Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SABE: EFFICIENT AND SCALABLE FILTERED ACCESS CONTROL IN DISTRIBUTED CLOUD DATA STORAGE

[1]NARESH VURUKONDA, [2]B.THIRUMALA RAO

[1]Research Scholar, Department of Computer Science Engineering, KLUniversity, A.P, India

[2]Professor, Department of Computer Science Engineering, KLUniversity, A.P.India

E-mail: [1]naresh.vurukonda@gmail.com, [2]drbtrao@kluniversity.in

ABSTRACT

Distributed cloud data storage is an advanced and empirical concept in present days for out sourcing of data in cloud. Distributed file storage requires users trustable on their required data to service provider of the cloud. Because of increasing security and protection concerns in out sourced data in clouds, traditionally several approaches like Attribute Based Encryption (ABE) have been proposed for gained access control in out sourced data in distributed cloud environment. This schema follows symmetric key approaches to provide security in cloud computing. Symmetric key approach is not suitable for support authorization effectively because, it uses single key for encryption and decryption. Presently authors focus on centralized approaches for proving security using single key distribution center, shares attributes to all the users. A new decentralized grained access control approach is required for privacy on data storage that supports anonymous authentication. In this paper we introduce to propose and develop an approach i.e. Scalable Attribute Based Encryption (SABE) to achieve grained with flexible and scalable access control in cloud computing for secure distributed cloud storage. Our proposed approach is not only perform scalable due to its pyramid structure, it also share effective and flexible access control in supporting on ABE, it also assigns for user expiration time and revocation efficient than existing schemas. Our experimental results show effective data share in distributed environment with feasible data retrieval with access control for outsourced data in cloud computing with reliable experimental evaluation.

Keywords: *Cloud Computing, Attribute Based Encryption Flexible, Access Control, and Pyramid Structure.*

1. INTRODUCTION

Cloud computing is a casual keyword for the delivery of hosted services over web service which includes computer resources. Different companies enable cloud computing to compute resources as utility to maintaining cloud infrastructures with relevant network services in network. Cloud computing promises attractive benefits for business and end users, main benefits of cloud computing are 1. Individual Data Outsourcing 2. Elasticity with Flexibility 3. User Services by Pay Money. These 3 services can be public, private and hybrid. Private services are outcome from business with maintain data centers to applications used users in data storage. Private cloud services achieve connivance, preserving management control and security. In public cloud model, middle service provider achieves and outcome cloud service over web service provider. These services are sold on demand and usage on cloud computing, customers pay for CPU operations, storage and bandwidth of clients consuming. Cloud service providers like Amazon Web Service, Microsoft and Google Search engine. Hybrid cloud is combination of both public cloud services and on premises private cloud services with normal cloud assessment with feasible operations.

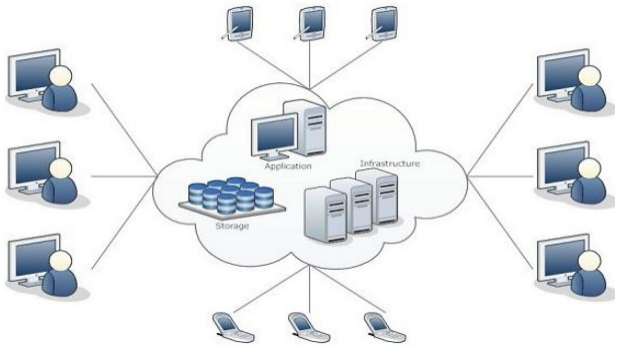

Figure 1: Distributed Cloud Infrastructure Framework.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

As shown in figure 1, distributed cloud computing refers to configure, manipulate applications on web with application processes. If offers online data storage, infrastructure and application outsourcing in cloud. It offers development and service models for manipulate applications in distributed storage system [2][3]. Recently cloud file storage is an emerging concept in implementation of distributed cloud computing, users concerns about privacy of data storage that impacts cloud computing from different operations. These concerns are complicated from sensible data in public cloud; it is maintained by unfavorable CSP. Attribute Based Encryption follows primitive security from untrusted users while data sharing in cloud. Still now there are two kinds of ABE approaches were proposed to provide security in cloud: Key Policy based ABE (KP-ABE) and Cipher text Policy ABE (CP-ABE). In KP-ABE, access control policy is assigned in secure format in terms of private key with sequential storage of cloud data, where as CP-ABE follows security as private key in terms of cipher text [5]. By preferring these conditions ABE gives privacy & way for data user to distribute out sourced data to un trusted data storage service provider instead of described and feasible server with specified large amount of users in cloud computing[24][25].

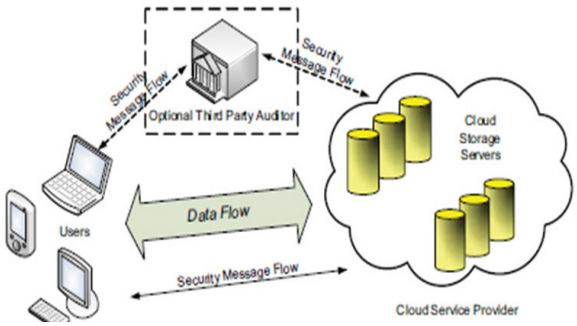

Figure 2: Ensuring data storage security in distributed cloud computing.

