Scientific Journal of Impact Factor (SJIF): 4.14

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

International Journal of Advance Engineering and Research Development

Volume 3, Issue 9, September -2016

Improving Security using Arbitrary state attribute Base Encryption

Suraj Kumar[1], Rohit Rai[2],Abhishek Poddar[3]

Department of Computer engineering, Dr D Y patil institute of engineering and technology,ambi ,pune

Abstract — *For secure knowledge sharing in cloud cipher text policy attribute based mostly coding is promising as a result of knowledge owner having full management over access policy of shared knowledge. however CP-ABE having a key written agreement downside whereby the key keys of users need to be issued by a trusty key authority. CP-ABE schemes cannot support attribute with absolute state. Thus we have a tendency to get back attribute-based knowledge sharing to resolve the key written agreement issue however additionally improve the quality of attribute, in order that the ensuing theme is a lot of friendly to cloud computing applications. we have a tendency to propose AN improved two-party key issuance protocol will that may Guarantee that neither key authority nor cloud service supplier can compromise the total secret key of a user one by one. Moreover, we have a tendency to introduce the conception of attribute with weight, being provided to boost the expression of attribute, which may not solely extend the expression from binary to absolute state, however additionally lighten the quality of access policy, additionally time server is additional and it provides file interval.*

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

I. INTRODUCTION

In ciphertext attribute base coding theme (CP-ABE) could be a secure coding technique use in cloud computing. during this theme information owner has full authority to assign all access permission .But In recent situation information user area unit increase, thus with the increasing range of cloud users there's a risk of users secret key are written agreement. Key of knowledge owner are manage or written agreement as a result of the key authority or cloud service supplier each don't seem to be trusty. thus to manage key of knowledge homeowners and implement attribute with whimsical state. thus we tend to propose a theme with 2 party key provision mechanism with weighted attribute. thus each storage price and coding quality for ciphertext area unit solve.

The weighted attribute is introduced to not solely extend attribute expression from binary to whimsical state, however additionally to modify access policy. Thus, the storage price and coding price for a ciphertext will be alleviated. we tend to use the subsequent example to additional illustrate our approach.

The weighted attribute is introduced to not solely extend attribute expression from binary to whimsical state, however additionally to modify access policy. Thus, the storage price and coding price for a ciphertext will be alleviated. we tend to use the subsequent example to additional illustrate our approach.

We propose AN attribute-based information sharing theme for cloud computing applications, that is denoted as ciphertext-policy weighted ABE theme with removing written agreement (CP-WABE-RE). It with success resolves 2 forms of problems: key written agreement and arbitrary-sate attribute expression.

We propose AN improved key provision protocol to resolve the key written agreement downside of CP-ABE in cloud computing. The protocol will forestall Ka and CSP from knowing every other's master secret key so none of them will produce the complete secret keys of users on an individual basis therefore, the totally trusty Ka will be semi-trusted. Data. We divide a conventional attribute in 2 elements 1st is attribute and second is its price. for instance, the standard attributes will be denoted as . The improved attributes area unit denoted as: , wherever "Career" represents AN attribute and "Doctor", "Professor" and "Engineer" denote the values of the attribute "Career".

Time server is supplemental in whereas uploading the file and specify time thereupon file so file is accessible to users just for time assign by time server.

SCOPE - Redesigned Associate in Nursing attribute-based information sharing theme in cloud computing and improved key supplying protocol for to resolve the key written agreement drawback. It enhances information confidentiality and privacy in cloud system against the managers of Hindu deity and CSP further as malicious system outsiders, wherever Hindu deity and CSP area unit semi-trusted. Additionally, the weighted attribute improves the expression of attribute,

which might not solely describe capricious state attributes, however conjointly cut back the complexness of access policy, in order that the storage value of cipher text and time value in coding is saved

II .LITRATURE SURVEY

2.1 Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Authors: Melissa Chase, Sherman S.M. Chow

Description: It is surreal to assume there's one authority which might monitor each single attribute of all users. Multi-authority attribute-based encoding allows a lot of realistic readying of attribute-based access management, specified totally different authorities square measure chargeable for issuance different sets of attributes. The first answer by Chase employs a trustworthy central authority and also the use of a world symbol for every user, which implies the confidentiality depends critically on the safety of the central authority and also the user-privacy depends on the honest behavior of the attribute-authorities.

2.2 Randomizable Proofs and Delegable Anonymous Credentials

Authors: Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham

Description: Users will anonymously and unlink ably acquire credentials for many authority, delegate their credentials to alternative users, and prove possession of a certificate L levels off from a given authority. we tend to revise the complete approach to constructing anonymous credentials and determine randomizable zero-knowledge proof of data systems because the key building block. we tend to formally outline the notion of randomizable non-interactive zero-knowledge proofs, and provides the primary instance of controlled re-randomization of non-interactive zero-knowledge proofs by a third-party.

2.3 Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Authors: Melissa Chase, Sherman S.M. Chow.

Description: It is unrealistic to assume there's one authority which might monitor each single attribute of all users. Multi-authority attribute-based encoding allows a lot of realistic preparation of attribute-based access management, such totally different authorities square measure answerable for issuance different sets of attributes. The first resolution by Chase employs a trustworthy central authority and therefore the use of a world symbol for every user, which suggests the confidentiality depends critically on the protection of the central authority and therefore the user-privacy depends on the honest behavior of the attribute-authorities.

