IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURED DATA ACCESS PRIVILEGE WITH ATTRIBUTE-BASED ENCRYPTION USING KEY EXPOSURE IN CLOUD

[1]Prof. R.B. Maria Sofia,

[1]Assitant Professor,
[1]Department of Computer Applications,
[1]Christ College of Arts and Science, Kilachery.

Abstract: Cloud computing is a revolutionary computing paradigm, which enables flexible, on- demand, and low- cost operation of calculating coffers, but the data is outsourced to some Cloud waiters, and colorful sequestration enterprises crop from it. colorful schemes grounded on the trait- grounded encryption have been proposed to secure the Cloud storehouse. still, utmost work focuses on the data contents sequestration and the access control, while lower attention is paid to the honor control and the identity sequestration. In this paper, we present a semi-anonymous honor control scheme AnonyControl to address not only the data sequestration, but also the stoner identity sequestration in being access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and therefore achieves semi-anonymity. either, it also generalizes the train access control to the honor control, by which boons of all operations on the Cloud data can be managed in a fine- granulated manner. latterly, we present the AnonyControl- F, which completely prevents the identity leakage and achieve the full obscurity. Our security analysis shows that both AnonyControl and AnonyControl- F are secure under the decisional bilinear Diffie – Hellman supposition, and our performance evaluation exhibits the feasibility of our schemes.

Index Terms - Anonymity, multi-authority, attribute-based encryption, AnonyControl**.**

I. INTRODUCTION

Cloud computing is a revolutionary computing fashion, by which computing coffers are handed stoutly via Internet and the data storehouse and calculation are outsourced to someone or some party in a 'Cloud'. It greatly attracts attention and interest from both academia and assiduity due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the stylish of our knowledge. First of all, data confidentiality should be guaranteed. The data sequestration isn't only about the data contents. Since the most seductive part of the Cloud computing is the calculation outsourcing, it's far beyond enough to just conduct an access control. More likely, druggies want to control the boons of data manipulation over other druggies or Cloud waiters. This is because when sensitive information or calculation is outsourced to the Cloud waiters or another stoner, which is out of druggies' control in utmost cases, sequestration pitfalls would rise dramatically because the waiters might immorally check druggies' data and access sensitive information, or other druggies might be suitable to infer sensitive information from the outsourced calculation. thus, not only the access but also the operation should be controlled.

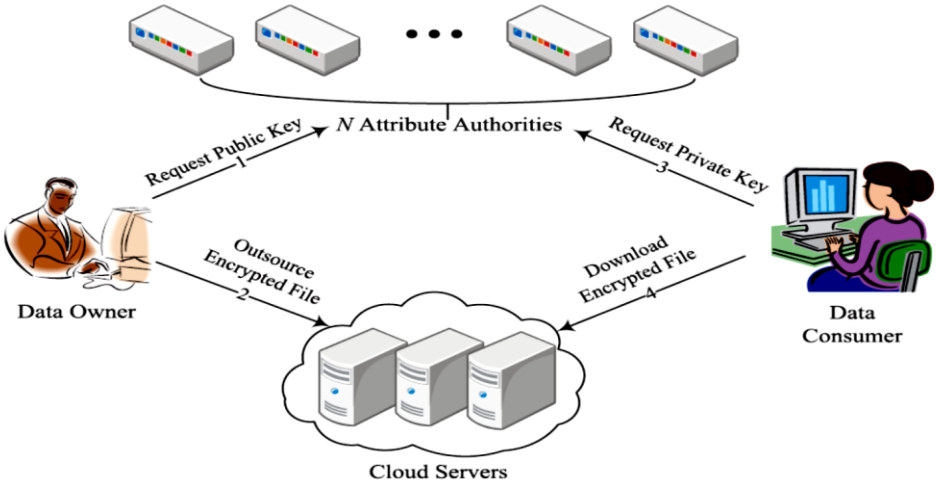

Fig-1. General flow of our scheme.

Secondly, particular information (defined by each stoner's attributes set) is at threat because one's identity is authenticated grounded on his information for the purpose of access control (or honor control in this paper). As people are getting more concerned about their identity sequestration these days, the identity sequestration also needs to be defended before the Cloud enters our life. rather, any authority or garçon alone shouldn't know any customer's particular information. Last but not least, the Cloud calculating system should be flexible in the case of security breach in which some part of the system is compromised by bushwhackers. colorful ways have been proposed to cover the data contents sequestration via access control.

Identity- grounded encryption (IBE) was first introduced by Shamir [1], in which the sender of a communication can specifies an identity similar that only a receiver with matching identity can decipher it. Many times, latterly, Fuzzy Identity-Grounded Encryption is proposed, which is also known as trait- Grounded Encryption (ABE). In similar encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypters identity has some overlaps with the one specified in the ciphertext. Soon later, more general tree- grounded ABE schemes, crucial- Policy trait- Grounded Encryption (KP-ABE) and Ciphertext- Policy trait Grounded Encryption (CP- ABE) [2], are presented to express more general condition than simple 'imbrication'. They're counterparts to each other in the sense that the decision of encryption policy (who can or cannot decipher the communication) is made by different parties.

