Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 04, April -2018

IMPROVING SECURITY AND EFFICIENCY IN ATTRIBUTE BASED DATA SHARING USING CLOUD COMPUTING

Rohan Shendkar[1], Saurabh Kshirsagar[2], Sharayu Kotkar[3] , Monika Rokade[4]
Prof. Aparna Lavangade

[1]*Department of Computer Engineering, Indira College Engineering and Management –PUNE*
[21]*Department of Computer Engineering, Indira College Engineering and Management –PUNE*
[31]*Department of Computer Engineering, Indira College Engineering and Management –PUNE*
[41]*Department of Computer Engineering, Indira College Engineering and Management –PUNE*

Abstract — *For secure information partaking in cloud figure content approach property based encryption is promising on the grounds that information proprietor having full control over access arrangement of shared information. However, CP-ABE having a key escrow issue whereby the mystery keys of clients must be issued by a trusted key specialist. CP-ABE plans can't bolster property with self-assertive state. So we return to credit based information sharing to settle the key escrow issue yet in addition enhance the expressiveness of property, so the subsequent plan is all the more agreeable to distributed computing applications. We propose an enhanced two-party key issuing convention that can Guarantee that neither key specialist nor cloud specialist co-op can trade off the entire mystery key of a client exclusively. In addition, we present the idea of property with weight, being given to upgrade the declaration of characteristic, which can not just stretch out the articulation from twofold to subjective state, yet in addition help the unpredictability of access strategy.*

Keywords; *Secure data sharing, Attribute-based encryption, Removing escrow, Weighted attribute, Cloud computing.*

I. INTRODUCTION

In ciphertext trait base encryption conspire (CP-ABE) is a safe encryption procedure use in distributed computing. In this plan Data proprietor has full specialist to dole out all entrance consent .But In late situation information client are increment, so with the expanding number of cloud clients there is a danger of clients mystery key will be escrow. Key of information proprietor will be oversee or escrow on the grounds that the key specialist or cloud specialist co-op both are not trusted. So to oversee key of information proprietors and execute quality with self-assertive state. So we propose a plan with two gathering key issuing system with weighted property. along these lines both capacity cost and encryption unpredictability for ciphertext are explain. The weighted ascribe is acquainted with not just stretch out credit articulation from twofold to discretionary state, yet additionally to disentangle get to arrangement. Therefore, the capacity cost and encryption cost for a ciphertext can be assuaged. We utilize the accompanying case to additionally represent our approach. We propose a characteristic based information sharing plan for distributed computing applications, which is meant as ciphertext-approach weighted ABE plot with evacuating escrow (CP-WABE-RE). It effectively settle two sorts of issues: key escrow and subjective satiate property articulation. The commitments of our work are as per the following: we propose an enhanced key issuing convention to determine the key escrow issue of CP-ABE in distributed computing. The convention can keep KA and CSP from knowing each other's lord mystery key with the goal that none of them can make the entire mystery keys of clients independently Thus, the completely trusted KA can be semi-trusted. Information secrecy and protection can be guaranteed.

II. LITERATURE SURVEY

1] Improving Privacy and Security in Multi-Authority Attribute-Based Encryption
AUTHORS: Melissa Chase, Sherman S.M. Chow
Description: Multi-specialist property based encryption empowers a more practical sending of quality based access control, with the end goal that diverse experts are in charge of issuing distinctive arrangements of characteristics. The first arrangement by Chase utilizes a put stock in focal expert and the utilization of a worldwide identifier for every client, which implies the secrecy depends basically on the security of the focal specialist and the client protection relies upon the fair conduct of the quality experts. We propose a trait based encryption plot without the put stock in expert, and a mysterious key issuing convention which works for both existing plans and for our new development.

2] Randomizable Proofs and Delegatable Anonymous Credentials
AUTHORS: Mira Belenkiy, Jan Camenisch , Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham.

