ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

Privilege Data Access Control with Anonymity and Fully Anonymous Attribute-Based Encryption in Cloud Storage

Rashmi K [1], G S Girish[2]

P.G. Student, Department of Information Science, BNMIT, Bangalore, Karnataka, India[1]

Associate Professor, Department of Information Science, BNMIT, Bangalore, Karnataka, India[2]

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 job 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, semianonymous privilege control system is introduced, here AnonyControl is to address certainly not only the data personal privacy of privateness, but also an individual identification privacy. AnonyControl decentralizes the central authorities to limit the identity leakage and therefore achieves semianonymity. 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 present the AnonyControl-F, which fully prevents the identification leakage and obtain the complete anonymity.

KEYWORDS: Anonycontrol And Anonycontrol-F scheme , Attribute-based encryption.

I. 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 give below. Firstly security for the information should be provided. Privacy of information is not a 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 users 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.

II. 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 decrypter's character has a few covers with the one indicated in the ciphertext. 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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

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 ciphertext 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 ciphertext 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 fulfil 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, less exertion is 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 idintity data. Their fundamental benefits are:

1) The proposed plans can secure client's 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.

Whatever is left of the paper is composed as takes after. Section III presents priliminaries. At that point, Section IV formally characterizes problem formulation where our issue for the development of AnonyControl in Section V also, AnonyControl-F in Section VI.Security analysis in VII, At last conclusion in Section VIII.

III. PRILIMINARIES

A. privilege Trees Tp

In our work, encryption approach is portrayed with a tree called access tree. Each non-leaf hub of the tree is a limit door, also, every leaf hub is depicted by a quality. One access tree is required in each information document to characterize the encryption policy.

In this paper, we expand existing plans by summing up the access tree to a privilege tree. The benefit in our plan is characterized as like the benefits oversaw in customary working frameworks. An information document has a few operations executable on itself, and each of them is permitted just to approved clients with various level of capabilities. For illustration, {Read_mine, Read_all, Delete, Modify, Create} is a privilege set of understudies' evaluations. At that point, perusing Alice's evaluations is permitted to her and her teachers, yet all different benefits should be approved just to the educators, so we have to stipend the "Read_mine" to Alice and all other to the educators. Each operation is connected with one benefit p, which is depicted by a privilege tree Tp. On the off chance that a client's traits fulfill Tp, he is conceded the previlege p. Thusly, we not just control the record get to additionally control other executable operations, which makes the record controlling fine-grained and along these lines suitable for distributed storage administration. In our plan, a few trees are required in each information record to check clients' personality and to concede him a privilege appropriately. There should be r these sort of structures, which implies there are r diverse privilege characterized for the comparing information record. The privilege 0 is characterized as the privilege to peruse the record, and different privilege might be characterized self-assertively (the m-th privilege does not as a matter of course have all the more capable previlege than the n-th one when m > n). The tree is comparable to the one characterized in [4]. Given a tree, if numx is the number of the hub x's child hub and kx is its limit esteem 0 <kx ≤ numx , then hub x is doled out a genuine worth if in any event kx children hubs have been relegated genuine worth. Uniquely, the hub turns into an OR entryway when kx = 1 and an AND door at the point when kx = numx[7,8,9] .

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

B. Fulfilling the Privilege Tree

On the off chance that a client's attribute set S fulfills the privilege tree Tp or the hub x, we characterize it as Tp(S) = 1 or x(S) = 1 separately. Tp(S) is figured recursively as takes after. On the off chance that x is a leaf hub, x(S) = 1 if and just if att (x) ∈ S. In the event that x is a non-leaf hub, x(S) = 1 just when in any event kx type hubs return 1. For the root hub Rp of Tp, Tp(S) = 1 just if Rp(S) = 1[10,11,12,13].

