ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014, Available at: www.researchpublish.com

Securing Cloud Server & Data Access with Multi-Authorities

Tejaswini R M[1], Roopa C K[2] , Ayesha Taranum[3].

[1,3](PG Student) Software Engineering, Sri Jayachamarajandra College of engineering,Mysore,Karnataka, India;
[2] Assistant Professor, Dept of IS & E, Sri Jayachamarajandra College of engineering,Mysore,Karnataka, India

Abstract: **With the rise of the era of "cloud computing", concerns about "Security" continue to increase. Cloud computing environments impose new challenges on access control techniques due to the growing scale and dynamicity of hosts within the cloud infrastructure; we proposed Multi-Authority System (MAS) architecture. This architecture consists of agents: Cloud Service Provider Agent (CSPA), Control Agent (CA), Third party Auditor (TPA) and Attribute Authority Agent (AAA). The TPA provides a graphical interface to the cloud user that facilitates the access to the services offered by the Cloud Service Provider (CSPA).**

Keywords: **Cloud Computing, Cloud Data Storage, Cloud Service Provider, Cloud Data Access Control, Multi-Authority System and Confidentiality.**

I. INTRODUCTION

Cloud computing describes applications that are extended to be accessible through the Internet. These cloud applications use large data centers or cloud data storage (CDS)and powerful servers that host Web applications and Web services. Anyone with a suitable Internet connection and a standard browser can access a cloud application. Cloud computing consists of multiple cloud computing service providers (CSPs). In terms of software and hardware, a cloud system is composed of many types of computers, storage devices, communications equipment, and software systems running on such devices.

Cloud storage is composed of thousands of storage devices clustered by network, distributed file systems and other storage middleware to provide cloud storage service for cloud users. The typical structure of cloud storage includes storage resource pool, distributed file system, service level agreements (SLAs), and service interfaces, etc. Globally, they can be divided by physical and logical functions boundaries and relationships to provide more compatibilities and interactions. Cloud storage is tending to combined with cloud security, which will provide more robust security [1].
Cloud Data access control issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations where in some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users [2, 3, 4].

Access control regulates accesses to resources by principals. It is one of the most important aspects of the security of a system. A protection state or policy contains all information needed by a reference monitor to enforce access control. The syntax used to represent a policy is called an access control model.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014, Available at: www.researchpublish.com

The aim of this paper is to study the data access control issue in multi-authority cloud storage systems. One critical requirement in the design of access control schemes is the efficiency in computation. There are two operations in access control that require efficient computation, namely decryption and revocation. The users may use their smart phones to access the data in nowadays cloud storage systems, but the computation ability of smart phones is not as strong as the PCs. Thus, the decryption on each user should be as efficient as possible in the design of data access control schemes. When a user is degraded or leaving the system, some attributes should be revoked from this user. There are two requirements of the efficient attribute revocation: 1) The revoked user (whose attribute is revoked) cannot decrypt the new ciphertext that is encrypted with new public key (Forward Security); 2) The newly joined user can also decrypt the previous published ciphertexts that are encrypted with previous public key if it has sufficient attributes (Backward Security).

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 Third party auditor (TPA) which acts as a proxy server to safeguard the cloud server.

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.