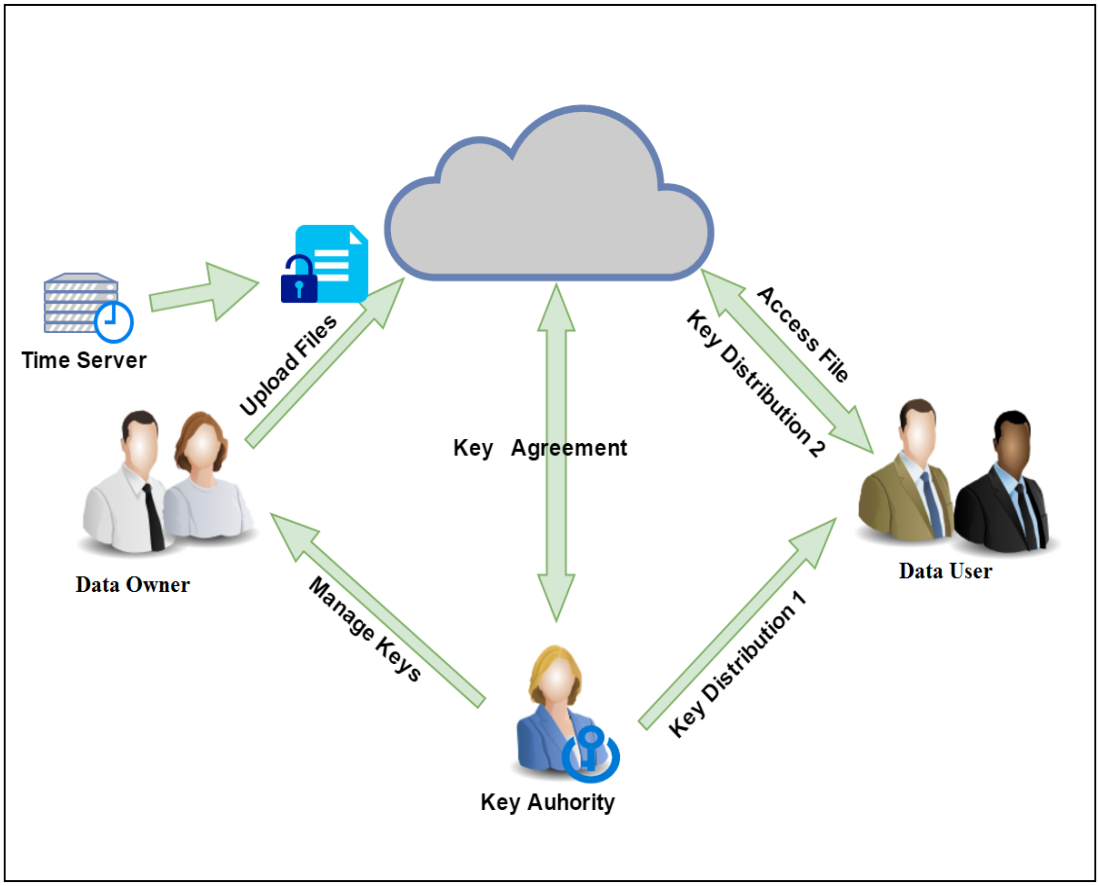
Description: In this paper We reexamine the whole way to deal with developing unknown qualifications and distinguish randomizable zero-learning verification of information frameworks as the key building square. We formally characterize the thought of randomizable non-intelligent zero-information confirmations, and give the primary case of controlled rerandomization of non-intuitive zero-learning proofs by an outsider. Our development utilizes Groth-Sahai proofs.

3] Removing Escrow from Identity-Based Encryption
AUTHORS: Sherman S.M. Chow
Description: In this paper we initially demonstrate to prepare an IBE plot by Gentry with ACI − KGC. Second, we propose another framework design with an unknown private key age convention to such an extent that the KGC can issue a private key to a verified client without knowing the rundown of clients personalities. This too better matches the training that confirmation ought to be finished with the nearby enlistment experts rather than the KGC. Our proposition can be seen as alleviating the key escrow issue in an unexpected measurement in comparison to dispersed KGCs approach.