IV. PROBLEM FORMULATION

A. Framework Model

In our framework, figure 1 there are five sorts of elements: N Attribute Powers (signified as A), central authority, Cloud Server, Data Owners and Data Consumers. A client can be a Data Owner and a Data Customer all the while. Attribute authority and central authority are accepted to have intense calculation capacities, what's more, they are regulated by government workplaces in light of the fact that a few traits incompletely contain clients' by and by identifiable data. The entire attribute set is partitioned into N disjoint sets and controlled by every attribute authority, along these lines every attribute authority knows about just piece of information. Central authority is the trusted party where data owner and data consumer are communicated to attribute authority through central authority. A Data Owner is the substance who wishes to outsource encoded information record to the Cloud Servers. The Cloud Server, why should expected have sufficient capacity limit, does only store them. Recently joined Data Consumers ask for private keys from all of the Attribute authority , and they don't know which Attribute are controlled by which Attribute authority. At the point when the Data Consumers demand their private keys from the Attribute authority, Attribute authority together make relating private key and send it to them. All Data Consumers can download any of the scrambled information documents, however just those whose private keys fulfil the privilege tree Tp can execute the operation connected with benefit p. The server is designated to execute an operation p if and just if the client's accreditations are checked through the privilege tree Tp.

V. ANONYCONTROL CONSTRUCTION

Setup:

First setup the connection between all the entities like attribute authority, central authority, data owner and data consumer. Here central authority is going act like a admin. It whole control over all the entities. central authority and attribute authority are the trusted parties. This central authority establish the connection between multiple attribute authorities and data user(may be data owner or data user) .

Key generation:

Once the connection is established between multiple attribute authority and central authority global key pairs are generated.

And connection between data owner and attribute authority is established signature is generated by attribute authority. When a new user wants to join the system, he requests the private key from all of the authorities by following this process

1) Attribute Key Generation for every attribute to compute the partial private keys and the valid secret key

2) Key Aggregation: User u, after receiving attribute key aggregates the components as his private key.

Encryption:

Data Owner encrypts the data with any existing symmetric encryption scheme, and generates the decryption key. Then, he determines a set of privilege trees and executes Encryption process. Shamir's secret sharing technique is directly used to implement the threshold gate in privilege trees. Shamir's t-out of-n secret share scheme allows one to divide a secret to n shares, and the original secret can be recovered. So, in our tree, the node value of the gate is recovered if and only if at least particular values of children nodes are recovered in recursive manner. The random number, which is used to mask the decryption key, is stored at the root of the privilege tree and is secret-shared to its children nodes, and the secret shares in the children nodes are secret-shared to their children nodes, so and so forth until the recursive secret sharing reaches the leaf nodes[14].

Decryption:

Every user within the system can download the cipher text from the Cloud Server, but he is able to execute operations on encrypted data only after he successfully decrypts it. A recursive algorithm is used to decrypt the data.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

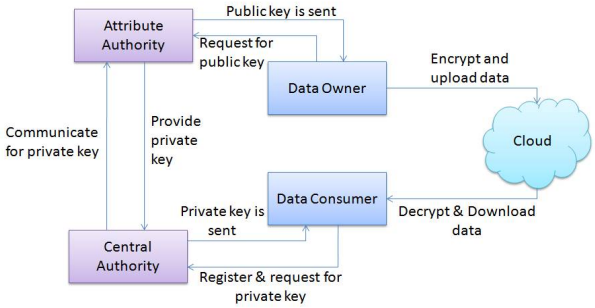

Figure 1:System Architecture.

VI. ACCOMPLISHING FULL ANONYMITY

We have expected semi-fair compelling voices in AnonyControl furthermore, we expected that they won't connive with each other. This is an important suspicion in AnonyControl on the grounds that each power is accountable for a subset of the entire qualities set, also, for the traits that it is accountable for, it knows the careful data of the key requester. In the event that the data from all Attribute authority is accumulated through and through, the complete property set of the key requester is recuperated and accordingly his character is unveiled to the powers. In this sense, AnonyControl is semianonymous since fractional personality data is revealed to every power, except we can accomplish a full-namelessness furthermore permit the plot of the powers. The key purpose of the Attribute data spillage we had in our past plan and also every current characteristic based encryption plans is that key generator.

The RAS algorithm is used for encryption and decryption of data in this paper.

