Decentralizes the central authorities in Cloud for Data Access Control

SAI BHARGAVI[1] , K.Rajiv[2] &Dr.K.Ramakrishna[3]

[1]M-Tech Dept. of IT Sridevi Women's Engineering College Hyderabad

[2]Assistant Professor, Dept. of IT Sridevi Women's Engineering College Hyderabad

[3]Professor & HOD, Dept. of IT Sridevi Women's Engineering College Hyderabad

Abstract- Cloud computing is an innovative processing paradigm, which allows flexible, and low cost utilization of computing methods, nevertheless the data is outsourced for some cloud, and various privacy security concerns arise from it. Various plans based on the attribute-based encryption have been recommended to secure the cloud hosting storage. However, most jobs focuses on the information contents privacy and the access control, while significantly less attention is paid to the privilege control as well as the identity privacy. In this paper, semi anonymous privilege control system is introduced; here AnonyControl is to address certainly not only the data personal privacy of privateers, but also individual identification privacy. AnonyControl decentralizes the central authorities to limit the identity leakage and therefore achieves semi anonymity. Besides, it also generalizes the file access control towards the privilege control, by which usually privileges of all functions on the cloud information can be managed within just a fine-grained manner. Therefore this paper presents the AnonyControl-F, which fully prevents the identification leakage and obtains the complete anonymity.

Keywords: Anon control And Anon control-F scheme, Attribute-based encryption.

1. Introduction

Nowadays cloud computing has become a revolutionary processing computation, by which resources are provided through internet where data can be stored in some party storage space called ‘cloud’. While out sourcing the data to the third party it should satisfy the two challenges. The challenges are giving below. Firstly security for the information should be provided. Privacy of information is not an only about the content in the record. The interesting part of the cloud is out sourcing the data, it is enough just to perform an access control. Here user likes to control the privilege of information over other users. Because when data is out sourced to the third party, privacy risks will arise because server may illegally use the user’s data and access the information. Hence this operation should be controlled. Second, One's personal identification is authenticate based on the data for access control; his identity might be at risk. Since people are becoming more concern about their identity, Identity privacy should be provided before out sourcing the data. Any authority should be unaware of User identity.

1.1 LITERATURE SURVEY

Different procedures have been proposed to secure the information substance security by means of access control. Identity based encryption (IBE) was initially presented by Shamir [1], in which the sender of a message can indicate a personality such that just a beneficiary with coordinating personality can decode it. Couple of years after the fact, Fuzzy Identity-Based Encryption [2] is proposed, which is otherwise called Attribute-Based Encryption (ABE).

In such encryption conspire, a personality is seen as an arrangement of engaging characteristics, and unscrambling is conceivable if a descriptor's character has a few covers with the one indicated in the cipher text. Before long, more broad tree-based ABE plans, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Ciphertext-Policy Attribute- Based Encryption (CP-ABE) [4], are displayed to express more broad condition than basic 'cover'. They are partners to each other in the sense that the choice of encryption approach (who can or can't unscramble the message) is made by various parties. In the KP-ABE, a cipher text is connected with a set of traits, and a private key is connected with a monotonic access structure like a tree, which portrays this client's personality. A client can decrypt the cipher text if and only if the access tree in his private key is fulfilled by the attribute in the ciphertext. Be that as it may, the encryption approach is depicted in the keys, so the encrypter does not have whole control over the encryption approach. He needs to trust that the key generators issue keys with right structures to right clients.

Moreover, when a re-encryption happens, the greater part of the clients in the same framework must have their private keys re-issued in order to access the re-encoded documents, and this procedure causes significant issues in usage. Then again, those issues and overhead are all illuminated in the CP-ABE. In the CP-ABE, ciphertexts are made with an access structure, which indicates the encryption strategy, and private keys are produced by properties. A client can decode the ciphertext if and only if his properties in the private key fulfill the access tree indicated in the ciphertext. Thus, the encrypter holds a definitive power about the encryption arrangement. Likewise, the as of now issued private keys will never be changed unless the entire framework reboots.

Not at all like the information classification, is less exertion paid to secure clients' personality protection amid those intelligent conventions. Clients' identification, which are portrayed with their attribute, are for the most part revealed to key guarantors, and the backers issue private keys as indicated by their traits. However, it appears to be normal that clients are willing to keep their identity mystery while they still get their private keys. Accordingly, we propose AnonyControl and AnonyControl-F to permit cloud servers to control clients' access privileges without knowing their identity data. Their fundamental benefits are: 1) the proposed plans can secure clients privacy against every single authority. Fractional data is uncovered in AnonyControl and no data is uncovered in AnonyControl-F.

2) The proposed plans are tolerant against authority trade off, and bargaining of up to (N −2) aohuroty does not cut the entire framework down.

2. Related Work

A multi-authority system is presented in which each user has an ID and they can interact with each key generator using different pseudonyms. One user's different pseudonyms are tied to his private key, but key generators never know about the private keys, and thus they are not able to link multiple pseudonyms belonging to the same user. Also, the whole attribute set is divided into N disjoint sets and managed by N attributes authorities. In this setting, each authority knows only a part of any user's attributes, which are not enough to figure out the user's identity.

The work by Chase et al. considered the basic threshold based KP-ABE, which lacks generality in the encryption policy expression. Many attribute based encryption schemes having multiple authorities have been proposed afterwards, but they either also employ a threshold based ABE or have a semi honest central authority ,or cannot tolerate arbitrarily many users collusion attack. The work by Lewko et al. and Muller et al. are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones. Lewko et al. use a LSS matrix as an access structure, but their scheme only convert the AND, OR gates to the LSS matrix, which limits their encryption policy to boolean formula, while we inherit the flexibility of the access tree having threshold gates. Mulle et al. also supports only Disjunctive Normal Form (DNF) in their encryption policy. Besides the fact that we can express arbitrarily general encryption policy, our system also tolerates the compromise attack towards attributes authorities which is not covered in many existing works.