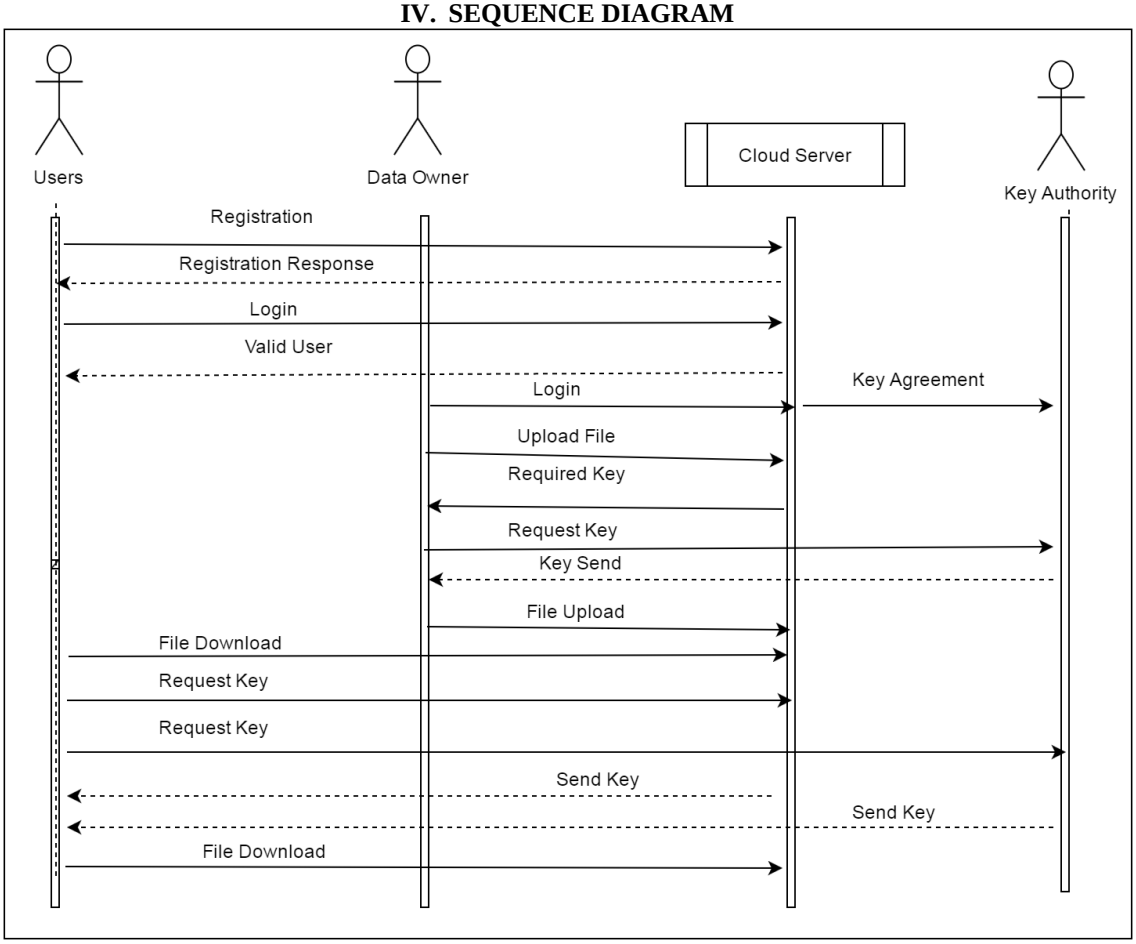
4] Arbitrary-State Attribute-Based Encryption with Dynamic Membership
AUTHORS: Chun-I Fan, Vincent Shi-Ming Huang, He-Ming Ruan.
Description: In this paper, we proposed a ciphertext-strategy trait based encryption plot with dynamic participation. A client is permitted to select and leave from an ABE framework, and she/he can likewise change her/his characteristics and the qualities comparing to the traits. It is superfluous for any other person to refresh her/his private key when enlistment, leaving, or characteristic refreshing happens. Likewise, to the best of our insight, our plan is the main ABE plot which can bolster discretionary state traits and characteristic (and esteem) refreshing with Sender Updating Only. These favorable circumstances will make an ABE benefit more productive and adaptable for pragmatic applications.

5] Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data
AUTHORS: Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters
Description: In this paper, we acquaint new methods with execute fine grained get to control. In our strategies, the information is put away on the server in an encoded shape while diverse clients are still permitted to unscramble distinctive bits of information per the security arrangement. This adequately disposes of the need to depend on the capacity server for anticipating unapproved information get to.

III. SYSTEM ARCHITECTURE



IV. SEQUENCE DIAGRAM



V MATHEMATICAL MODEL

INPUT:-

Let S be the Whole system S= {I,P,O}
I-input
P-procedure
O-output
Where,
Input (I):
I= F
Where F is Collection of documents which created by owner
F= f1, f2,.. , fn
f1, f2 { document fragmentation}
κ=security parameter
PP=public parameter
G_0 = bilinear group
P=prime order
g=Generator
qx=polynomial
S=Set of weighted attribute.
t=Users
Procedure(p):
P={SI,De,Kg,De}
CP-WABE-RE contains four phases
Phase 1:System Initialization.{SI}
It includes: **KA**.**Setup** and **CSP**.**Setup**.
(1) **KA**.**Setup**(1κ). KA runs the algorithm which inputs a security parameter κ. Then, KA chooses random $\alpha 1, \beta \in Zp$ and computes $h = g\beta$ and $u1 = \hat{e}(g, g)\alpha 1$. Lastly, it obtains PP1 and MSK1 as the formula
:PP1 = {G0, g, h, $u1$}, MSK1 = {$\alpha 1$, β}

(2) **CSP**.**Setup**(**1**κ). CSP executes the operation which inputs a security parameter κ. Based on the κ, CSP chooses a random number $\alpha 2 \in Zp$ and calculates $u2 = \hat{}e(g, g)\alpha 2$. Then, it sets PP2 and MSK2 as the formula :
PP2 = $\{u2\}$, MSK2 = $\{\alpha 2\}$
Finally, the public parameter and master secret key of system
are denoted as PP = $\{G0, g, h, u = u1 \cdot u2 = \hat{}e(g, g)\alpha\}$,
where $\alpha = \alpha 1 + \alpha 2$, and MSK = $\{\{\alpha 1, \beta\}, \{\alpha 2\}\}$.

