IJDCST @ Dec-2017, Issue- V-5, I-8, SW-11
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Anonymous ABE: Enhanced efficient user Revocation Mechanism

Trumani Durga Hemanth Kumar[1], Praneetha Surapaneni[2], Swathi Voddi[3]
[1]M.tech (cse), Dhanekula Institute of Engineering & Technology, A.P., India.
[2]Assistant Professor,Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering & Technology, A.P., India.
[3]Assistant Professor,Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering & Technology, A.P., India.

Abstract **—**cloud storage service for storing and accessing information. In such conditions the data owner management and privacy preservation cryptographic techniques are used frequently. We represented a privacy preserving access control scheme for data storage, which supports authentication and decentralized key management. AnonyControl to address to the data privacy, and the user identity privacy in existing access control schemes. Here we use the user revocation in users to activating and deactivating users. Revoked users are maintained in the revoke user list and make publicly available in the cloud. User revoke will decide which user should may in cloud storage server to access data or which will remove. The data access privilege will be depending upon misbehaviour of user in cloud server. 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.

Keywords — Access control, Attributes-Based Encryption, data storage, Multi-Authority, user revoke.

Introduction

Till now, there are many ABE schemes proposed, which can be divided into two categories; Key Policy Attributebased 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. 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. 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.

User Revocation Based ABE ALGORITHM:

The concept of **attribute based encryption** is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent about attributes. In a system, the decryption of a cipher text is possible only if the set of

attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Step 1: Select File attribute1 – say File name
Step 2: Convert the file name to Binary Codes
Step 3: Select File attribute 2 – say file size
Step 4 : Convert the file size to Binary Codes
Step 5: Perform AND Operation of File Attribute 1 and 2
Step 6: Perform OR Operation of File Attribute 1 and 2
Step 7: Result of AND Operation Stored as Secret Key
Step 8: Result of OR Operation Stored as Public Key

Literature Survey

Matthew Pirretti and Brent Waters introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives also they propose cryptographic optimizations in Secure Attribute Based Systems in 2007. A performance analysis of ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions. Through this, demonstrates that the attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems. Decryption decrypts a ciphertext encrypted by the Encryption. This process begins with the decrypting party verifying that they have the required attributes. The party performing decryption will then use their attributes to decrypt the decrypt the ciphertext in order to obtain the AES and HMAC key.

Junbeom Hur, Dong Kun Noh introduces the concept of Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems in May 16, 2012. The attribute based crypto-systems were introduced such as Ciphertext-Policy Attribute-Base Encryption (CP-ABE) with an addition of two new functions. The first function is KEKGen(U)) which is used to generate keys to encrypt attributes for groups. The other extra function is the ReEncrypt(CT;G) which is a reencryption that takes the ciphertext and re-encrypt it so that a user in Group G can only access it.

Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati describes combination of access control and cryptography in 2010. It illustrates the basic principles on which architecture for combining access control and cryptography can be built. Then illustrate an approach for enforcing authorization policies and supporting dynamic authorizations, allowing policy changes and data updates at a limited cost in terms of bandwidth and computational power. It also described an approach for policy evolution that takes into account the main features of the scenario and is able to guarantee in most cases confidentiality of the information in the presence of significant policy updates, clearly identifying the exposure to collusion when this risk may arise. Other issues to be investigated include the integration with the Web paradigm, and the efficient execution of queries.

Mr. ParjanyaC.A and Mr. Prasanna Kumar describe the concept of Advance Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud in March 2014. They were presented the new framework for MONA. In this method further presented how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability. Extensive analyses show that proposed scheme satisfies the desired security requirements and guarantees efficiency as well. Here it also show that how user gets extra time even after the time out this also one of the advantage of proposed schema.

Proposed System

In this Project, we show how *AnonyControl-F* extends the User Revocation algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing. Third, we formally prove the security of the proposed scheme based on the security Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these

solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.

Related Work

In security analysis of attribute revocation in multi-authority data access control for cloud storage systems proposed the mechanism in dealing with attribute revocation could achieve both forward security and backward security. Analysis and investigation show that the work adopts a bidirectional re-encryption method in ciphertext updating, so security vulnerability appears. Also proposed attack method demonstrates that a revoked user can still decrypt new ciphertexts that are claimed to require the new version secret keys to decrypt [1]. In a semi anonymous privilege control scheme Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. The AnonyControl-F, which was fully prevents the identity leakage and achieve the full anonymity. Author's security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and author's performance evaluation exhibits the feasibility of scheme [2]. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. For that designed an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where multiple authorities coexist and each authority was able to issue attributes independently. Specifically, it proposed a revocable multiauthority CP-ABE scheme, and applies it as the underlying techniques to design the data access control scheme [3]. Sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is a challenging issue, due to the frequent change of the membership. For that proposes a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users [4]. 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. Further, by efficiently combining the traditional multi-authority scheme with TMACS, construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness.

The scheme structure of TMACS summarised in Fig. 1. In TMACS, AAs must firstly register to CA to gain the corresponding identity and certificate (aid, aid.cert). Then AAs will be involved in the construction of the system, assisting CA to finish the establishment of system parameters. CA accepts users' registration and issues the certificate (uid, uid.cert) to each legal user. With the certificate, the user can contract with any t AAs one by one to gain his/her secret key (SK). Owners who want share their data in the cloud can gain the public key (PK) from CA. Then the owner can encrypt his/her data under predefined access policy and upload the ciphertext (CT) to the cloud server. User can freely download the ciphertexts (CT) that he/she is interested in from the cloud server. However, he/she can't decrypt the ciphertext (CT) unless his/her attributes. ful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

Newly joined Data Consumers request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data Consumers request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree Tp can execute the operation associated with privilege p. The server is delegated to execute an operation p if and only if the user's credentials are verified through the privilege tree Tp.

Conclusion and Future Work

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that Anony- Control both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the
AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes. Making our schemes compatible with existing ABE schemes who support efficient user revocation is one of our future works.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE SP, May 2007, pp. 321–334.
[5] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.
[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.
[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.
[8] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.
[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 2013, pp. 573–577.
[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.
[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.
[12] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.
[13] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext-policy attribute-based encryption with accountability,"
in Proc. 6th ASIACCS, 2011, pp. 386–390.
[14] H. Ma, G. Zeng, Z. Wang, and J. Xu, "Fully secure multi-authority attribute-based traitor tracing," J. Comput. Inf. Syst., vol. 9, no. 7, pp. 2793–2800, 2013.

About authors:

Mr.TIRUMANI DURGA HEMANTH KUMARis a student of Dhanekula Institute of Engineering and Technology, Ganguru, VIJAYAWADA. He is presently pursuing hisM.Tech degree from JNTU,Kakinada.
Mrs. S.PRANEETHAis presently working as Assistant professor in CSE department,Dhanekula Institute of Engineering and Technology, Ganguru, Vijayawada.

Mrs. SWATHI VODDI is presently working as Assistant professor in CSE department, **DHANEKULA INSTITUTE OF ENGINEERING AND TECHNOLOGY,** ganguru, Vijayawada.