Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Dual Access Control For Cloud Based Data Storage And Sharing

First Author: Mrs.P.V.N RAJESWARI Associate Professor, Dept.of CSE, visvodaya Engg. College, kavali, Nellore(DT)

Second Author: Miss.K.LAVANYA, as M.Tech student in the Dept. ofCSE at visvodaya Engg.College, kavali,Nellore(DT)

Abstract:

Data access control is an efficient way to provide the data security in the cloud but due to data outsourcing over un-trusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Attribute-based Encryption (ABE) technique is regarded as a most trustworthy cryptographic conducting tool to guarantee data owner's direct control on their data in public cloud storage. The previous ABE schemes involve only one authority to maintain the complete attribute set, which can bring a single-point hindrance on both security and performance. Paper proposed the design, an expressive, efficient and revocable decentralized manner data access control scheme for multi-authority cloud storage systems, where there are multiple authorities exist and every authority is able to issue attributes independently.

1. Introduction:

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead they can store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures. Cloud storage is more flexible, but security and privacy are available for the outsourced data becomes a serious concern.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user.

Attribute-based Encryption is one of the most suitable schemes for data access control in public clouds for it can ensures data owners direct control over 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) as well as Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in ciphertexts it is labeled with special attribute sets, for attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner defines the access policies and encrypts the data according to the defined policies. Every user will be issued a secret key reflecting its attributes. A user can decrypt the data

whenever its attributes match the access policies.

Access control methods ensure that authorized user access data of the system. Access control is a policy or procedure that allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a mechanism which is very much important for protection in computer security. The Cloud storage is a very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud environment. A big challenge to data access control scheme is data hosting and data access services. Because data owners do not completely trust the cloud servers also they can no longer rely on servers to do access control, so the data access control becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme is introduced.

2. Related work

To apply fine-grained policy-based control over encrypted data, ABE [9], [29] has been introduced in the literature. Concretely, ABE has two main research branches: one is CP-ABE, and the other is KP-ABE which refers to as key-policy ABE. This paper mainly deals with the former. In a CP-ABE, decryption key is associated with attribute set and ciphertext is embedded with access policy. This feature makes CP-ABE quite suitable for secure cloud data sharing (compared to KP-ABE). Note this is so because KP-ABE requires decryption key to be associated with access pol-icy which yields heavy storage cost for cloud user. Since the introduction of seminal CP-ABE [9], many works have been proposed to employ CP-ABE in various applications, e.g., accountable and traceable CP-ABE [22], [23], [24], [25], multi-authority [10], [17], outsourced CP-ABE [15], [16], [21], and extendable variants [34].

Although being able to support fine-grained data access, CP-ABE, acting as a single solution, is far from practical and effective to hold against EDoS attack [11] which is the case of DDoS in the cloud setting [11], [39]. Several counter-measures to the attack [12], [33] have been proposed in the literature. But Xue et al. [38] stated that the previous works could not fully defend the EDoS attack in the algorithmic (or protocol) level, and they further proposed a solution to secure cloud data sharing from the attack. However, [38] suffers from two disadvantages. First, the data owner is required to generate a set of challenge ciphertexts in order to resist the attack, which enhances its computational burden. Second, a data user is required to decrypt one of the chal-lenge ciphertexts as a test, which costs a plenty of expensive operations (e.g., pairing). Here the computational complex-ity of both parties is inevitably increased and meanwhile, high network bandwidth is required for the delivery of ciphertexts. The considerable computational power of cloud is not fully considered in [38]. In this paper, we will present a new solution that requires less computation and communi-cation cost to stand still in front of the EDoS attack. Recently, Antonis Michalas [20] proposed a data sharing protocol that combines symmetric searchable encryption and ABE, which allows users to directly search over encrypted data. To implement the functionality of key revocation in ABE, the protocol utilizes SGX to host a revocation authority. Bakas and Michalas [3] later extended the protocol in [20] and proposed a hybrid encryption scheme that reduces the problem of multi-user data sharing to that of a single-user. In particular, the symmetric key used for data encryption is stored in an

SGX enclave, which is encrypted with an ABE scheme. Similar to [20], it deals with the revocation problem in the context of ABE by employing the SGX enclave. In this work, we employ SGX to enable the control of the download request (such that the DDoS/EDoS attacks can be prevented). In this sense, the purpose and the technique of ours are different from that of the protocols in [3], [20].

