Designing Robust Multiple Authority Control Access for Cloud Storage

Ms. Mona Padole
Prof. Nutan Dhande, Department of Computer Science and Engineering
ACE Nagthana Wardha India

Abstract

Data access control is a challenging issue in public cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Users may be stuck in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. Although multi authority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point bottleneck and low efficiency, due to the fact that each of the authorities still independently manages a disjoint attribute set. In this paper we propose a system that improves the approach of CP-ABE from text based asymmetric to Image based symmetric approach for faster encryption as well as access to data. We also propose a multiple access policy generation for single user where we will be able to implement one to many and many to many methodology.

Keywords: Cloud storage, Access control, CPABE. AES Encryption

Introduction

Cloud storage is a promising and important service paradigm in cloud computing[1–4]. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to name just a few. Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which is a critical issue to ensure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labelled with his/her own attributes. Only if the attributes associated with the user's secret key satisfy the access structure, can the user decrypt the corresponding cipher text to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario [5–9], and multi authority scenario [10–12]. Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation. Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set.

Literature Survey

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has so far been regarded as one of the most promising techniques for data access control in cloud storage systems. This technology offers users flexible, fine-grained and secure access control of outsourced data. It was first formulated by Goyal et al. in [1].

Then the first CP-ABE scheme was proposed by Benthencourt et al. in [2], but this scheme was proved secure only in the generic group model. Subsequently, some cryptographically stronger CP-ABE constructions [3] were proposed, but these schemes imposed some restrictions that the original CP-ABE does not have.

In [4], Waters proposed three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive as [4].

To improve efficiency of this encryption technique, Emura et al. [5] proposed a CP-ABE scheme with a constant ciphertext length. Unlike the above schemes which are only limited to express monotonic access structures, Obtrovsky et al. [5] proposed a more expressive CP-ABE scheme which can support non-monotonic access structures.

Recently, Hohenberger and Waters [6] proposed an online/offline ABE technique for CPABE which enables the user to do as much pre-computation as possible to save online computation. It’s a promising technique for resource-limited devices. In general, there are two categories of CP-ABE schemes classified by the number of participating authorities in key distribution process. One category is the single-authority scheme, the other is multi-authority scheme. In single authority schemes, only one authority is involved to manage the universal attribute set, generate and distribute secret keys for all users.

In [7], the authors respectively proposed CP-ABE schemes with efficient attribute revocation capability for data outsourcing systems. Wu et al. [5] proposed a Multi-message Ciphertext-Policy Attribute Based Encryption (MCP-ABE) which encrypts multiple messages within one ciphertext so as to enforce flexible attribute based access control on scalable media.

The literatures [9] took the efficiency issue into consideration, but they mainly considered the computation complexity inside the cryptography algorithms rather than interaction protocols between different entities in the real world, such as the procedure of user legitimacy verification. To sum up, in single-authority schemes, the single-point performance bottleneck has not been widely addressed so far. To meet some scenarios where users’ attributes come from multiple authorities, some multi-authority schemes have been proposed.

Proposed System

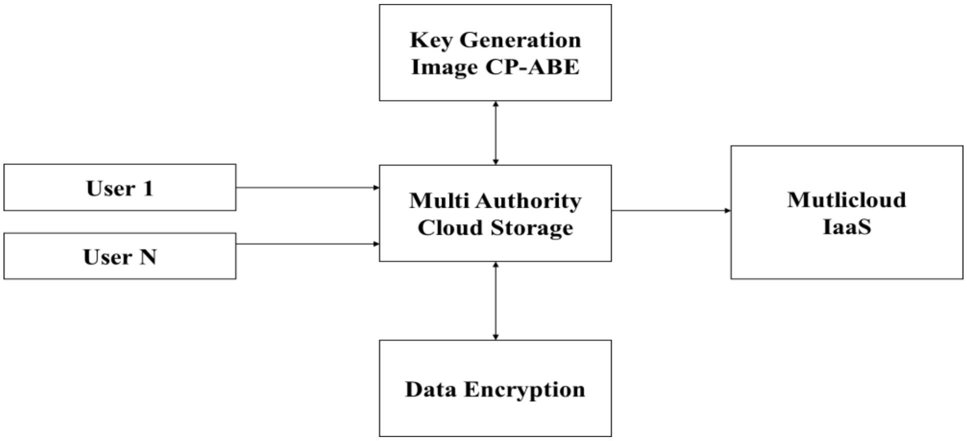

Fig: Proposed Architecture

In this paper, we present an efficient heterogeneous framework with single CA/multiple AAs to address the problem of single-point performance bottleneck. The novel idea of our proposed scheme is that the complicated and time-consuming user legitimacy verification is executed only once by one selected users. Furthermore, an auditing mechanism is proposed to ensure the traceability of malicious users. Thus our scheme can not only remove the single-point performance bottleneck but also be able to provide a robust, high-efficient, and secure access control for public cloud storage. Also we plan to extend this system from single to multicloud Databases using IaaS.

