatly facilitates data providers who want to outsource their data to the cloud without disclosing their sensitive data to external parties and would like users with certain credentials to be able to access the data. An encryption technique that meets this requirement where a user's private key is associated with an attribute set, a message is encrypted under an access over which is a technique to save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud. On the other hand, to the best of our knowledge of sharing or resources in secure methodology. The system that achieves the standard notion of data confidentiality in secure authentication of access to systems by resorting to the cloud architecture. We put forth a methodology to modify a ciphertext over one access policy into cipher texts of the same plaintext but under any other access policies without revealing the underlying plaintext. This technique might be of independent interest in addition to the application in the proposed storage system. We propose an approach based on two cryptographic primitives, including a zero-knowledge proof of knowledge and a commitment scheme to achieve data consistency in the system.

II. OBJECTIVE

Data access secure policy attribute based storage system with secure data consists of the following algorithms:
Setup private key generation algorithm KeyGen, SHA-1 encryption algorithm Encrypt and decrypt validity testing algorithm.
Algorithm implementation

Taking the security parameter as the input, this setup algorithm outputs the public parameter and the private key framing for the system. This algorithm is run by the each data set encrypted by general encrypted algorithms. The cipher text which includes the encryption data of set of data as well as the access structure a, cipher text computing along with decrypted data in secure authentication. Data will be encrypted before it is stored in the cloud so that for decryption and data search time consuming will be there. For the decryption and search some process needed which increases the cost. In some cases it is not sufficient for the security of the data.

With regard to a storage system, it is crucial to ensure consistency to resist duplicate faking attacks such that a legitimate message will not be unnoticeably replaced by a fake one. Storage system with secure duplication can be divided into ciphertext consistency, tag and label consistency. Ciphertext consistency guarantees that given a ciphertext outsourced by an honest data provider, an adversary who has no idea about the encrypted data cannot generate another valid ciphertext with the same tag but under a different plaintext to cheat the private cloud. Data used in the tag/label derivation and the ciphertext generation such that an adversary is not able to create a tag/label that does not match the underlying data to cheat a user having access to the encrypted data.

Private Key, data computing with ciphertext, the label, the tag, the decryption key and the access structure, respectively. Comparing the storage complexity of our system with that it is clear that our system is efficient in terms of the introduced storage overhead, which adds the underlying data scheme with each elements to the system public parameter and each sub element to the ciphertext stored by the public cloud, with an additional private cloud storing data elements.

Let each data set be the number of attributes presented in an access structure, and can be the size of an attribute set associated with the private key. Denote each data set by the number of existing data encrypted stored by the private cloud. Each exponential operations to decrypt a ciphertext. Each comparison of data set with key computational costs incurred at the data provider, the cloud, and the user for one file storage between the system in and our system. It is not difficult to see that the computational requirement for the user in our system is almost twice that in the underlying data scheme. With regard to the data provider, it requires each extra exponential operations resulted from the tag, label, proof and private key in addition to the computational cost of the underlying scheme in lacking the capability of secure duplication. Related to the cipher text regeneration if necessary and each pairing operations are calculated to check whether the plaintext hidden in the outsourcing request has existed in the public cloud. Security notion for the cloud storage system with secure duplication, hybrid cloud architecture, consisting of a pair of public and private clouds, is introduced in our storage system such that the semantic security becomes achievable for the public cloud.

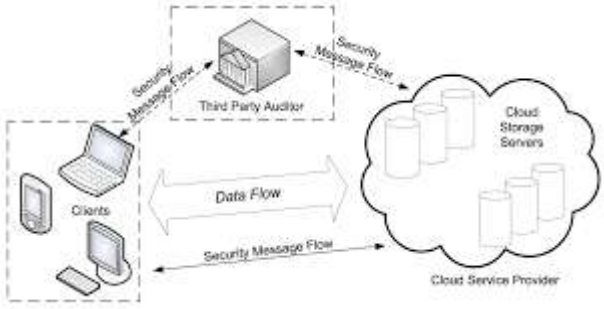

Figure: Data set flow in cloud computing.

Cloud computing is an industry with rapid and continued growth, repeating the efficiencies and cost reductions that can be obtained through economies of scale, improved global accessibility, and simplified, `outsourced' management and configuration.