3. Proposed System

To achieve the security requirements of anonymous data sharing, confidentiality of shared data and access control on shared data, we employ the CP-ABE technique as the basic building block. Specifically, we present the construction based on the CP-ABE scheme in due to its efficiency and elegant construction. To achieve the security requirements of anonymous download request and access control on download request, we design an effective mechanism that the cloud can judge whether a data user is authorized or not without revealing any sensitive information (including the identity of the data user, the plaintext of the outsourced data) to it. In the first system, the cloud needs the help of the authority during the judgement on the download request (sent by a data user). As a result, the authority needs to be always online. However, in some other cases in practice, the authority may not be always online. This leads to the second (enhanced) system where the authority can be offline after the parameter initialization procedure. In particular, we employ the SGX technique to replace the role of the authority during the access control on download request procedure.

We now explain the rationale behind our proposed systems. In order to provide strong security and privacy guarantees for shared data on the cloud (that could defend the EDoS attack), a cloud-based data sharing system should support dual access control as described. We start from the CP-ABE system proposed, and adapt it to the KEM/DEM setting. However, simply employing the CP-ABE construction from in the KEM/DEM setting is not sufficient to provide dual access control. New technique needs to be introduced such that the control of both data access and download request can be guaranteed. Different from the straw man solution described, we intro-duce a new approach to avoid using the “testing” ciphertext in the straw man solution. Specifically, we allow the data owner to generate a download request, which contains a randomized form of the secret key held by the data owner. The download request retains the “decryption capability” of the secret key such that it can be used to test whether the underlying data owner is capable to decrypt the shared ciphertext(s). Since the above mentioned component contained in the download request is randomized, it cannot be utilized to infer the owner of the secret key. That is, the download request enables the cloud to check whether the data owner of the download request is authorized without leaking the identity of the underlying data owner (i.e., the download request is anonymous). To further prevent leaking secret information to the cloud, the verification of download request needs the help of the authority or the enclave of Intel SGX. Our first system is designed for the case where the verification of download request involves the help of the authority, while the second system is designed for the case where the enclave of Intel SGX is involved during the verification of download request procedure. We note that our technique described above is general in the sense that it can be applied to most of the current CP-ABE constructions based on bilinear maps.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

There are five entities in system as shown in Fig. 2, a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). A global trusted certificate authority in the system is CA. CA sets up the system and also accepts the registration of all the users as well as AAs in the system. For each legal user in the system, the CA assigns a unique user identity to it and also generates a unique public key for that user. However, the CA do not involved in attribute management and creation of secret keys that are associated with attributes.

For example, the CA may be the Social Security Administration, an independent agency of the United States government. Every user can be issued unique Social Security Number (SSN) as its global identity. Each AA is an independent attribute authority that is responsible for entitling and revoking users attributes according to their role or identity in its domain. In this proposed scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. And each AA has total control over the structure and semantics of its attributes. Every AA are responsible for generating a public attribute key for every attribute it manages and a secret key for each user reflecting their attributes.

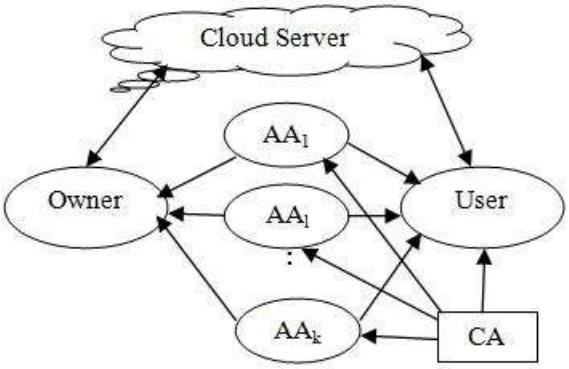

Fig.1: Decentralized manner data access controlling

4. Conclusion

Proposed a revocable decentralized data access control system can support efficient attribute revocation for multi-authority cloud storage systems. It eliminates decryption overhead of users according to attributes. This secure attribute based encryption technique for robust data security that is being shared in the cloud. This revocable multi-authority data access scheme with verifiable outsourced decryption and it is secure and verifiable. This scheme will be a promising technique, which can be applied in any remote storage systems and online social networks etc.

5. Reference

[1] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.

[2] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.

[3] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.

[4] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of en-crypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.

[5] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.

[6] Christofer Hoff. Cloud computing security: From ddos (distribut-ed denial of service) to edos (economic denial of

sustainability). http://www. rationalsurvivability.com/blog/?p=66.