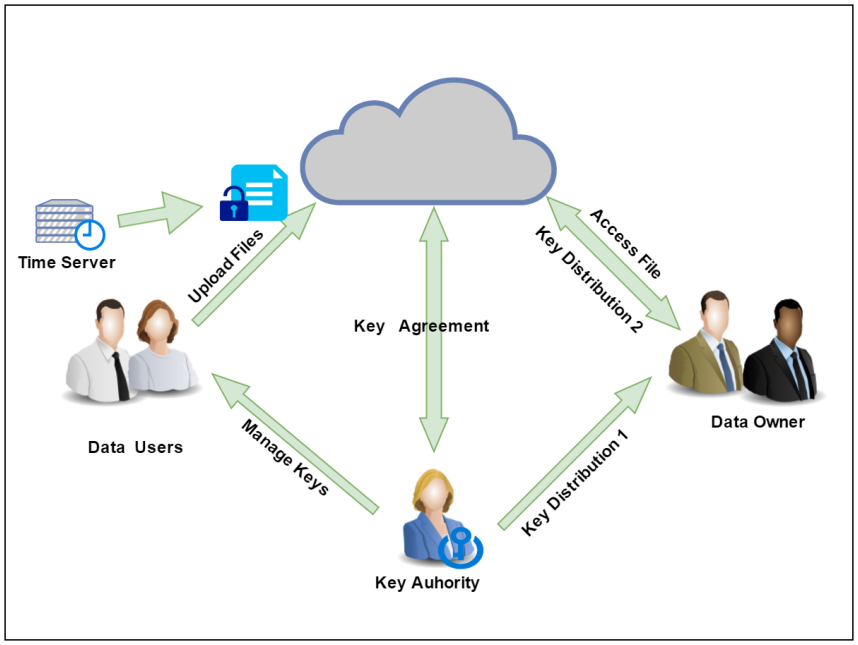
III. PRAPOSED SYSTEM:

We propose associate attribute-based knowledge sharing theme for cloud computing applications, that is denoted as cipher text-policy weighted ABE theme with removing written agreement (CP-WABE-RE). we tend to propose associate improved key issuance protocol to resolve the key written agreement downside of CP-ABE in cloud computing. The protocol will stop Ka and CSP from knowing every other's master secret key in order that none of them will produce the total secret keys of users on an individual basis therefore, the totally trusty Ka will be semi-trusted. knowledge confidentiality and privacy will be ensured. we tend to gift weighted attribute to boost the expression of attribute. The weighted attribute cannot solely specific arbitrary-state attribute (instead of the normal binary state), however conjointly cut back the quality of access policy. therefore the storage price of cipher text and computation quality in coding will be reduced. Besides, it will specific larger attribute house than ever beneath constant condition. we tend to conduct and implement comprehensive experiment for the planned theme. The simulation shows that CP-WABE-RE theme is economical each in terms of computation quality and storage price. additionally, the safety of CP-WABE-RE theme is additionally established beneath the generic cluster model. Time server is introducing for distribution a time interval with file at time of uploading. thus this file is accessible to user just for time such that by time server.

3.1 CP-WABE-RE(Ciphertext policy-Weighted attribute base encryption revisited in cloud)

In Ciphertext- policy attribute base cryptography Associate in Nursing improved key issuance protocol to resolve the key written agreement drawback of CP-ABE in cloud computing. The protocol will stop Hindu deity and CSP from knowing

every other's master secret key in order that none of them will produce the total secret keys of users singly therefore, the totally trustworthy Hindu deity is semi-trusted. knowledge confidentiality and privacy is ensured. we tend to gift weighted attribute to boost the expression of attribute. The weighted attribute cannot solely specific arbitrary-state attribute (instead of the normal binary state), however additionally scale back the quality of access policy.
Weighted attribute to boost the expression of attribute. The weighted attribute cannot solely specific arbitrary-state attribute (instead of the normal binary state), however additionally scale back the quality of access policy. therefore the storage value of ciphertext and computation quality in cryptography is reduced. Besides, it will specific larger attribute area than ever underneath constant condition



3.2 Key Authority (KA).
It is a semi-trusted entity in cloud system. Namely, Ka is honest-but-curious, which may honestly perform the appointed tasks and come back correct results. However, it'll collect as several sensitive contents as potential. In cloud system, the entity is chargeable for the users' enrollment. Meanwhile, it not solely generates most a part of system parameter, however additionally creates most a part of secret key for every user.

3.3 Time Server
In our system we tend to propose a Time Server. we tend to use Time server in our system for assignment a time to a file that is uploading in cloud. By assignment a time to file we tend to outline a time base access permission to file. By assign a time to file specific user access this file for that point amount solely .After assign time is completed file is mechanically unavailable for user for access.

3.4 Advantages of propose system:
2.4.1 Proposed an arbitrary-state ABE to solve the issue of the dynamic membership management.

2.4.2 The attributes are divided into multiple levels to achieve fine-grained access control for hierarchical attributes, but the attributes can only express binary state.

IV. Mathematical Model

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*, *u*1}, MSK1 = {$\alpha 1, \beta$}

(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 = {*u*2}, 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 {*X*1,PoK(ρ1, *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*.

V. CONCLUSION

In this paper, we tend to style an improved attribute base sharing theme is cloud computing. This improved protocol was conferred to unravel a key written agreement downside in cloud computing. Additionally improves a confidentiality and privacy in cloud computing against Key authority and cloud service suppliers and additionally from any outside malicious system. In addition, the weighted attribute was projected to enhance the expression of attribute, which may not solely describe arbitrary state attributes, however additionally scale back the complexness of access policy, so the storage value of ciphertext and time value in cryptography will be saved. Finally, we tend to conferred the performance and security analyses for the projected theme, during which the results demonstrate high potency and security of our theme.

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.

VI. 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.

AUTHORS