Phase2:Data Encryption{De}:(PP, *ck*, *T*).
The improved algorithm is executed by DO which inputs PP, *ck* and *T* . It outputs CT. beginning from the root node *R*, DO sets $qR(0) = s(s \in Zp)$, where *s* is randomly selected. And DO randomly selects *dR* other points of the polynomial *qR* to define it completely. For each non-root node *x*, it sets $qx(0)$ $qparent(x)(index(x))$ and randomly chooses *dx* other points to completely define *qx*. Meanwhile, each leaf node denotes an attribute with weight.
Finally, DO sends the integrated ciphertext $\{ID, CT, Eck(M)\}$ to CSP.

Phase 3 : **User Key Generation{Kg}**. This phase consists of **KA**.**KeyGen** and **CSP**.**KeyGen**.
KA.**KeyGen:** (MSK1, *r*, *S*):input to KA is $r \in Zp$ chosen randomly. for each weighted attribute $j \in S$, it possesses weighted value $\omega j(\omega j \in W)$. Finally, it computes SK1 described by *S* as the formula :
SK1 = $\{L = g^r, \forall_j \in S : D_j = H(j)^{r\omega j}\}$ and complet key is
SK= $\{D = g^{\alpha}h^r, L = g^r, \forall_j \in S : D_j = H(j)^{r\omega j}\}$

CSP.**KeyGen**. We provide an improved key issuing protocol between KA and CSP to execute the work of CSP.
KeyComKA↔CSP(MSK1, *IDt*, *r*,MSK2). Assume that user *t* needs a secret key
KA choose $r \in Zp$ for users, CSP selects a random number $\rho 1 \in Zp$ to calculate
$X1 = g^{x/\rho 1} = g^{(\alpha 1+\alpha 2)\beta/\rho 1}$ and transmits $\{X1, PoK(\rho 1, x)\}$ to KA.
CSP calcultes $D = Y^{1/\rho 2}_3 = g^{(\alpha 1+\alpha 2)}h^r = g^{\alpha}h^r$ and sends a personalized key component SK2 = $\{D = g^{\alpha}h^r\}$ to the corresponding user *t*.

Phase 4:Data Decrypt{De} ($Eck(M)$, *ck*):
User inputs file ciphertext $Eck(M)$ and content key *ck*
Dck denotes a symmetric decryption operation with the key *ck*.
$Dck[Eck(M)] = M$.
Output:
Users decrypt data by using both keys and they get data in decrypted format if both keys are at users and user is valid.

Data structure use in this project is stack.

VI. CONCLUSION

Overhauled a attribute based information sharing plan in distributed computing. The enhanced key issuing convention was exhibited to determine the key escrow issue. It improves information secrecy and protection in cloud framework against the supervisors of KA and CSP and also noxious framework pariahs, where KA and CSP are semi-trusted. Moreover, the weighted ascribe was proposed to enhance the declaration of property, which can portray arbitrarystate properties, as well as decrease the many-sided quality of access arrangement, with the goal that the capacity cost of ciphertext and time cost in encryption can be spared.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFRENCES

[1] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of smart grid. *IEEE Transactions on Cloud Computing*, 3(2):233–244, 2015.
[2] A. Balu and K. Kuppusamy. An expressive and provably secure ciphertext-policy attribute-based encryption. *Information Sciences*, 276(4):354–362, 2014.
[3] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. *Proceedings of the 29th Annual International Cryptology Conference*, pages 108–125, 2009.
[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attributebased encryption. *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, 2001.
[6] M. Chase. Multi-authority attribute based encryption. *Proceedings of the 4th Conference on Theory of Cryptography*, pages 515–534, 2007.
[7] M. Chase and S. S. Chow. Improving privacy and security in multiauthority attribute-based encryption. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pages 121–130, 2009.
[8] L. Cheung and C. Newport. Provably secure ciphertext policy ABE. *Proceedings of the 14th ACM conference on Computer and communications security*, pages 456–465, 2007.
[9] S. S. Chow. Removing escrow from identity-based encryption. *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography*, pages 256–276, 2009.
[10] C. K. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou. Security concerns in popular cloud storage services. *IEEE Pervasive Computing*, 12(4):50–57, 2013.
[11] A. De Caro and V. Iovino. JPBC: java pairing based cryptography. *IEEE Symposium on Computers and Communications*, 22(3):850–855, 2011.
[12] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and W. Shi. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. *Information Sciences*, 275(11):370–384, 2014.
[13] C. Fan, S. Huang, and H. Rung. Arbitrary-state attribute-based encryption with dynamic membership. *IEEE Transactions on Computers*, 63(8):1951–1961, 2014.
[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98, 2006.
[15] J. Hur. Improving security and efficiency in attribute-based data sharing. *IEEE Transactions on Knowledge and Data Engineering*, 25(10):2271– 2282, 2013.

