International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 02 – Issue 10 || October 2017 || PP. 37-42

Enhancing Reliability and Efficiency for Quality Based Data Sharing In Cloud Computing

M. Vijaya Durga Rasamayi[1], Prof. R. Suresh[2]

*[1]M.Tech, Chadalawada Ramanamma Engineering College, Chadalawada Nagar,
Renigunta Road,Tirupati*
*[2]Professor, Chadalawada Ramanamma Engineering College, Chadalawada Nagar,
Renigunta Road,Tirupati*

Abstract: In gift system, there's conjointly Associate in Nursing economical file hierarchy attribute-centered cryptography theme in cloud computing. The bedded access structures area unit constitutional into one access constitution, and then the hierarchal documents area unit encrypted with the constitutional access structure. The ciphertext components involving attributes can be shared by technique of the records. Consequently, each ciphertext storage and time rate of cryptography area unit saved. To boot, the planned theme is tested to be snug below the general assumption. Experimental simulation indicates that the planned theme is unbelievably effective in terms of cryptography and cryptography. With the number of the files growing, the advantages of our theme grow to be a lot of and a lot of conspicuous. We have a tendency to tend to advocate a very distinctive CP-ABE theme for Associate in nursing information sharing technique by victimization exploiting the characteristic of the tactic structure. The planned theme points resulting achievements: (1) the key legal instrument crisis may well be resolved by escrow-free key issue protocol, that's developed utilizing the secure two-social gathering computation between the important issue new unhitch core and conjointly the data storing center, (2) high-quality-grained user revocation per each and every attribute can be completed with the assistance of proxy cryptography that takes competencies of the selective attribute crew key distribution on high of the ABE. The efficiency and protection analyses indicate that the planned theme is effective to soundly manage the data assigned among the info sharing procedure.

Index Terms: Data sharing, attribute-based encoding, revocation, access management, removing written agreement

Introduction:

With the burgeoning of network science and cell terminal, on-line information sharing has end up an innovative “pet”, harking back to facebook, MySpace, and Badoo. Meanwhile, cloud computing is one in each of the foremost promising utility platforms to remedy the explosive increasing of knowledge sharing. In cloud computing, to shield information from leaky, users have gotten to write down in code their info before being shared. Entry manage is dominant because it is that the initial line of protection that forestalls unauthorized entry to the shared info. Merely lately, attribute situated committal to writing (ABE) has been attracted rather plenty of attentions because of the particular indisputable fact that it would very preserve info privacy and fully grasp first-rate-grained, one-to-many, and non-interactive entry manipulates. Ciphertext-coverage attribute situated committal to writing (CP-ABE) is taken into consideration one in each of potential schemes that has far more flexibility and is extra applicable for common applications.

Up to currently development of the network and computing science permits for many folks to effortlessly share their info with others victimization on-line external storages. Humans can share their lives with acquaintances by suggests that of uploading their personal graphics or messages into internet social networks hold dear Facebook and MySpace; or add very touchy personal successfulness documents (PHRs) into on-line info servers hold dear Microsoft health Vault, Google successfulness for straightforward sharing with their foremost medical professionals or for price saving. As folks fancy the advantages of these new applied sciences and offerings, their issues concerning information protection and access manage as well come back up. Mistaken use of the info by suggests that of the storage server or unauthorized entry by suggests that of outside users may be advantage threats to their info. People would like to produce their sensitive or exclusive info solely accessible to the authorized folks with credentials them actual. Attribute-established committal to writing (ABE) is also a promising science strategy that achieves a fine-grained info entry manipulate. It provides how of shaping entry insurance policies supported distinctive attributes of the requester, atmosphere, or the data object.

Peculiarly, ciphertext-coverage attribute-founded committal to writing (CP-ABE) permits for associate encryptor to stipulate the attribute set over a universe of attributes that a decoder has to possess with the intention to decode the ciphertext, and place smart it on the contents. As a result, each shopper with an additional set of attributes is allowed to decipher one in each of a kind piece of knowledge per the protection coverage. This effortlessly eliminates the ought to depend on the data storage server for preventing unauthorized info access, that's that the natural entry manage strategy of like a results of the reference reveal.

