Preserving Data Access Control and Security in Cloud for Multi-Organization

Sahana M. Beelagi
M. Tech Scholor
Department of Computer Science & Engineering
Bellary, Karnataka, India

Kavitha Juliet
Assistant Professor
Department of Computer Science & Engineering
Bellary, Karnataka, India

Abstract

Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Cipher text-Policy Attribute-based Encryption (CP-ABE) is a promising technique for access control of encrypted data. It requires a trusted authority manages all the attributes and distributes keys in the system. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. However, existing CP-ABE schemes cannot be directly applied to the access control for multi-authority cloud storage systems, due to the inefficiency of decryption and revocation.

Keywords: Access control, attribute revocation, revocation security, CP-ABE algorithm, multi-authority cloud

I. INTRODUCTION

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed, including [1], [2],[3].Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. However, the data access control (DAC) issue of cloud computing systems has been escalated by the surge in attacks such as collusion, wiretapping and distort, so that DAC must be designed with sufficient resistance. DAC issues are mainly related to the security policies provided to the users accessing the uploaded data, and the techniques of DAC must specify their own defined security access policies and the further support of policy updates, based on which each valid user can have access to some particular sets of data whereas invalid users are unauthorized to access the data. One approach to alleviate attacks is to store the outsourcing data in encrypted form. However, due to the normally semi trusted cloud and its arrangement issues of administration rights, cloud-based access control approaches with traditional encryption are no longer applicable to cloud storage systems [5]. Sahai and Waters [5] laid a theoretical foundation for solving above encryption problem by introducing the new concept of attribute-based encryption (ABE) whose prototype is the identity-based encryption (IBE). The ABE notion has been the promising cryptographic approach on which more intensive research is based. V. Goyal et al. first proposed the key-policy attribute based encryption for fine-grained access control (KP-ABE). In KP-ABE, the data was encrypted by attribute set, and decryption was possible only when the user's policy tree matched the attribute set in the cipher text. Shortly after KP-ABE, J. Bethencourt introduced the mechanism of cipher text policy attribute-based encryption (CP-ABE), in which the user received attributes and secret keys from the attribute authority and was able to decrypt cipher text only if it held sufficient attributes that satisfied the access policy embedded in the cipher text. Proposed DAC-MACS and EDAC-MACS, due to the open and non-secure communication channel, the retracted users can still bang the backward revocation when they eavesdrop to obtain more than two valid users and Key Update Keys to update their own Secret Keys, or when they intercept the Cipher text Update Key delivered from attribute authority to cloud. In both scenarios, each revoked user can retrieve its ability to decrypt any secret information as a non-revoked user.

II. RELATED WORKS

In the literature, many approaches have been explored related to.Attribute-based encryption(ABE) and Data Access Control Attribute-based encryption. Sahai and Waters [11] proposed the notion of attribute-based encryption (ABE). In subsequent works [8], [12], they focused on policies across multiple authorities and the issue of what expressions they could achieve. Up until recently, Sahai and Waters [9] raised a construction for realizing KPABE for general circuits. Prior to this method, the strongest form of expression is boolean formulas in ABE systems, which is still a far cry from being able to express access control in the form of any program or circuit. Actually, there still remain two problems. The first one is their have no construction for realizing

CPABE for general circuits, which is conceptually closer to traditional access control. The other is related to the efficiency, since the exiting circuit ABE scheme is just a bit encryption one. Thus, it is apparently still remains a pivotal open problem to design an efficient circuit CP-ABE scheme.

Data Access Control: A plurality of data access control systems (e.g. [2], [3], [9]-[10]) based on the promising CPABE technique are proposed to construct the efficient, secure, fine grained and revocable access schemes. S.Ruj et al. (2011) proposed a distributed access control scheme in clouds (DACC) [9] that supported attribute revocation. In DACC, one or more key distribution centers (KDCs) distributed keys to data owners and users. Technically, it requires not only forward security but more indispensable backward security in context of the attribute revocation. However, DACC supported attribute revocation with vulnerable forward security.