II. RELATED WORK

Due to the significance of ensuring that only authorised users have access to reliable service, access control in clouds is receiving more attention. The cloud is being used to store an enormous amount of data, much of its sensitive data. Access control of this sensitive material, which frequently relates to health, essential documents (such as those in Google Docs or Dropbox), or even personal information, should be ensured (as in social networking). User-based access control (UBAC), role-based access control (RBAC), and attribute-based access control are the three main categories of access control (ABAC). Users who have permission to access data are listed in the access control list (ACL) in UBAC. Given the volume of users in clouds, this is not practical. According to their unique functions, users are categorised according to RBAC (established by [1]). Users with the appropriate roles can access the data. The system establishes the roles. For instance, junior secretaries might not have access to data; only faculty members and senior secretaries might. The ABAC has a wider reach and includes attributes for users as well as an attached access policy for the data. Only users who meet the access policy requirements and have a valid set of attributes can access the data.

For instance, in the aforementioned case, senior secretaries with more than eight years of experience and faculty members with more than ten years of research experience may both have access to specific documents. In the benefits and drawbacks of RBAC and ABAC are explored. On ABAC in clouds, some work has been done. All of these works employ Attribute Based Encryption, a cryptographic building block (ABE). A user in ABE has a number of properties in addition to their individual ID. ABEs are divided into two classes.

In key-policy ABE or KP- ABE, the sender has an access policy to encrypt data (Goyal et al. [3]). A writer whose keys and attributes have been revoked is unable to write back outdated data. If information has matching attributes, the recipient can decrypt it by receiving attributes and secret keys from the attribute authority. In the text policy for cyphers, CP-ABE ([4], [5]), the receiver

has a monotonic access structure with AND, OR, and other threshold gates, and an access policy in the shape of a tree with characteristics as leaves.

III. PRELIMINARIES

In our research, an access tree is used to define encryption policy. The tree's non-leaf nodes are all threshold gates, and each branch node is characterised by a feature. Every data train requires one access tree to provide the encryption policy. In this study, we generalise the access tree to a rights tree, extending being schemes. Our scheme defines the rights as being comparable to those controlled by common operating systems. A data train can do a number of operations on itself, but only authorised drug users with specific job credentials are allowed to perform each one.

An appropriate set of student grades might be "Read_mine, Read_all, cancel, Modify, produce," for instance. Additionally, reading Alice's grades is permitted for both her and her professors, but all other rights should only be granted to the professors. As a result, we must offer Alice the "Read mine" permission while reserving all other permissions for the professors. One rights p, which is described by a rights tree Tp, is connected to each operation. He is given the privileges, nonetheless, if a user's characteristics meet Tp. As a result, we have more granular control on the train access as well as other executable processes, making the train control appropriate for cloud storage services.

IV. PROBLEM FORMULATION

The System Model, the N Attribute Authorities (abbreviated as A), Cloud Server, Data Owners, and Data Consumers are the four different sorts of entities in our system. A user may simultaneously act as both a data owner and a data consumer. Because some attributes partially contain users' personally identifiable information, authorities are considered to have strong computation skills and are under the control of government agencies. Each authority has jurisdiction over one of N disjoint sets that make up the entire attribute set. As a result, each authority only knows about a portion of the attributes.

The organisation that wants to send encrypted data files to cloud servers is known as a data owner. They are only stored by the Cloud Server, which is believed to have sufficient storage capacity.

Newly joined Data Consumers ask for private keys from each authority since they are unsure of which authority controls which attributes. Authorities jointly construct the relevant private key and provide it to Data Consumers when they ask for their private keys. Any encrypted data file may be downloaded by any Data Consumer, but only those whose private keys comply with the privilege tree Tp can carry out the operation associated with the privilege p. The privilege tree Tp is used to verify the user's credentials, and only then is the server authorised to carry out an operation p.