II. SYSTEM MODEL

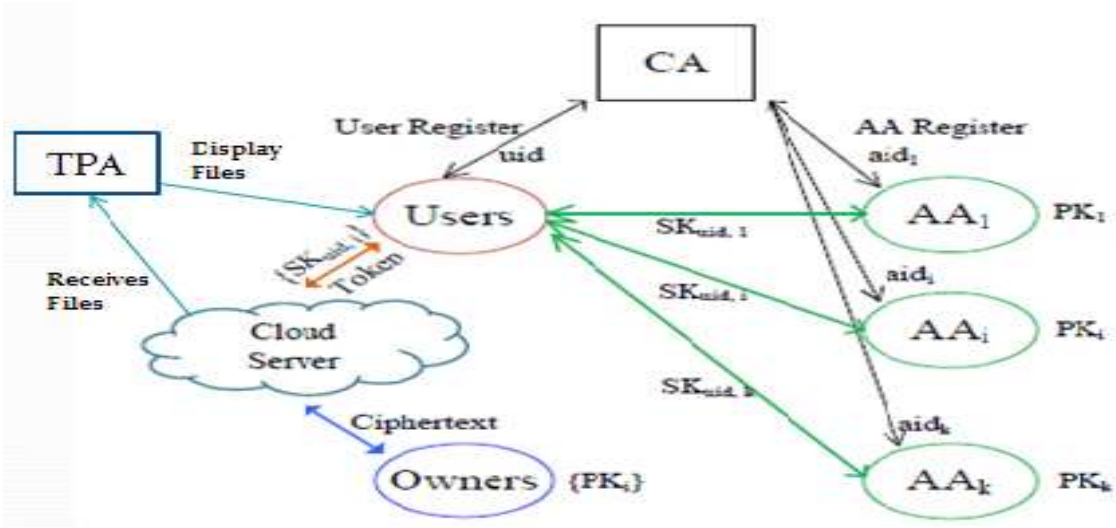

Fig 1: System Model

As shown in Fig.1. The system model consists of Six types of entities: a global certificate authority (CA), the attribute authorities (AAs), the cloud server (server), the data owners(owners),the data consumers (users) and the Third Party auditor (TPA).

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.

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. 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.

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

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 ciphertext can be accessed by all the legal users in the system

The Third Party Auditor (TPA) allows the user to view the files on the cloud server, It also give information about which file is stored in which server. The TPA provides security to the Cloud server so that the attacker may not attack the server & hack the data

III. PROPOSED SOLUTION

Although the existing multi-authority CP-ABE scheme [10] has high policy expressiveness and has been extended to support attribute revocation in [14], it still cannot be applied to access control for multi-authority cloud storage systems due to the inefficiency of decryption and revocation. In order to design an efficient access control scheme for multi-authority systems, we first construct a new multi-authority CP-ABE scheme with efficient decryption and then propose an efficient attribute revocation for it.

Without a central authority, it is hard to tie together different components of a user's secret key and use the key randomization method to prevent the collusion attack. In our method, we separate the authority into a global certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up the system and accepts the registration of all the users and AAs in the system. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. The CA assigns a global user identity uid to each user and a global authority identity aid to each attribute authority in the system. Since the uid is global unique in the system, secret keys issued by different AAs for the same uid can be tied together for decryption. Also, since each AA is associated with an aid, every attribute is distinguishable even though some AAs may issue the same attribute. Thus, the collusion attack can be resisted by using the aid and uid.

To achieve efficient decryption on the user, we propose a token-based decryption outsourcing method. We apply the decryption outsourcing idea from [14] and extend it to multiple authority systems by letting the CA generate a pair of global secret key and global public key for each legal user in the system. During the decryption, the user submits its secret keys issued by AAs to the server and asks the server to compute a decryption token for the ciphertext. The user can then decrypt the ciphertext by using the decryption token together with its global secret key.

To solve the attribute revocation problem, we assign a version number for each attribute, such that when an attribute revocation happens, only those components associated with the revoked attribute in secret keys and ciphertexts need to be updated. When an attribute of a user is revoked from any AA, the AA generates a new version number and generate several user update keys and a ciphertext update key. With the user update key, each non-revoked user who holds the revoked attributes can update their secret key. Because the update keys are distinguishable for different users, the revoked user cannot update its secret key by using other users' update keys (Forward Security). By using the ciphertext update key, the component associated with the revoked in the ciphertext can be updated to the current version. To improve the efficiency, we delegate the ciphertext update workload to the server by using the proxy re-encryption method, such that the new joined user is also able to decrypt the previous published data which are published before it joins the system (Backward Security). Moreover, all the users need to hold the latest secret key, rather than to keep records on all the previous secret keys.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014, Available at: www.researchpublish.com

IV. PERFORMANCE ANALYSIS

We conduct the performance analysis between our Methodology and the Ruj's IACC scheme under the metrics of Storage Overhead, Communication Cost and Computation Cost.