Data Sharing Architecture:

System Description and Key Management:

Fig. 1 shows the architecture of the data sharing system, which consists of the following system entities.

Key generation middle: It's a key authority that generates public and secret parameters for CPABE. It's answerable of provide, revoking, and alter attribute keys for purchasers. It guarantees differential entry rights to individual customers targeted on their attributes.

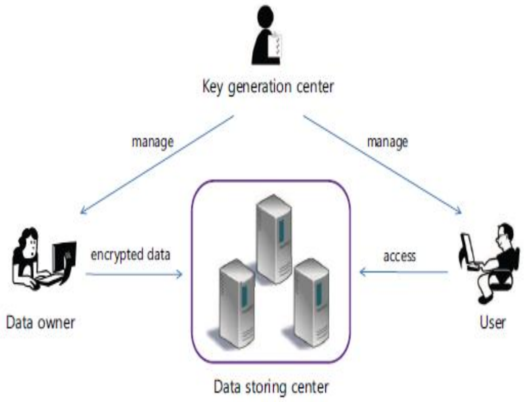

Fig. 1. Architecture of a data sharing system

It's assumed to be honest but- curious. That is, it's planning to honestly execute the allotted tasks at intervals the procedure; however, it wish to be tutored power of encrypted Contents per se plenty as possible. For this reason, it ought to be averted from having access to the plaintext of the encrypted data despite the particular indisputable fact that it's honest.

Data storing middle: It's associate degree entity that features a data sharing service. It's answerable of dominant the accesses from external users to the storing data and providing corresponding contents offerings. The information storing core is a further key authority that generates made-to-order user key with the KGC, and problems and revokes attribute cluster keys to legitimate customers per every attribute, that unit of measurement used to implement a best-grained shopper access manipulate. Reasonably just like the sooner schemes, we've a bent to expect the information storing middle may additionally be semi-depended on (that is, sincere-however-curious) rather just like the KGC.

Data owner: it is a shopper United Nations agency owns information, and desires to feature it into the surface information storing center for easy sharing or for fee saving. Associate degree information owner is accountable for outlining (attribute situated) entry policy, and implementing it on it possess information by encrypting the data below the policy before distributing it.

Consumer: its associate degree entity United Nations agency wishes to access the data. If a shopper possesses a set of attributes pleasing the entry coverage of the encrypted information, and isn't revoked in any of the legitimate attribute corporations, then he's planning to be competent to rewrite the ciphertext and acquire the information. Seeing that each of the important issue managers, the KGC and thus the information storing center, unit of measurement semi-trusted, they have to be compelled to be deterred from gaining access to plaintext of the information to be shared; within the within the meanwhile, they're going to have to be compelled to be notwithstanding capable to limitation secret keys to users. With a purpose to know this fairly contradictory demand, the two parties have interaction among the arithmetic 2PC protocol with master secret keys of their possess, and mental confusion impartial key add-ons to customers at intervals the course of the important issue provide section. The 2PC protocol deters them from knowing each different grasp secrets and techniques therefore none of them can generate the whole set of secret keys of users severally. Therefore, we've a bent to require associate degree assumption that the KGC does not conspire with the information storing center due to the particular truth they're honest as in (otherwise, they're going to guess the key keys of every user with the assistance of sharing their master secrets and techniques).

Proposed CP-ABE Scheme:

In view that the primary CP-ABE theme planned through Bethencourt et al., dozens of consecutive CP-ABE schemes area unit endorsed, that might be sometimes affected by methodology of further rigorous protection proof within the traditional model. However, most of the schemes did not acquire the standard of the Bethencourt et al.'s theme that painted a cheap approach that was expressive during this it allowed associate degree encryptor to specific associate degree entry predicate in terms of any monotonic technique over attributes. As a result, on this section, we have a tendency to tend to enhance a variation of the CP-ABE formula part settled on (however not restricted to) Bethencourt et al.'s construction so on enhance the standard of the access manage coverage instead of building a unique CP-ABE theme from scratch. Its key iteration procedure is modified for our intent of doing away with official document. The planned theme is then created on this new CP-ABE version with the assistance of additional group action it into the proxy re-encryption protocol for the person revocation.