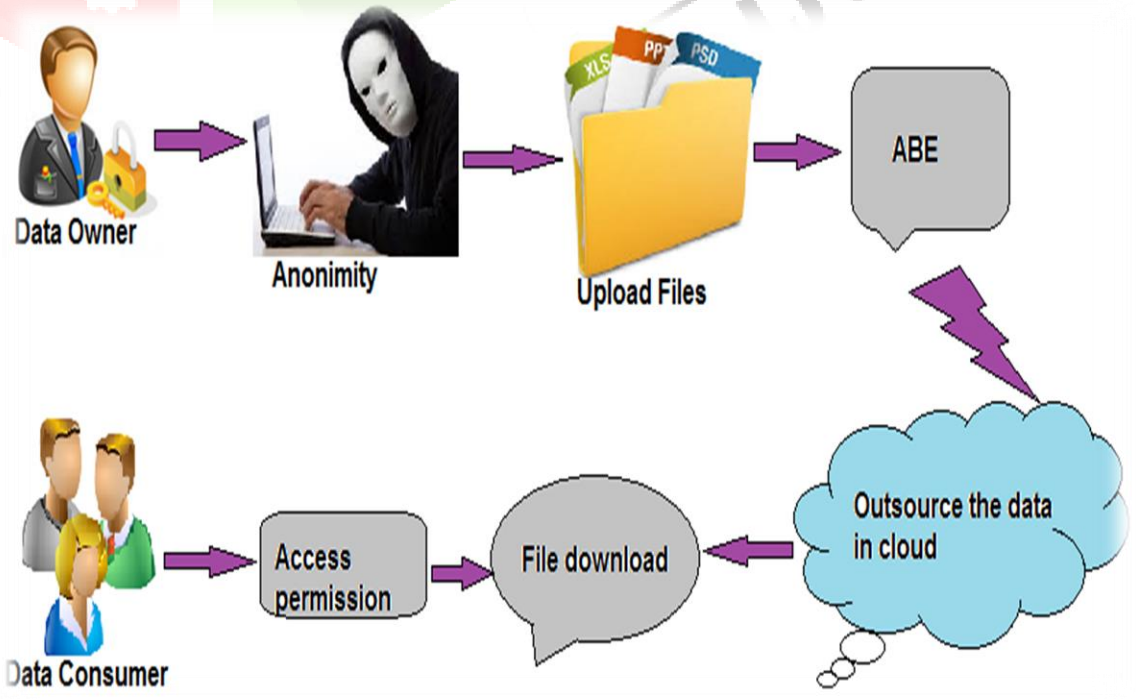

Fig-2. Proposed Architecture

ACHIEVING COMPLETE ANONYMITY, In AnonyControl, we have presumptively honest authorities, and we have assumed that they won't conspire with one another. This is a crucial presumption in AnonyControl since each authority is responsible for a portion of the total collection of characteristics, and for those attributes, it is aware of the precise details of the key requester. If the data from all authorities is combined, the key requester's entire attribute set can be reconstructed, revealing his identity to the authorities.

In this sense, AnonyControl is semi-anonymous because each authority receives partial identification information (expressed as some attributes), but we can also achieve full anonymity and permit authority cooperation. Key generators (or attribute authorities in our scheme) issue attribute keys based on the reported attribute, and in order to do so, they need to be aware of the user's attribute. This is the key to the identity information leakage we experienced in our previous scheme as well as in every other attribute-based encryption scheme currently in use.

To enable key generators to give the right attribute key without being aware of what attributes the users possess, a new method must be introduced. Giving the key requester access to all of the attribute keys for all of the attributes and allowing him to choose what he wants is a simplistic method. As a result, the key generator is unaware of the attribute keys that the key requester chose, therefore we must have complete faith that he will not choose any that are forbidden to him. To solve this, we leverage the following Oblivious Transfer (OT).

Algorithm 1 1-Out-of-2 Oblivious Transfer

1: Bob randomly picks a secret s and publishes gs to Alice.

2: Alice creates an encryption/decryption key pair:{gr,r}

3: Alice chooses i and calculates E Ki = gr, E Ki−1 = gs gr and sends E K0 to Bob.

4: Bob calculates E K1 = gs E K0 and encrypts M0 using E K0 and M1 using E K1 and sends two cipher texts EE K0 (M0), EE K1 (M1) to Alice.

5: Alice can use r to decrypt the desired cipher text EE Ki(Mi), but she cannot decrypt the other one. Meanwhile, Bob does not know which cipher text is decrypted.

1-Out-of-N Ignorant Transfer The sender Bob has n messages M1,..., Mn, and the receiver Alice wishes to choose one Mi from those M1,..., Mn in a 1-out-of-n OT. Without having any useful knowledge of the other messages, Alice successfully completes Mi, and Bob is unaware of which Mi Alice chose. We use [6] as a foundational element from a variety of implementations [6]-[8].

We introduce the 1-out-of-n OT stated in Algorithm 2 using the 1-out-of-2 OT (Algorithm 1), in which Alice chooses Mi from Bob's M0, M1. In Algorithm 2, Alice can only complete Mi if she chooses ti for the I where she wishes the message to be sent and sk for any k = i. She cannot retrieve any messages if she picks multiple tk's since certain sk's are missing.