[7] Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

[8] Simon Johnson, Vinnie Scarlata, Carlos Rozas, Ernie Brickell, and Frank Mckeen. Intel R software guard extensions: Epid provision-ing and attestation services. White Paper, 1:1–10, 2016.

[9] Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado. Inferring fine-grained control flow inside sgx enclaves with branch shadowing. In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.

[10] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksf-oabe: outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Transactions on Services Computing, 10(5):715–725, 2017.

[11] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Ful-l verifiability for outsourced decryption in attribute based encryption. IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2017.2710190, 2017.

[12] Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong. Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage. IEEE Transactions on parallel and distributed systems, 27(5):1484–1496, 2016.

[13] Ben Lynn et al. The pairing-based cryptography library. Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013], 2006.

[14] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V. Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Sava-gaonkar. Innovative instructions and software model for isolated execution. In HASP@ISCA 2013, page 10, 2013.

[15] Antonis Michalas. The lord of the shares: combining attribute-based encryption and searchable encryption for flexible data shar-ing. In SAC 2019, pages 146–155, 2019.

[16] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei. Auditable -time outsourced attribute-based en-cryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018.

[17] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei. White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively. IEEE Transactions on Dependable and Secure Computing, 15(5):883–897, 2018.

[18] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Lifei Wei, and Xiaodong Lin. Large universe ciphertext-policy attribute-based encryption with white-box traceability. In Computer Security-ESORICS 2014, pages 55–72. Springer, 2014.

[19] Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei. Ac-countable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In Computer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[20] Jianting Ning, Xiaolei Dong, Zhenfu Cao, Lifei Wei, and Xiaodong Lin. White-box traceable ciphertext-policy attribute-based encryp-tion supporting flexible attributes. IEEE Transactions on Information Forensics and Security, 10(6):1274–1288, 2015.

[26] Olga Ohrimenko, Felix Schuster, Cedric´ Fournet, Aastha Mehta, Sebastian Nowozin, Kapil Vaswani, and Manuel Costa. Oblivious multi-party machine learning on trusted processors. In USENIX Security Symposium, pages 619–636, 2016 JOURNAL OF LTEX CLASS FILES, VOL. , NO. , 2019

[27] Ashay Rane, Calvin Lin, and Mohit Tiwari. Raccoon: Closing dig-ital side-channels through obfuscated execution. In 24th USENIX Security Symposium, USENIX Security 2015, pages 431–446, 2015.

[28] Phillip Rogaway. Authenticated-encryption with associated-data. In Proceedings of the 9th ACM conference on Computer and communi-cations security, pages 98–107. ACM, 2002.

[29] Amit Sahai and Brent Waters. Fuzzy identity-based encryp-tion. In Advances in

Cryptology–EUROCRYPT 2005, pages 457–473. Springer, 2005.

[30] Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado. T-sgx: Eradicating controlled-channel attacks against enclave pro-grams. In NDSS 2017, 2017.

[31] Victor Shoup. A proposal for an iso standard for public key encryption (version 2.1). IACR Eprint Archive, 112, 2001.

[32] Gaurav Somani, Manoj Singh Gaur, and Dheeraj Sanghi. D-dos/edos attack in cloud: affecting everyone out there! In SIN 2015, pages 169–176. ACM, 2015.

[33] Mohammed H Sqalli, Fahd Al-Haidari, and Khaled Salah. Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In UCC 2011, pages 49–56. IEEE, 2011.

[34] Willy Susilo, Peng Jiang, Fuchun Guo, Guomin Yang, Yong Yu, and Yi Mu. Eacsip: Extendable access control system with in-tegrity protection for enhancing collaboration in the cloud. IEEE Transactions on Information Forensics and Security, 12(12):3110–3122, 2017.

[35] Florian Tramer, Fan Zhang, Huang Lin, Jean-Pierre Hubaux, Ari Juels, and Elaine Shi. Sealed-glass proofs: Using transparent enclaves to prove and sell knowledge. In EuroS&P 2017, pages 19–34. IEEE, 2017.

[36] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Public Key Cryptography–PKC 2011, pages 53–70. Springer, 2011.

[37] Yuanzhong Xu, Weidong Cui, and Marcus Peinado. Controlled-channel attacks: Deterministic side channels for untrusted operat-ing systems. In S&P 2015, pages 640–656. IEEE, 2015.

[38] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 2018.