To handle the fine-grained shopper revocation, the information storing core need to be compelled to accumulate the client entry (or revocation) record for each and every attribute staff, once you are taking into consideration that within the alternative case revocation cannot take result finally. These surroundings where the information storing middle is tuned in to the revocation list does not violate the protection standards, for the explanation that it's exclusively allowed to re-encrypt the ciphertexts and would possibly in no methodology acquire any understanding relating to the attribute keys of users. On account that the planned theme is built on, we have a tendency to tend to recapitulate some definitions in to clarify our development on this, quite like entry tree, encrypt, and decipher formula definitions.

1) Setup(1^k)
$PK= \{G_{0,} g, h=g^{\beta}, e(g,g)^{\alpha}\}$
$MSK= \{ g^{\alpha},\beta \}$

2) KeyGen (PK,MSK,S)
$SK = \{ D = g^{\alpha} . h^r \}$
$\{ D_j = g^r . H_1 (j)^r_j , D'_j = h^r_j \}$

3) Encrypt :
$C_{(x,y)} = h^{q(x,y)(0)}$
$C'_{(x,y)=} H1(att(x,y))^{q(x,y)(0)}$

4) Decrypt:
DecryptNode(CT,SK,(x,y))

$$= \frac{e(D_i,C_{(x,y))}}{e(D'_i, C'(_{x,y))}}$$

$$= \frac{e(g_r H_1(i)^r_{i,} h^{q(x,y)(0))}}{e(h^r_i, H_1(att(x,y)^{q(x,y)(0))}}$$

$$= e(g,g)^{r\beta q(x,y)(0)}$$

Scheme Analysis:

On this half, we tend to tend to investigate and compare the ability of the planned theme with the earlier CP-ABE schemes (that is, Bethencourt et al.'s theme (BSW), Attrapadung's theme (BCP-ABE2), and Yu et al.'s theme (YWRL) in theoretical and wise aspects. Then, the efficiency of the planned theme is valid among the network simulation in terms of the voice communication fee. We tend to tend besides discuss its power once applied with actual parameters and assess these results with these got through the alternative schemes.

Key understanding and Revocation (Key escrow and revocation)

Table one suggests the revocation roughness and key understanding drawback of every theme. The rekeying among the planned theme is going to be completed in a right away approach versus BSW. For that reason, a user are going to be revoked at any time even previous the expiration time that perhaps set to the attribute. This enhances protection of the shared data in terms of the backward/ahead secrecy by decreasing the house windows of vulnerability. Moreover, the planned theme realizes extra exceptional-grained user revocation for each and every attribute rather than for the whole procedure. For that reason, albeit a private drops some attributes at intervals the course of the carrier among the planned theme, he can still entry the knowledge with fully completely different attributes that he is maintaining as long as they satisfy the entry policy. The planned theme in addition resolves the important issue understanding quandary as a result of the escrow-free key issue protocol exploiting relaxed 2PC protocol versus the opposite schemes.

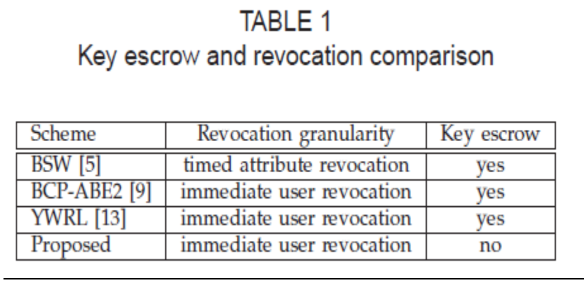

TABLE 1
Key escrow and revocation comparison

Scheme	Revocation granularity	Key escrow
BSW [5]	timed attribute revocation	yes
BCP-ABE2 [9]	immediate user revocation	yes
YWRL [13]	immediate user revocation	yes
Proposed	immediate user revocation	no

Efficiency

Within the assessment outcome, each and every theme is once place next in terms of ciphertext size, rekeying message live, exclusive and public key size. Ciphertext size implies the communication fee that data the information} owner must send to information storing middle its knowledge, or that the knowledge storing middle must send to users (CT' among the projected scheme). Rekeying message size represents the story price that the KGC or the knowledge storing middle needs to ship to be able to replace non revoked users' keys (Hdr within the projected scheme) in associate attribute crew or to revoke associate attribute. Confidential Key size represents the storage price required for every consumer to distributor secret keys. Public key size represents the dimensions of the authorities' public keys among the procedure.

