International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Vol.03,Issue.01,
May-2015,
Pages:0005-0007

Public-Key Patient-Controlled Encryption for Flexible Data Sharing in Cloud Storage

M. SRAVAN KUMAR REDDY[1], THOTTETI SUJATHA YADAV[2]
[1]Assistant Professor, Dept of CSE, RGMCET, Nandyala, AP, India, E-mail: sravankumarreddy.m@gmail.com.
[2]PG Scholar, Dept of CSE, RGMCET, Nandyala, AP, India, E-mail: sujathayadav.246@gmail.com.

Abstract: Data Sharing is an important service in Cloud Storage. In this paper, we can come to know how protectively, conveniently, and adaptably share data with others in Cloud Storage. We illustrate new public-key cryptosystems that provide fixed-size cipher texts. The originality is that anyone can combine any set of secret keys and make them as a single-key, but enclosing the power of all the keys being summarized. In other terms, the secret key holder can release a fixed-size summation-key for alternative of cipher text set in the Cloud Storage, yet the other encrypted files outside the cloud remain private. This tightly packed summation key can be sent to others or to be stored in smart card with very limit secure storage. In the common model, we deliver security analysis and other applications of our project. In particular, our project gives the first public-key patient controlled encryption for flexible hierarchy.

Keywords: Cloud Storage, Data Sharing, Key-Aggregate Encryption, Patient-Controlled Encryption.

I. INTRODUCTION

A. Cloud Storage

In recent years, the Cloud storage had gained its popularity. In case of enterprise settings, the demand for data outsourcing is increased today. In case of the strategic management of corporate data, the data outsourcing should be assisted. This process is also used as a core technology for many online services. For online application, these online services were used. Presently, this scheme is easy in order to apply for free accounts for mail, photograph album, sharing of file with storage size which is more than 25GB. By using the current wireless technology, cloud users will access almost all of their files, emails and directories by using a mobile phone from any corner of the world.

B. Data Privacy in Cloud Computing Environment

The data privacy in cloud computing environment is considered. A traditional way to ensure data privacy is to rely on the server in order to develop the access control after authentication process, which means an increase of any unexpected privilege may expose all data. Things become even bad, in case of shared-lease cloud computing environment. Data obtained from different users will be hosted on separate virtual machines (VMs) but may reside on a single physical machine. Data present in a target Virtual Machine can be stolen by instantiating another Virtual Machine co-occupant along with the target one.

C. Data Availability in Cloud Storage

Regarding the availability and security of files, there exist a more number of cryptographic schemes that are proposed. This scheme will allow a third-party auditor in order to check the availability of files apart from the data owner without leakage of any information regarding the information, or without compromising the data owner's secrecy.

D. Cryptography Schemes Used For Data Storage

Similarly, the cloud users will not have more belief that the cloud server is performing a good quality job in case of privacy. A cryptographic solution, along with proven security which is relied on number-theoretic assumptions is more attractive. When the user is not perfectly satisfied with the honesty of the technical staff or the security of the VM, those users are motivated for encrypting their data along with their own keys before uploading the data to the server.

E. Data Sharing In Cloud

In cloud storage, the data sharing is an important functionality. Consider an example that the bloggers can allow their friends views a subset of their private pictures; an enterprise can allow his /her employees access to a portion of susceptible data. Sharing encrypted data is the challenging problem. The users can download the encrypted data which is obtained from the storage and decrypt them, and then it is sent to other people for sharing, but it may lose the value of cloud storage. Users are able to give the access rights of the sharing data to other people so that they can access the data directly from the server. However, finding an efficient and secure way to share partial data in case of cloud storage is not trivial.

II. KEY SHARING METHODOLOGY

Key sharing methodology is performed based on two methods:

- Alice will encrypt all files by using a single encryption key and it Bob directly gives the corresponding secret key.

- Alice will encrypt files with distinct keys and it sends Bob to the corresponding secret keys.

Obviously, the first method is considered as inadequate since all unchosen data will also be leaked to Bob. Incase of the second method, there are practical concerns present on efficiency. The number of such keys is required as many as the number of the shared photos, say, a thousand. Transferring these secret keys inherently will require a secure channel, and storing these keys requires rather expensive in case of secure storage. The costs and complexities were involved generally to increase along with the number of the decryption keys that are to be shared. In short, it is very heavy and costly to implement this.

III. KEY AGGREGATE CRYPTO SYSTEM

The proposed system design is an efficient public-key encryption scheme that supports flexible allocation. In this system, any subset of the cipher texts (which are produced by the encryption scheme) is decrypted by a constant-size decryption key (which is generated by the proprietor of the master-secret key). This problem is solved by the introduction of a special type of public-key encryption known as key-aggregate cryptosystem (KAC). In case of KAC, users can encrypt a message that is not only under a public-key, but also under the identifier of cipher text known as class. So, that cipher texts are further categorized into different classes. The owner of the key will hold a master-secret known as Master secret key as shown in Fig.1. The master-secret key is used for extraction of secret keys that are required for different classes. Moreover, the extracted key will be an aggregate key that is as compact as a secret key for a single class, but it aggregates the power of many such keys, such that the decryption power for any subset of cipher text classes. With this solution, Alice will simply send Bob a single aggregate key via a secure channel like email. Bob can download the encrypted photos from Alice's Drop box space and then this aggregate key is used in order to decrypt the mail.