Trustfulness of Users:

This is significantly better than the naive approach above, and it is outside the purview of this work to guarantee the accuracy of the attributes being reported. However, our AnonyControl-F must still trust the requester to choose the correct attribute keys in accordance with his identification. To the best of our knowledge, the declared attributes in the majority of ABE-related works are presumed to be verified by some external authentication (such as a government check).

Performance:

Only a few exponent calculations, which are insignificant, make up the additional processing that AnonyControl-F introduces. However, AnonyControl-F has a problem with added communication overhead. The user participates in a 1-out-of-n OT for each attribute category, requiring O(n) rounds of communication. Since the size of the complete attribute set is I, the communication overhead increases from O(1) in AnonyControl to O(I). This is our fully anonymous scheme's primary flaw, which we should address in our subsequent work.

V. SECURITY ANALYSIS

Tolerance Against Authorities' Collusion or Compromise Attack

According to the proposed approach, an authority Ak creates a set of secret parameters at random, communicates them with other authorities via a secure channel, and then uses those parameters to compute xk. According to the theory, the DDH issue cannot be solved in the group G0 of prime order p, hence gskj does not reveal any statistical data about skj. This indicates that there are still two parameters skj kept secret from the opponent even if the adversary is able to breach up to (N-2) authorities. As a result, the adversary is unable to create a valid secret key and is unable to estimate the legitimate gvk. As a result, the plan achieves tolerance for compromise up to (N-2) authorities compromise

Attackers can, however, compromise C-1 authorities in a cluster in order to generate legitimate master keys for that cluster if authorities are divided into many clusters with C authorities in each to reduce the setup phase's time complexity. As a result, there is a trade-off between complexity and tolerance. However, as the setup is a one-time operation at the very beginning of the system setup and the number of authorities is normally not particularly large, we advise adopting the traditional setup technique, whose complexity is O(N2).

The ciphertexts whose privilege trees only have those attributes may be illegally decrypted if the attacker issues all possible attribute keys to himself. This is because the compromised authorities are able to provide valid attribute keys for which they are responsible. It is difficult to compromise even one authority, and it is extremely unlikely to compromise enough authorities to forcibly decrypt some ciphertext. This is because the authorities are well-protected servers.

Tolerance Against Users' Collusion Attack

Attackers must discover Y s0 = e(g, g) in order to obtain a plaintext, which they can only do if they possess sufficient attributes to satisfy the tree T0. The distinct randomizers in each key prevent the combined key from passing through the polynomial interpolation step of the decryption method when two separate keys' components are merged. As a result, for a privilege tree to be satisfied, at least one key must be legitimate.

Formal Proof

We are prepared to explicitly prove that AnonyControl and AnonyControl-F are both secure thanks to the aforementioned qualities (indistinguishability of skj's and inability of interpolation using various users' keys). One must recover Y s0 from E0 = Ke Y s0 in order to obtain the file access privilege (Tp = T0), whereas Y s p must be recovered in order to obtain other rights. Since they are essentially the same parameters with different values, it is sufficient to demonstrate that no adversary with a significant advantage over polynomial time cannot win our security game (Section IV, defined only for the file access privilege) in order to demonstrate the security of our schemes rather than demonstrating it for all privileges.

VI. CONCLUSION AND POSSIBLE EXTENSIONS

In order to solve the issue of user privacy in a cloud storage server, this study suggests the semi-anonymous attribute-based permission control scheme AnonyControl and the fully-anonymous attribute-based privilege control method AnonyControl-F. Our suggested systems execute permission control based on users' identities while achieving fine-grained privilege control and identity anonymity by utilising different authorities in the cloud computing system. More importantly, our solution is highly preferable, especially in a cloud computing environment based on the Internet, as it can withstand up to N 2 authority breach. Additionally, we carried out a thorough investigation of security and performance, which demonstrates that AnonyControl is a secure and effective cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl, making it equally secure as it, however the 1-out-of-n oblivious transfer results in additional communication overhead. The introduction of a powerful user revocation mechanism on top of our anonymous ABE is one of the interesting future projects. Supporting user revocation is a crucial issue in practical applications, and doing so is difficult when using ABE schemes. One of our upcoming initiatives is to make our schemes compatible with current ABE schemes [9]–[11] that provide effective user revocation.

VII. REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[3] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[4] 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.

[5] 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.

[6] M. Naor and B. Pinkas, "Oblivious transfer and polynomial evaluation," in Proc. 31st STOC, 1999, pp. 245–254.

[7] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," Commun. ACM, vol. 28, no. 6, pp. 637–647, 1985.

[8] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," IEEE Trans. Comput., vol. 53, no. 2, pp. 232–240, Feb. 2004.

[9] W. Ren, K. Ren, W. Lou, and Y. Zhang, "Efficient user revocation for privacy-aware PKI," in Proc. ICST, 2008, Art. ID 11.

[10] 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 Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ASIACCS, 2010, pp. 261–270.