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.RSA involves a *public key* and a *private key*. The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.The basic principle behind RSA is the observation that it is practical to find three very large positive integers *e*,*d* and *n* such that with modular exponentiation for all *m*:

$$(m^e)^d \equiv m \pmod{n}$$

and that even knowing *e* and *n* or even *m* it can be extremely difficult to find *d*.

Additionally, for some operations it is convenient that the order of the two exponentiations can be changed and that this relation also implies:

$$(m^d)^e \equiv m \pmod{n}$$

Key distribution:

To enable Bob to send his encrypted messages, Alice transmits her public key (*n*, *e*) to Bob via a reliable, but not necessarily secret route. The private key is never distributed.

Encryption:

Suppose that Bob would like to send message *M* to Alice.

He first turns *M* into an integer *m*, such that $0 \leq m < n$ and $\gcd(m, n) = 1$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext *c*, using Alice's public key *e*, corresponding to

$$c \equiv m^e \pmod{n}$$

This can be done efficiently, even for 500-bit numbers, using modular exponentiation. Bob then transmits *c* to Alice.

Decryption:

Alice can recover *m* from *c* by using her private key exponent *d* by computing

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

Given *m*, she can recover the original message *M* by reversing the padding scheme.

Key generation:

The keys for the RSA algorithm are generated the following way:

1.Choose two distinct prime numbers *p* and *q*.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits to make factoring harder. Prime integers can be efficiently found using a primality test.
2.Compute $n = pq$.
n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3.Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n-(p+q-1)$, where φ is Euler's totient function. This value is kept private.
4.Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
5.Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$)
This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
e is released as the public key exponent.
d is kept as the private key exponent.
The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.
An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.
Since any common factors of (p − 1) and (q − 1) are present in the factorization of pq − 1,it is recommended that (p − 1) and (q − 1) have only very small common factors, if any besides the necessary 2.

VII. SECURITY ANALYSIS

A. *Resistance Against Authorities' Collusion*

Resistance Against Authorities' Collusion on the other hand Compromise Attack In the proposed plan, a Attribute authority Ak creates a set of irregular secret parameters {skj } and offers gskj it with different Attribute authority by means of secure channel, and xk is figured taking into account this parameters. It is trusted that DDH issue is immovable in the gathering G0 of prime request p, hence gskj does not release any factual data about skj. This infers regardless of the possibility that a foe can bargain up to (N − 2) Attribute authority, there are still two parameters skj kept obscure to the enemy. Thus, the foe is not ready to surmise the legitimate g∑vk , and he neglects to build a substantial secret key. Consequently, the plan accomplishes bargain resilience to up to (N − 2) Attribute authority trade off. In any case, on the off chance that we diminish the time multifaceted nature of the setup stage by isolating Attribute authority into a few groups having C dominant presences in every, assailants can trade off C − 1 dominant presences in a bunch to make legitimate master keys of that bunch. Along these lines, there is a tradeoff in the middle of resistance and multifaceted nature. Be that as it may, following the number of Attribute authority is commonly not exceptionally enormous, and the setup is one-time operation at the earliest reference point of the framework setup, we suggest utilizing the first setup calculation whose multifaceted nature is O(N2).
Note that the traded off powers can issue legitimate Attribute keys for which they are responsible for, so the ciphertexts whose privilege trees have just those traits may be illicitly unscrambled if the aggressor issue all conceivable Attribute keys to himself. Be that as it may, subsequent to Attribute authority are well secured servers, it is difficult to trade off even one Attribute authority[16], what's more, the likelihood of trading sufficiently off Attribute authority to illicitly unscramble some ciphertext is low.

B. Resistance Against Users' Collusion Attack

With a specific end goal to get to a plaintext, aggressors must recuperate Y s0 = e(g, g)s0∑vk , which can be recuperated just if the aggressors have enough credits to fulfill the tree T0. At the point when two distinct keys' parts are consolidated, the joined key can't experience the polynomial interjection in the decoding calculation because of the diverse randomizers in each key. Along these lines, no less than one key ought to be substantial to fulfill a privilege tree.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Special Issue 10, May 2016

VIII. 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.

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: Springer-Verlag, 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.