Implementation:

Subsequent, we have a tendency to tend Analyze to, research to investigate} Associate in Nursing live the computation value for encrypting (by an data owner) and decrypting (by suggests that of a consumer) an data. The cryptography price by methodology of a user entails the operations for decrypting the rekeying message just about pretty much as good as a result of the knowledge (in [13] and thus the projected scheme).We used a spread A curve (within the pairing-headquartered cryptography (PBC) library [20]) providing groups among that a additive map e: G0 × G0 → G1 is written. Notwithstanding such curves furnish glorious method efficiency (especially for pairing computation), the equal can now not keep from the difficulty of scan of the area required to symbolize cluster factors. truly each and every detail of G0 needs 512 bits at associate 80-bit security stage and 1536 bits once 128-little bit of safety unit chosen.

Performance Analysis:

To validate theoretical analysis, we implement FH-CP-ABE scheme based on the cpabe toolkit and the Java Pairing-Based Cryptography library (JPBC).When the number of files is fixed, the more the attributes is used, the more time cost of encryption and decryption in FH-CP-ABE.

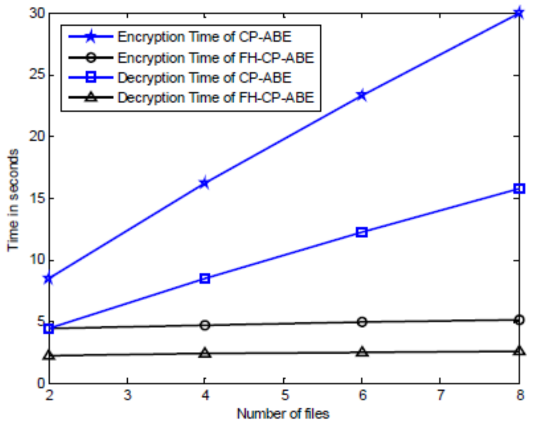

Fig: comparison of the encryption and decryption cost under 30 attributes

If the number of files is fixed, the more the number of attributes is used, the higher efficiency in our scheme is improved in terms of storage cost of ciphertext.

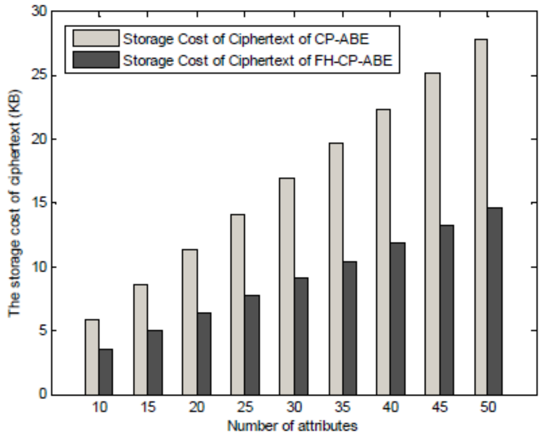

Fig: Storage cost comparison of two ciphertext files.

Conclusion:

The group action of access insurance policies and thus the help of coverage updates unit primary difficult issues within the information sharing systems. throughout this learn, we've got a bent to planned associate attribute-situated data sharing theme to implement a satisfactory-grained data access manage through exploiting the characteristic of the info sharing technique. The planned theme points a key offer mechanism that removes key agreement throughout the key iteration. The person secret keys unit generated through a snug two-celebration computation such any curious key new unleash middle or data storing core cannot derive the confidential keys in my opinion. As a result, the planned theme enhances data privacy and confidentiality inside the knowledge sharing procedure against any system manager’s just about nearly as good as adversarial outsiders whereas not corresponding (ample) credentials. The planned theme can do associate on the spot person revocation on each and every attribute set whereas taking full data of the scalable access manage stocked with through the ciphertext policy attribute placed committal to writing. As a consequence, the planned theme achieves extra comfortable and nice-grained data access management within the knowledge sharing methodology. We’ve got a bent to test that the planned theme is economical and scalable to firmly manipulate user data inside the knowledge sharing procedure.