1) Storage Overhead

The storage overhead is one of the most significant issues of the access control scheme in cloud storage systems. Suppose there are NA AAs in the system. Let |p| be the element size in the G;GT ;Zp. Let na;k and na;k;uid denote the total number of attributes managed by AAk and the number of attributes assigned to the user with uid from AAk respectively. We compare the storage overhead on each entity in the system, as shown in Table I

Table- I

COMPARISON OF STORAGE OVERHEAD

Entity	Ruj's DACC [16]	Our Method
AA_k	$2n_{a,k}\|p\|$	$(n_{a,k}+3)\|p\|$
Owner	$(n_c+2\sum_{k=1}^{N_A} n_{a,k})\|p\|$	$(3N_A+1+\sum_{k=1}^{N_A} n_{a,k})\|p\|$
User	$(n_{c,x}+\sum_{k=1}^{N_A} n_{a,k,uid})\|p\|$	$(2N_A+1+\sum_{k=1}^{N_A} n_{a,k,uid})\|p\|$
Server	$(3l+1)\|p\|$	$(3l+2)\|p\|$

n_c: total number of ciphertexts stored on the cloud server;
$n_{c,x}$:number of ciphertexts contain the revoked attribute x;
l: total number of attributes that appeared in the ciphertext.

2) Communication Cost

The communication cost of the normal access control is almost the same between our IAC-MACSS and Ruj's IACC scheme. Here, we only compare the communication cost of attribute revocation, as shown in Table II. It is easily to find that the communication cost of attribute revocation in Ruj's scheme is linear to the number of ciphertexts which contain the revoked attributes. Due to the large number of ciphertext in cloud storage system, Ruj's scheme incurs a heavy communication cost for attribute revocation.

Table -II

COMPARISON OF COMMUNICATION COST FOR ATTRIBUTE REVOCATION

Operation	Ruj's DACC [16]	Our Method
Key Update	N/A	$n_{non,x}\|p\|$
Ciphertext Update	$(n_{c,x}\cdot n_{non,x}+1)\|p\|$	$\|p\|$

$n_{non,x}$ is the number of non-revoked users who hold the revoked attribute x; $n_{c,x}$ is the number of ciphertexts which contain the revoked attribute x.

3) Computation Cost

We simulate the computation time of encryption, decryption and ciphertext re-encryption/update in both our IAC-MACSS and Ruj's IACC scheme. We do the simulation on a Linux system with an Intel Core 2 Duo CPU at 3.16GHz and 4.00GB RAM. The code uses the Pairing-Based Cryptography (PBC) library version 0.5.12 to simulate the access control schemes. We use a symmetric elliptic curve a-curve, where the base field size is 512-bit and the embedding degree is 2. The a- curve has a 160-bit group order, which means p is a 160-bit length prime. All the simulation results are the mean of 20 trials.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014, Available at: www.researchpublish.com

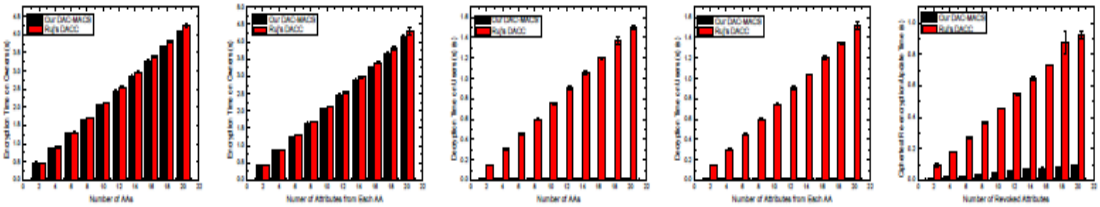

Fig2: Comparison of Encryption, Decryption& Ciphertext reencryption/update text

We compare the computation efficiency of both encryption and decryption in two criteria: the number of authorities and the number of attributes per authority, as shown in Fig. 2.Fig.2(a) describes the comparison of encryption time versus the number of AAs, where the involved number of attributes from each AA is set to be 10. Fig.2(b) gives the encryption time comparison versus the number of attributes from each AA, where the involved number of AAs is set to be 10. Suppose the user has the same number of attributes from each AA. Fig.2(c) shows the comparison of decryption time versus the number of AAs, where the number of attributes the user holds from each AA is set to be 10. Fig.2(d) describes the decryption time comparison versus the number of attributes the user holds from each AA. In Fig.2(d), the number of authority for the user is fixed to be 10. Fig.2(e) gives the comparison of ciphertext re-encryption/update versus the number of revoked attributes appeared in the ciphertext. The simulation results show that our IAC-MACSS incurs less computation cost on the encryption of owners, the decryption of users and the re-encryption of ciphertexts.

