International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Less Cost Data Infrastructure through Dropbox

Siddappa Byakod, H.P Ramyashree

MCA Department, P.E.S. College of Engineering, Mandya, Karnataka , India

ABSTRACT

Attribute-based Encryption (ABE) is regarded as a promising cryptographic conducting tool to guarantee data owners' direct control over their data in public cloud storage. The earlier ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. Subsequently, some multi-authority schemes are proposed, in which multiple authorities separately maintain disjoint attribute subsets. However, the single-point bottleneck problem remains unsolved. In this paper, from another perspective, we conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. Furthermore, by efficiently combining the traditional multi-authority scheme with TMACS, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

Keywords : MACS, CP-ABE, ABE, KP-ABE, TMACS, mCL-PKE

I. INTRODUCTION

Data sharing is an important functionality in cloud storage. Itshow how to securely, efficiently, and flexibly share data with others in cloud storage. It describe new public-key cryptosystems that produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the keys being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. It provide formal security analysis of our schemes in the standard model. It also describe other application of our schemes. In particular, our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.

The document can be uploaded by considering the probablilistic usage of algorithms to encrypt the file to make sure like the algorithm used for the encrypting technique of the file is not determined by any individual. Once the data is uploaded then the keys are generated for each file based on the random algorithms used to encrypt the file.

The keys are generated for each and every file and it will be unique in nature based on the algorithm used to generated that key. when the files are uploaded in the terms of batch the keys for single file is generated and also the aggregate key is generated for the whole batch of files.

The aggregate key is restricted to that particular batch itself and the keys are retained with the user who upload the files. The file can be opened by the key generated for the file or by the aggregated key generated by that batch of file. When the user wants to share the file with other users, he can send the file and he can provide access to that file by specifying the keys generated with that file.

II. SYSTEM MODEL

The document can be uploaded by considering the probablilistic usage of algorithms to encrypt the file to make sure like the algorithm used for the encrypting technique of the file is not determined by any individual. Once the data is uploaded then the keys are generated for each file based on the random algorithms used to encrypt the file.

The keys are generated for each and every file and it will be unique in nature based on the algorithm used to generated that key. when the files are uploaded in the terms of batch the keys for single file is generated and also the aggregate key is generated for the whole batch of files.The aggregate key is restricted to that particular batch itself and the keys are retained with the user who upload the files. The file can be opened by the key generated for the file or by the aggregated key generated by that batch of file. When the user wants to share the file with other users, he can send the file and he can provide access to that file by specifying the keys generated with that file.

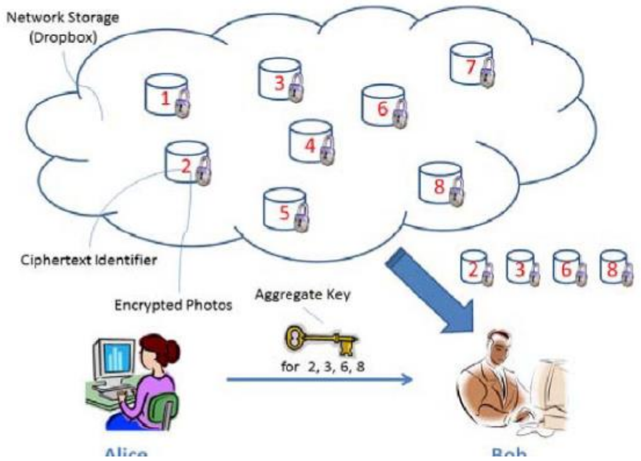

Figure 1. System Architecture

III. PREVIOUS WORK

Attribute-based Encryption (ABE) is regarded as one of the most suitable schemes to conduct data access control in public clouds for it can guarantee data owners' direct control over their data and provide a fine-grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories: Key-Policy Attribute-based Encryption (KP-ABE) and Ciphertext-Policy Attribute-based Encryption (CP-ABE).

In KP-ABE schemes, decrypt keys are associated with access structures while ciphertexts are only labeled with special attribute sets. On the contrary, in CP-ABE schemes, data owners can define an access policy for each file based on users' attributes, which can guarantee owners' more direct control over their data. Therefore, compared with KP-ABE, CP-ABE is a preferred choice for designing access control for public cloud storage.

IV. PROPOSED METHODOLOGY

In the proposed system it shows how to make a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size. Specifically, the problem statement is "To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the ciphertexts (produced by the encryption scheme) is decry ptable by a constant-size decryption key (generated by the owner of the master-secret key)." To solve this problem by introducing a special type of public-key encryption which calls key-aggregate cryptosystem (KAC). In KAC, users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes. We propose a robust and verifiable threshold multi-authority CP-ABE access control scheme, named TMACS, to deal with the single-point bottleneck on both security and performance in most existing schemes.

In TMACS, multiple authorities jointly manage the whole attribute set but no one has full control of any specific attribute. Since in CP-ABE schemes, there is always a secret key (SK) used to generate attribute private keys, we introduce (t; n) threshold secret sharing into our scheme to share the secret key among authorities.

In TMACS, we redefine the secret key in the traditional CP-ABE schemes as master key. The introduction of (t; n) threshold secret sharing guarantees that the master key cannot be obtained by any authority alone.

V. LITERATURE SURVEY

To date, the growth of electronic personal data leads to a trend that data owners prefer to remotely outsource their data to clouds for the enjoyment of the high-quality retrieval and storage service without worrying the burden of local data management and maintenance. However, secure share and search for the outsourced data is a formidable task, which may easily incur the leakage of sensitive personal information. Efficient data sharing and searching with security is of critical importance. This paper, for the first time, proposes a searchable attribute-based proxy reencryption system. When compared with the existing systems only supporting either searchable attribute-based functionality or attribute-based proxy reencryption, our new primitive supports both abilities and provides flexible keyword update service. In particular, the system enables a data owner to efficiently share his data to a specified group of users matching a sharing policy and meanwhile, the data will maintain its searchable property but also the corresponding search keyword(s) can be updated after the data sharing. The new mechanism is applicable to many real-world applications, such as electronic health record systems. It is also proved chosen ciphertext secure in the random oracle model.

Published in:
IEEE Transactions on Information Forensics and Security (Volume:10 , Issue: 9)

An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds

We propose a mediated certificateless encryption scheme without pairing operations for securely sharing sensitive information in public clouds. Mediated certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography. However, existing mCL-PKE schemes are either inefficient because of the use of expensive pairing operations or vulnerable against partial decryption attacks. In order to address the performance and security issues, in this paper, we first propose a mCL-PKE scheme without using pairing operations. We apply our mCL-PKE scheme to construct a practical solution to the problem of sharing sensitive information in public clouds. The cloud is employed as a secure storage as well as a key generation center. In our system, the data owner encrypts the sensitive data using the cloud generated users' public keys based on its access control policies and uploads the

VI. CONCLUSION

How to protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Itconsider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No matter which one among the power set of classes, the delegatee can always get an aggregate key of constant size. It is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. A limitation in a work is the predefined bound of the number of maximum ciphertext classes. In cloud storage, the number of ciphertexts usually grows rapidly. So have to reserve enough ciphertext classes for the future extension. Although the parameter can be downloaded with ciphertexts, it would be better if its size is independent of the maximum number of ciphertext classes.

VII. FUTURE SCOPES

Creation of application to which handles the cloud internal storage aspects with respect to the ciphertext. The combination of encryption algorithms must be checked with multiple combinations

VIII. 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.