The cloud that will be used is Google Drive and multiple access will be provided to user based on permission i.e. Read / Write and Delete.

AES Encryption

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable. AES became effective as a federal government standard on May 26, 2002, after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module (see Security of AES,

Architecture and Working of AES

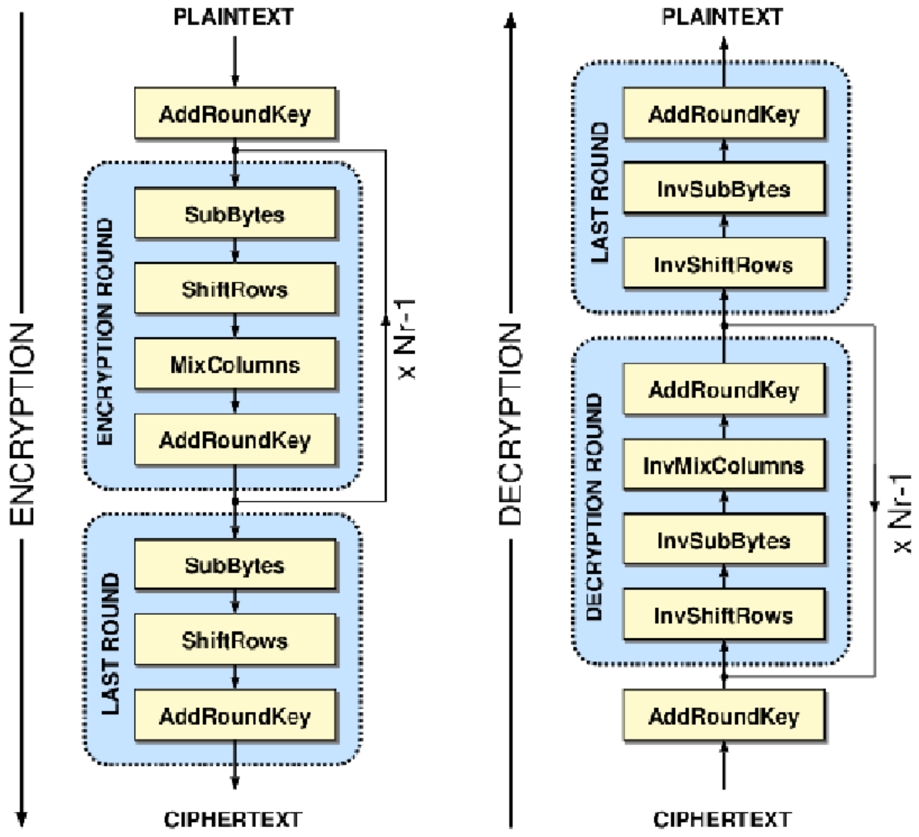

Fig: Working of AES

1. KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. InitialRound

1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes

2. ShiftRows

3. AddRoundKey.

Conclusion

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. In this paper we propose a system that improves the approach of CP-ABE from text based asymmetric to Image based symmetric approach for faster encryption as well as access to data. We also propose a multiple access policy generation for single user where we will be able to implement one to many and many to many methodology.

References

[1] Kaiping Xue, Yingjie Xue, Jianan Hong,” RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities

for Public Cloud Storage" IEEE ACCESS 2017

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[5] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[6] J. Hur, "Improving security and efficiency in attribute based data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282, 2013.

[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on time sensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011, pp. 568–588

[11] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proceedings of 2013 IEEE Conference on Computer Communications (INFOCOM 2013). IEEE, 2013, pp. 2895–2903.

[12] J. Chen and H. Ma, “Efficient decentralized attribute based access control for cloud storage with user revocation,” in Proceedings of 2014 IEEE International Conference on Communications (ICC 2014). IEEE, 2014, pp. 3782–3787.

[13] M. Chase and S. S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proceedings of the 16th ACM conference on Computer and Communications Security (CCS 2009). ACM, 2009, pp. 121–130.

[14] M. Lippert, E. G. Karatsiolis, A. Wiesmaier, and J. A. Buchmann, “Directory based registration in public key infrastructures.” in Proceedings of the 4th International Workshop for Applied PKI (IWAP 2005), 2005, pp. 17– 32.

[15] W. Li, K. Xue, Y. Xue, and J. Hong, “TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484– 1496, 2016.

[16] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, “Internet x.509 public key infrastructure certificate policy and certification practices framework,” IETF RFC, RFC3647, 2003.

[17] 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 2006). ACM, 2006, pp. 89–98.

[18] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext policy attribute-based encryption,” in Proceedings of IEEE Symposium on Security and Privacy (S&P 2007). IEEE, 2007, pp. 321–334.

[19] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” in Automata, languages and programming. Springer, 2008, pp. 579–591.

[20] L. Cheung and C. Newport, “Provably secure ciphertext policy abe,” in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007). ACM, 2007, pp. 456–465