V. CONCLUSION

In this paper, we proposed an effective data access control scheme for multi-authority cloud storage systems, IACMACS. We also construct a new multi-authority CP-ABE scheme, in which the main computation of decryption is outsourced to the server. We further designed an efficient attribute revocation method that can achieve both forward security and backward security. Our attribute revocation methods incurs less communication cost and less computation cost of the revocation, where only those components associated with the revoked attribute in the secret keys and the ciphertext need to be updated. Through the analysis and the simulation, we showed that our IAC-MACSS is provably secure in the random oracle model and incurs less storage overhead, communication cost and computation cost, compared to existing schemes

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology, Tech. Rep., 2009.
[2] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in Proceedings of the 2007 IEEE Symposium on Security and Privacy (S&P’07). IEEE Computer Society, 2007, pp. 321–334.
[3] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure ealization,” in Proceedings of the 4th International Conference on Practice and Theory in Public Key Cryptography (PKC’11). pringer, 2011, pp. 53–70.
[4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, “Bounded ciphertext policy attribute based encryption,” in Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP’08). Springer, 2008, pp. 579–591.
[5] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS’07). ACM, 2007, pp. 195–203.
[6] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology- UROCRYPT’10. Springer, 2010, pp. 62–91.
[7] M. Chase, “Multi-authority attribute based encryption,” in Proceedings of the 4th Theory of Cryptography Conference on Theory of Cryptography (TCC’07). Springer, 2007, pp. 515–534.

[8] S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute-based encryption," in Proceedings of the 11th International Conference on Information Security and Cryptology (ICISC'08). Springer, 2008, pp. 20–36.
[9] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09). ACM, 2009, pp. 121–130.
[10] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology - EUROCRYPT'11. Springer, 2011, pp. 568–588.
11] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proceedings of the 4st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'84. Springer, 1984, pp. 47–53.
[12] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proceedings of the 21st Annual International Cryptology Conference: Advances in Cryptology - CRYPTO'01. Springer, 2001, pp. 213–229.
[13] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Proceedings of the 8th IMA International Conference on Cryptography and Coding. Springer, 2001, pp. 360–363.
[14] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of abe ciphertexts," in Proceedings of the 20th USENIX Security Symposium. USENIX Association, 2011.
[15] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, 2011.
[16] S. Ruj, A. Nayak, and I. Stojmenovic, "IACC: Distributed Access Control in Clouds," in Proceeding of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'11). IEEE, 2011, pp. 91–98.
[17] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the 2nd USENIX Conference on File and Storage Technologies (FAST'03). USENIX, 2003.
[18] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proceedings of the Network and Distributed System Security Symposium (NDSS'03). The Internet Society, 2003.
[19] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," Electronic Colloquium on Computational Complexity (ECCC), no. 043, 2002.
[20] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in Proceedings of the first ACM Cloud Computing Security Workshop (CCSW'09). ACM, 2009, pp. 103–114.
[21] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," Journal of Computer Security, vol. 19, no. 3, pp. 367–397, 2011.
[22] E. Damiani, S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Key management for multi-user encrypted databases," in Proceedings of the 2005 ACM Workshop On Storage Security And Survivability (StorageSS'05). ACM, 2005, pp. 74–83.
[23] W. Wang, Z. Li, R. Owens, and B. K. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the first ACM Cloud Computing Security Workshop (CCSW'09). ACM, 2009, pp. 55–66.
[24] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology - EUROCRYPT'05. Springer, 2005, pp. 457–473.
[25] 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'06). ACM, 2006, pp. 89–98.
[26] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS'10). ACM, 2010, pp. 261–270.
[27] S. Jahid, P. Mittal, and N. Borisov, "Easier: encryption-based access control in social networks with efficient revocation," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11). ACM, 2011, pp. 411–415.
[28] 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.
[29] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," in Proceedings of the 6th ACM Symposium on Information, Computer and communications Security (ASIACCS'11). ACM, 2011, pp. 386–390.
[30] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, 2012.