References:

[1]. J. Anderson, “Computer Security Planning Study,” Technical report 73-51, Air Force Electronic System Division, 1972.

[2]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, “Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,” Proc. WISA 2009, LNCS 5932, pp. 309–323, 2009.

[3]. A. Sahai, B. Waters, “Fuzzy Identity-Based Encryption,” Proc.Eurocrypt 2005, pp. 457–473, 2005.

[4]. V. Goyal, O. Pandey, A. Sahai, B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,”Proc. ACM Conference on Computer and Communications Security 2006, pp. 89–98, 2006.

[5]. J. Bethencourt, A. Sahai, B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symposium on Security and Privacy 2007, pp. 321–334, 2007.

[6]. R. Ostrovsky, A. Sahai, B. Waters, “Attribute-Based Encryption with Non-Monotonic Access Structures,” Proc. ACM Conference on Computer and Communications Security 2007, pp. 195–203, 2007.

[7]. A. Lewko, A. Sahai, B. Waters, “Revocation Systems with VerySmall Private Keys,” Proc. IEEE Symposium on Security andPrivacy 2010, pp. 273–285, 2010.

[8]. A. Boldyreva, V. Goyal, V. Kumar, ”Identity-Based Encryptionwith Efficient Revocation,” Proc. ACM Conference on Computer and Communications Security 2008, pp. 417–426, 2008.

[9]. N. Attrapadung, H. Imai, “Conjunctive Broadcast and Attribute-Based Encryption,” Proc. Pairing 2009, LNCS 5671,pp. 248–265, 2009.

[10]. M. Pirretti, P. Traynor, P. McDaniel, B. Waters, “SecureAttribute-Based Systems,” Proc. ACM Conference on Computer and Communications Security 2006, 2006.

[11]. S. Rafaeli, D. Hutchison,”A Survey of Key Management for Secure Group Communications,” ACM Computing Surveys,vol. 35, no 3, pp. 309–329, 2003.

[12]. P. Golle, J. Staddon, M. Gagne, P. Rasmussen, "A Content-Driven Access Control System," Proc. Symposium on Identity and Trust on the Internet, pp. 26–35, 2008.

[13]. S. Yu, C. Wang, K. Ren, W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ASIACCS '10, 2010.

[14]. S. D. C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P.Samarati, "Over-encryption: Management of Access Control Evolution on Outsourced Data," Proc. VLDB'07, 2007.

[15]. D. Boneh, M. K. Franklin, "Identity-based Encryption from the Weil Pairing," Proc. CRYPTO 2001, LNCS vol. 2139, pp. 213–229, 2001.

[16]. A. Kate, G. Zaverucha, and I. Goldberg, "Pairing-based onion routing," Proc. Privacy Enhancing Technologies Symposium 2007, LNCS vol. 4776, pp. 95–112, 2007.

[17]. L. Cheung, C. Newport, "Provably Secure Ciphertext Policy ABE," ACM Conference on Computer and Communications Security, pp. 456–465, 2007.

[18]. V. Goyal, A. Jain, O. Pandey, A. Sahai, "Bounded Ciphertext Policy Attribute-Based Encryption," Proc. ICALP, pp. 579–591,2008.

[19]. X. Liang, Z. Cao, H. Lin, D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption,"Proc. ASIACCS, pp. 343–352, 2009.

Author Profile

M. Vijaya Durga Rasamayi is currently pursuing M.tech in the Department of computer science and Engineering from Chadalawada Ramanamma Engineering College, Tirupati. India.She has received her B.Tech degree in Computer Science and Engineering from Annamacharya Institute of Technology and sciences, Tirupati, India.

R. Suresh is currently working as an professor in Chadalawada Ramanamma Engineering College, Tirupati. India. Presently he is pursuing his Ph.D in the topic "Image processing-Medicial Imaging".He has published 2 International Papers , 2 conference papers and 2 Research papers.