Properties of KAC:

- The Decryption key size is constant.
- The Cipher text size is constant.
- The Encryption type is public-key.

Advantages:

- A decryption key is more powerful that it will allow decryption of multiple cipher texts, without raising its size.
- The size of master-secret key, public-key and cipher text, aggregate key in the KAC schemes are all kept constant size.
- KAC scheme is flexible that there is no special relation that is required along the classes.
- A canonical application of KAC is considered as an efficient data sharing scheme.
- When the delegation key is to be efficient and flexible the key aggregation property is especially useful.
- The schemes will enable a content provider in order to share the data in a confidential and selective way, along with a fixed and small cipher text expansion, by distributing to each authorized user as a single, compact and small aggregate key.
- The delegation of decryption will be efficiently implemented along with the aggregate key.
- The number of cipher text classes is large.
- It is easy to implement key management.
- Particular user can view their messages.
- It can provide rigorous security analysis and extensive performance.

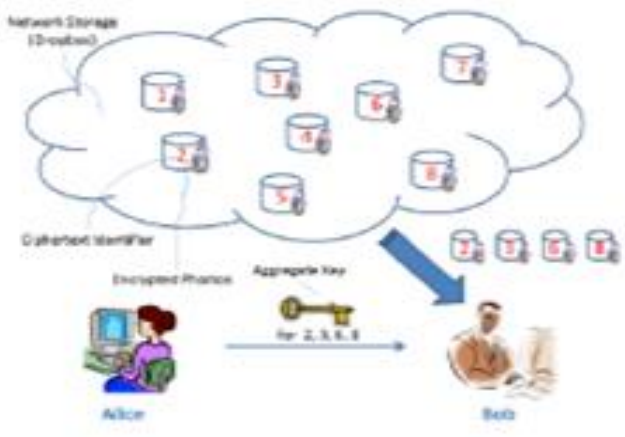

Fig.1. Alice shares files with identifiers 2,3,6 and 8 with Bob by sending him a single key.

TABLE I: Comparative Study on Existing Vs Proposed System

Methods	Existing System	Proposed System
Technique	• Key-Policy Attribute-Based Encryption (KP-ABE) • Multi-Identity Single-Key Decryption (MISKD)	Key Aggregate Cryptosystem (KAC)
Key	Symmetric	Asymmetric Key
Size Of The Decryption Key	constant-size decryption key	constant-size decryption key
Relationship between Classes	Required	Not Required

IV. CONCLUSION

In this survey, the compression of secret keys present in public-key cryptosystems is studied. This compressed key will support delegation of secret keys for different cipher text classes present in cloud storage. This approach is more flexible compared to hierarchical key assignment. If all the key-holders are sharing a similar set of privileges, the compressed key can only save spaces.

V. 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," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.

[2] L. Hardesty, Secure Computers Aren't so Secure. MIT press, http://www.physorg.com/news176107396.html, 2009.
[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, Feb. 2013.
[4] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.
[5] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, "Dynamic Secure Cloud Storage with Provenance," Cryptography and Security, pp. 442-464, Springer, 2012.
[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.
[7] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, 2009.
[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.
[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398, 2007.
[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.
[11] S.G. Akl and P.D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans. Computer Systems, vol. 1, no. 3, pp. 239-248, 1983.
[12] G.C. Chick and S.E. Tavares, "Flexible Access Control with Master Keys," Proc. Advances in Cryptology (CRYPTO '89), vol. 435, pp. 316-322, 1989.
[13] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Trans. Knowledge and Data Eng., vol. 14, no. 1, pp. 182-188, Jan./Feb. 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," Proc. IEEE INFOCOM '04, 2004.
[17] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," Proc. IEEE Global Telecomm. Conf.
(GLOBECOM '04), pp. 2067-2071, 2004.
[18] J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," technical report, Microsoft Research, 2009.
[19] B. Alomair and R. Poovendran, "Information Theoretically Secure Encryption with Almost Free Authentication," J. Universal Computer Science, vol. 15, no. 15, pp. 2937-2956, 2009.
[20] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229, 2001.
[21] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473, 2005.
[22] S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, 2010.

Author's Profile:

Thotteti Sujatha Yadav has received B.Tech, Dept. of Computer Science and Information Technology from Sri KrishnaDevaraya University, Anantapur (College- G. Pulla Reddy Engineering College, Kurnool, (autonomous) and pursuing M.Tech Computer Science & Engineering from Jawaharlal Nehru Technological University, Anantapur, (College-Rajeev Gandhi Memorial College of Engineering & Technology, Nandyal).

M.Sravan Kumar Reddy has received Bachelor's degree in Computer Science & Information Technology, Jawaharlal Nehru Technological University, Hyderabad. (College- ALFA College of Engineering & Tech., Allagadda) and Masters in Software ngineering from Jawaharlal Nehru Technological University, Hyderabad. (College- CVSR College of Engg.) and working as an Asst. Prof.in RGM college of Engineering & Technology, Nandyal.