2.1 PROPOSED SYSTEM:

Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage.Various techniques have been proposed to protect the data contents privacy via access control. We propose AnonyControl and Anony Control- to allow cloud servers to control users' access privileges without knowing their identity information.They will follow our proposed protocol in general, but try to find out as much information as possible individually. The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F.

We firstly implement the real toolkit of a multiauthority based encryption scheme AnonyControl and AnonyControl-F.

Various techniques have been introduced to protect the data content privacy via access control. We propose AnonyControl and AnonyControl-F (fig.1) to allow cloud servers to control user's access privileges without knowing their identity information.

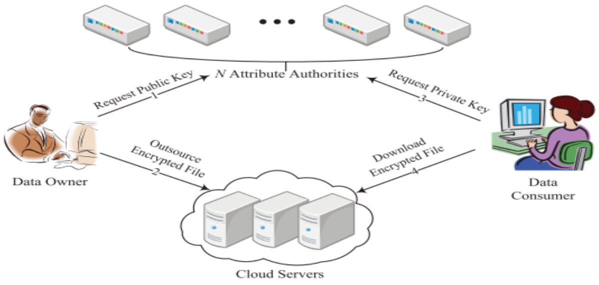


Fig 1: General Flow of our scheme.

1) The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. The proposed schemes are tolerant against authority compromise, and compromising of up to (N-2) authorities does not bring the whole system down. We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F.

3. Implementation

3.1 Attribute Authorities:

They are assumed to have powerful computation abilities on 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.

3.2 Data Owner:

A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers.

3.3 Cloud Server:

The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

3.4 Data Consumers:

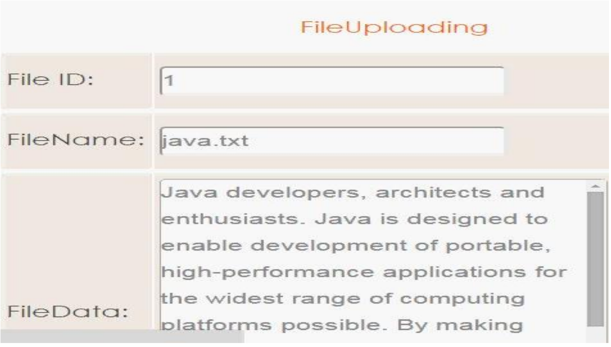
All Data Consumers are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree *Tp* can execute the operation associated with privilege *p*. The server is delegated to execute an operation *p* if and only if the user's credentials are verified through the privilege tree *Tp*.

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.

3.5 CP-ABE Algorithm:

In the CP-ABE, ciphertexts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots.

4. Experimental Work



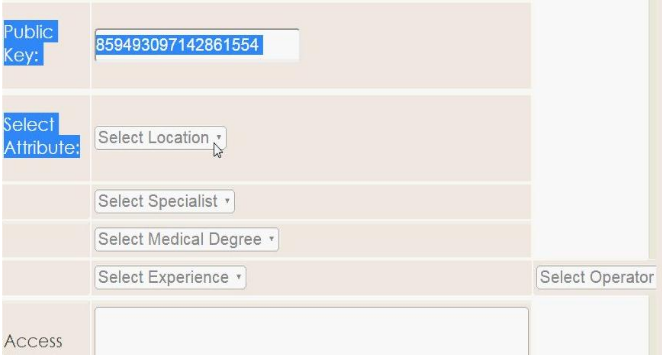
FileUploading

File ID: 1

FileName: java.txt

FileData: Java developers, architects and enthusiasts. Java is designed to enable development of portable, high-performance applications for the widest range of computing platforms possible. By making

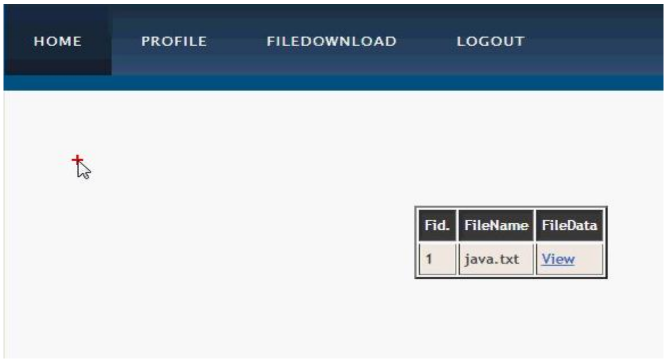
Fig 2: File Data to Uploading cloud.



Public Key: 859493097142861554

Select Attribute:

Fig 3: File Data TO Uploading Cloud with Attribute and Public Key/



Fid.	FileName	FileData
1	java.txt	View

Fig 4: View File Data for Downloading.

5. Conclusion

This paper proposes a semi-unknown trait based privilege control plan AnonyControl and a completely unknown property based privilege control plan AnonyControl-F to address the client security issue in a distributed storage server. Utilizing numerous Attribute authority as a part of the distributed computing framework, our proposed plans accomplish not just fine-grained privilege control additionally personality secrecy while directing privilege control in view of clients' personality data. All the more essentially, our framework can endure up to N − 2 Attribute authority trade off, which is exceptionally ideal particularly in Internet-based distributed computing environment. We additionally direct the security and execution investigation which demonstrates that AnonyControl both secure and proficient for distributed storage framework.

6. 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.

[15] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public-Key Cryptography. Berlin, Germany: SpringerVerlag, 2013, pp. 162–179.

[16] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[17] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attributebased encryption supporting efficient decryption test," in Proc. 8th ASIACCS, 2013, pp. 511–516.