Efficiency of Outsourcing Decryption: Green et al. [11] (2011) introduced the notion of outsourcing ABE decryption, and presented two concrete ABE schemes with outsourced decryption, which outsourced the main computation of the decryption and only incurred a small overhead of plaintext recovery for the user by using a token-based decryption method. When outsourcing the decryption of ABE cipher text, data confidentiality against the curious but honest cloud servers or an adversary can be guaranteed; however, most ABE schemes provide no guarantee on the correctness of the outsourced transformation done by the cloud servers. Cloud service providers are postulated to be semi-trusted and may have profit motives to reduce the computation and return incorrect answers which are unlikely to be detected by valid users. Recently, Lai [12] (2013) modified the original model of Green's ABE schemes [11] to allow for verifiability of the outsourced transformations. However, the storage, computation and communication overheads of the additional redundancy in scheme [12] all scale linearly with the complexity of the transmitted cipher text and cannot be practical and flexible in more general scenario.

III. SYSTEM ANALYSIS

A. Problem Statement

Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Cloud storage service separates the roles of the data owner from the data service provider, and the data owner does not interact with the user directly for providing data access service, which makes the data access control a challenging issue in cloud storage systems. Because the cloud server cannot be fully trusted by data owners, traditional server-based access control methods are no longer applicable to cloud storage systems.

B. Goal and Motivation

An efficient and reliable application is developed to A myriad of data access control techniques based on CP-ABE are used to construct the efficient, secure, fine-grained and attribute-level-revocable access schemes in a semi-trusted cloud storage system. s. Our proposed scheme mainly includes two improvements on the DAC-MACS at Secret Key Generation phase and Attribute Revocation phase, and it can run correctly.

IV. PROPOSED APPROACH

A. Proposed Technique

In this paper we first construct a new multi-authority CPABE scheme with efficient decryption and design an efficient attribute revocation method for it. Then, we apply them to design an effective access control scheme for multi-authority systems. The main contributions of this work can be summarized as follows.

1) We propose DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme for multi-authority cloud storage systems, which is provably secure in the random oracle model and has better performance than existing schemes.
2) We construct a new multi-authority CP-ABE scheme with efficient decryption. Specifically, we outsource the main computation of the decryption by using a token based decryption method.
3) We also design an efficient immediate attribute revocation method for multi-authority CP-ABE scheme that achieves both forward security and backward security. It is efficient in the sense that it incurs less communication cost and computation cost of the revocation.

B. System Overview

As shown in Fig below a cloud storage system with multiple attribute authorities (DAC-MACS) has five types of entities involved: global certificate authority (CA), users, cloud servers, data owners, and attribute authority (AA).

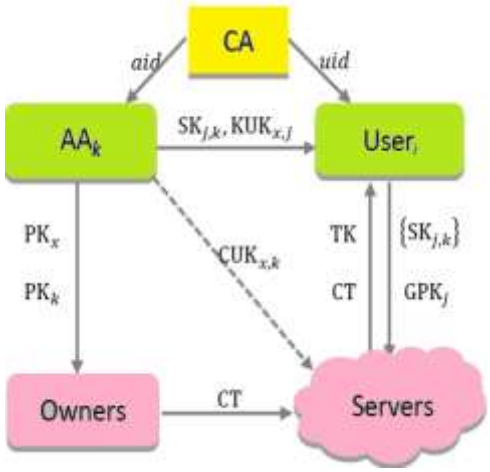

Fig. 1: Block diagram of proposed system

V. MAIN MODULES

A. Algorithm used: CP-ABE algorithms

1) Global trusted certificate authority:

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. The CA is responsible for the distribution of global secret key and global public key for each legal user in the system. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity.

2) Attribute Authority (AA):

Every AA is an independent attribute authority that is responsible for issuing, revoking and updating user's attributes According to their role or identity in its domain. In DACMACS every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user associates with their attributes.