III. PROPOSAL

We presented a novel approach based on hash function storage system supporting secure duplication. Our storage system is built under a hybrid cloud architecture, where a private cloud manipulates the computation and a public cloud manages the storage. The private cloud is provided with a trapdoor key associated with the corresponding cipher text, with which it can transfer the cipher text over one access policy into cipher texts of the same plaintext under any other access policies without being aware of the underlying plaintext.

Figure: cloud computing architecture.

After receiving a storage request, the private cloud first checks the validity of the uploaded item through the attached data sets. Encrypted data to the cloud and can share the data with users possessing specified credentials.

Access controls regulate the actions that a principal |human user, application, software, process, and so on may perform, e.g. to read or write data, reconfigure a system, use a particular service, etc. These actions typically relate to data.

Applications/services use access controls to manage data they hold, through authentication (identification) of the principal (\you are who you say you are") and authorizing the actions the principal attempts to take. Authorization involves applying a policy at a particular policy enforcement point with in the application/service. This determines whether the action is allowed. As a simple illustration, one may log-in to a social media platform (authentication), where authorization rules ensure that one may only view a pro le's detail if they are `friends'. This would be evaluated on an attempt to view each data users. Access controls tend to operate within the scope of the particular application/service. Policy is enforced as the action is attempted, considering the principal(s) directly involved.

Enable data to be managed beyond application and system boundaries, i.e. within and between applications, cloud services, and throughout the cloud supply chain. This is particularly relevant as cloud becomes part of wider architectures, such as for the Internet of Things.

Facilitate visibility to determine when/where data owners, to help identify the occurrence of any leakage and/or other data obligation failures. This provides evidence indicating who may (or may not) be responsible. Flexibly deal with the subtleties and nuances of data management requirements, which may be contextual, or apply only to certain data items, etc.

V. CONCLUSIONS

Encryption d a t a has been widely used in cloud computing where data providers outsource their encrypted data to the cloud and can share the data with users possessing specified credentials. On the other hand, duplication is an important technique to save the storage space and network data, which eliminates duplicate, do not support secure duplication, which makes them costly to be applied in some commercial storage services. In this paper, we presented a novel approach to realize an attribute-based storage system supporting secure duplication. Our storage system is built under a hybrid cloud architecture, where a private cloud manipulates the computation and a public cloud manages the storage. The private cloud is provided with a trapdoor key associated with the corresponding cipher text, with which it can transfer the cipher text over one access policy into cipher texts of the same plaintext under any other access policies without being aware of the underlying plaintext. After receiving a storage request, the private cloud first checks the validity of the uploaded item through the attached proof. If the proof is valid, the private cloud runs a tag matching algorithm to see whether the same data underlying the cipher text has been stored. If so, whenever it is necessary, it regenerates the cipher text into a cipher text of the same plaintext over an access policy which is the union set of both access policies. The proposed storage system enjoys two major advantages.

Firstly, it can be used to confidentially share data with other users by specifying an access policy rather than sharing the decryption key. Secondly, it achieves the standard notion of semantic security while existing duplication schemes only achieve it under a weaker security notion

REFERENCES

[1]. Mohammad I., Imad M. Handbook of Sensor Networks. CRC Press; London: 2005. pp. 117–140.

[2]. D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing / Elsevier, 2014. [On-line]. Available: http://www.elsevier.com/books/cloud-storage-forensics/quick/978-0-12-419970-5

[3]. K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptog-raphy: Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[4]. K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud foren-sics: State-of-the-art and future directions," Digital Investigation, vol. 18, pp. 77–78, 2016.

[5]. Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

[6]. D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.

[7]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Ad-vances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[8]. B. Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneck in the data domain deduplication file system," in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 26-29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[9]. M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[10]. M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, "Message-locked encryption for lock-dependent messages," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer, 2013, pp. 374–391.

[11]. S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Server-aided encryption for deduplicated storage," in Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. USENIX Association, 2013, pp. 179–194.

[12]. M. Bellare and S. Keelveedhi, "Interactive message-locked encryp-tion and secure deduplication," in Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol. 9020. Springer, 2015, pp. 516–538.