3) Cloud Server:

The cloud server stores the owners' data and provides data access service to users. It generates the decryption token of a cipher text for the user by using the secret keys of the user issued by the AAs. The server also does the cipher text update when an attribute revocation happens.

4) Data Owner:

The data owners define the access policies and encrypt the data under the policies before hosting them in the cloud. They do not rely on the server to do the data access control. Instead, the cipher text can be accessed by all the legal users in the system. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text, the user can decrypt the cipher text.

5) User:

Each user is assigned with a global user identity from the CA. Each user can freely get the cipher texts from the server. To decrypt a cipher text, each user may submit their secret keys issued by some AAs together with its global public key to the server and ask it to generate an decryption token for some cipher text. Upon receiving the decryption token, the user can decrypt the cipher text by using its global secret key. Only when the user's attributes satisfy the access policy defined in the cipher text, the server can generate the correct decryption token. The secret keys and the global user's public key can be stored on the server; subsequently, the user does not need to submit any secret keys if no secret keys are updated for the further decryption token generation.

VI. EXPERIMENTAL RESULTS

A. System initialization

1) CA setup: The certificate authority initializes the system with the CA setup algorithm.

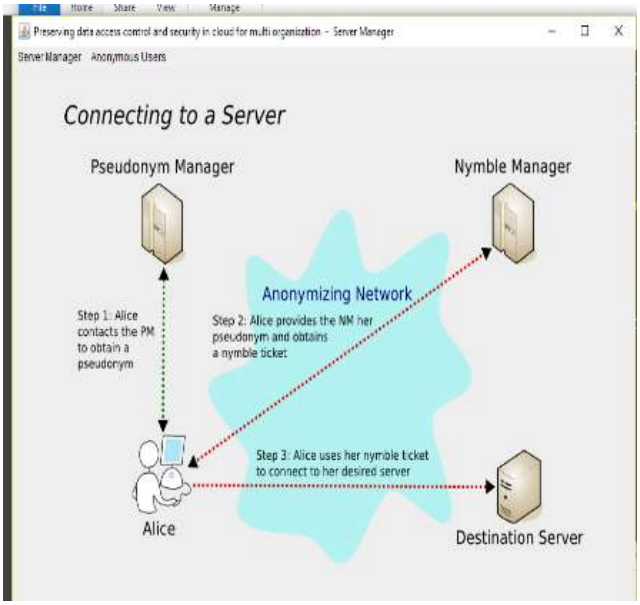

Fig. 2:

2) User Registration

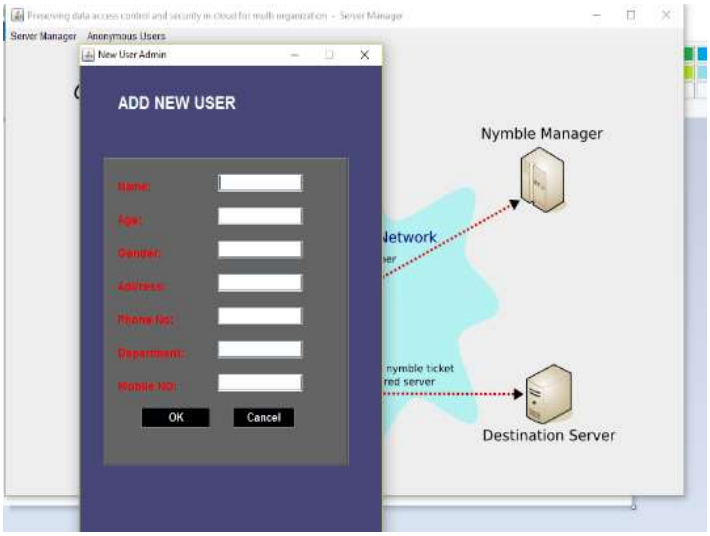

Fig. 3:

3) AA Registration

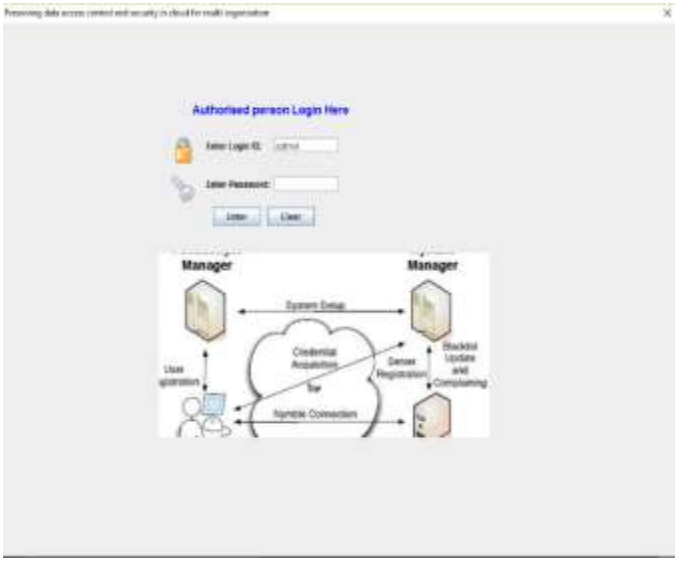

Fig. 4:

4) Attribute Revocation and Encryption

Fig. 5:

5) Attack user information

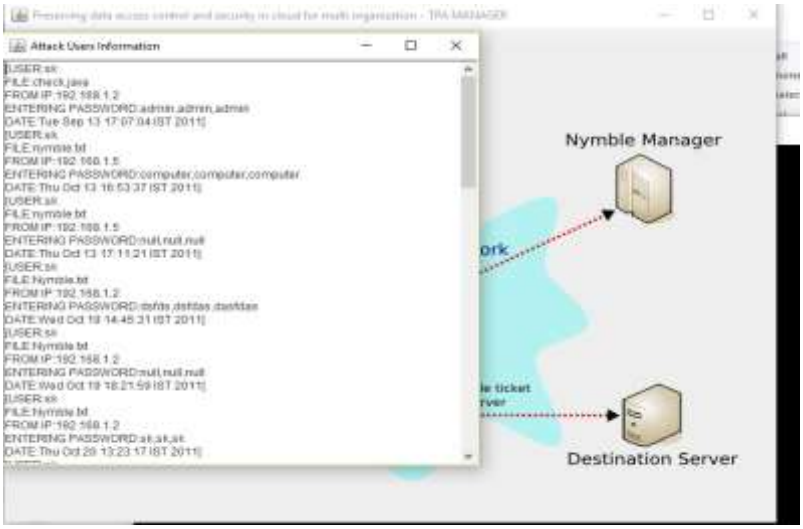

Fig. 6:

VII. CONCLUSION

To diagnose the malaria an efficient and reliable approach for data accessing on cloud safely is implemented in this this paper. A new effective data access control scheme for multi-authority cloud storage systems (NEDAC-MACS) is proposed. NEDACMACS can withstand the two vulnerabilities even though the non-revoked users reveal their received key update keys to the revoked user. The revoked user has no chance to decrypt any objective cipher text even if it actively eavesdrop to obtain an arbitrary number of non-revoked users.

The application ensures the security of the users accessing the data in the cloud environment.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334
[4] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective data access control for multiauthority cloud storage systems," IEEE Trans. Information Forensics and Security, vol. 8, no. 11, pp. 1790-1801, Nov. 2013
[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. EUROCRYPT' 05, pp. 457-473, 2005
[6] J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.
[7] J. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012. [9] S. Garg, C. Gentry, S. Halevi, A. Sahai
[8] S. Garg, C. Gentry, S. Halevi, A. Sahai and B. Waters, "Attribute-Based Encryption for Circuits from Multilinear Maps," in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin, Heidelberg, 2013.
[9] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007
[10] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multiauthority ciphertext policy attribute-based encryption with accountability," Proc. ASIACCS'11, pp. 386-390, ACM, 2011
[11] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011
[12] J. Z. Lai, R. H. Deng, C. W. Guan, and J. Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, vol. 8, pp. 1343-1354, Aug 2013