Consider the effective disadvantage of ABE is communication with computational cost while decoding with decryption phase in data sharing. Procedure of ensuring secure file storage environment as shown in figure 2. ABE needs to increase efficiency, introduce outsourced anonymity ABE which provides outsourcing intensive computed task during decryption phase to CSP without producing data or primitive keys, was introduced in [6][7]. For example, in mobile cloud application development; data collecting nodes as mobile devices or sensors has limited computation ability to complete encryption and decryption stages with residual execution of data sharing to protect sensitive data in public cloud. Therefore computational storage intensive tasks performed by resource constrained user's data sharing cloud. Beyond that decryption is heavy complex task while more number private keys used in data sharing from group of users then it may overload while features authority in cloud data storage. So in this paper we propose to develop Scalable Attribute Based Encryption (SABE) for access control in cloud computing. SABE enhances the cipher text policy attribute based encryption for data prediction and secure storage with hierarchical or pyramidal structure of system users presentation to achieve scalable, flexible and fine grained access control procedure in real time distributed environment. Contributions of proposed work as follows:

1. We show how SABE coming from ABE with pyramid structure to improve scalability, flexibility while at the same time extends the properties of fine grained access control of attribute set based encryption (ASBE).

2. Demonstrate and implement full-fledged fine grained access control based on ABE, This schema supports for pyramid based structure with user grant and revoke, file creation, file forwarding, file deletion in distributed cloud data storage.

3. Formalize the security of our proposed approach based on CP-ABE schema and then analyze its performance in terms of computational time and overhead to perform above conditions.

4. Implement SABE and then conduct comprehensive experiments in terms of performance evaluation that demonstrate SABE gives satisfactory performance with reduced complexity.

Remaining sections of this paper organized as follows: Section 2 describes related work with literature review on security in cloud computing.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Section 3 describes attribute based encryption procedure for providing privacy to data sharing in cloud computing with architectural implementation. Section 4 formal to implement Scalable Attribute Based Encryption implementation with design. Section 5 discuss experimental evaluation with comparative results to decrease computational overhead to provide security in cloud computing. Section 6 concludes overall conclusion of providing security using SABE with decrease of computational overhead in cloud computing.

2. BACKGROUND RELATED WORK

In it, we review the process of feature centered protection and also provide brief summary of the feature set centered protection and also we analyze current accessibility management schemas depending on feature centered protection.

K, et al This document explains Information accessibility management is a highly efficient approach so that the details protection in the reasoning. Despite, because of details freelancing and untrusted reasoning web servers, the details accessibility management becomes a examining problem in allocated storage frameworks.

W.- G. Tzeng [5] et al This document shows recommend efficient and protected (string) unaware transfer (OT1n) programs for any n _ 2. We set up our OT1 n strategy from central cryptographic techniques straight. The receiver's decision is truly protected and the secret of the unclosed expert information relies upon on the solidity of the decisional Diffie-Hellman problem. S. Yu, C. Wang, K. Ren, and W. Lou[5] This document represents Personal Health Record (PHR) is a creating patient-driven model of wellness data trade, which is frequently contracted to be put away at an outsider, for example, reasoning providers [11]. However, there have been wide protection problems as individual wellness data could be provided to those outsider web servers and to unapproved events.

A. Shamir[1] et al This document current a novel kind of cryptographic strategy, which encourages any pair of customers to provide securely and to validate each other 's represents without trading personal or open important factors, without keeping key indices , and without using the companies of an outsider [12]. The program expect t h e existence of reliable key era concentrates, whose only objective is t o give every customer a personalized amazing card v when he first be a part of st he organize.

A. Sahai et al This document current another sort of Identity-Based Encryption (IBE) strategy that we contact Unclear Identity-Based Encryption. In Unclear IBE we see a way of life as set of informative features. A Unclear IBE strategy considers a personal key for a personality, ω, to decipher a cipher text scrambled with a personality, ω_ , if and just if the individualities ω and ω are near each different as calculated by the "set cover" separating measurement [13].

V. Goyal[3] et al This document shows As more sensitive details is shipped and put away by outsider places on the Internet, there will be a need to scribe details put away at these locations. One issue with development details is that it can be specifically allocated just at a coarse-grained level (i.e., giving another collecting your personal key). We build up another cryptosystem for fine-grained discussing of secured details that we contact Key-Policy-Attribute-Based Encryption (KPABE) [7].

By and by, the agreement utilized the cover up strategy and in this way leaded to spilling of personal details. Atallah and Li analyzed the problem of handling the modify separating between two successions and showed a highly efficient conference to securely delegate collection connection with two web servers. Moreover, Ben and Atallah maintained to the point of protected freelancing for generally appropriate direct statistical computations. In fact, the suggested conferences required the expensive functions of homomorphic protection. Atallah what's more, Frikken further focused on this problem and provided improved conferences considering the expected incapable secret covering doubt [8][9]. These days, Wang et al. provided efficient elements for protected freelancing of straight development computation. We take note of that however a few programs have been knowledgeable about securely delegate sorts of expensive computations, they are not appropriate for keeping in mind ABE computational expense of exponentiation at customer side. To achieve this purpose, the traditional technique is to use server-helped techniques. Be that as it may, past jobs are found to quickening the rate of exponentiation using untrusted web servers. Straightforwardly using these systems in ABE will not perform

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

efficiently. Another technique may be to guide delayed wide freelancing process or giving computation in light of completely homomorphic protection or user-friendly proof structure. In any case, Gentry has revealed that notwithstanding for incapable protection factors on ""bootstrapping"" function of the homomorphic protection, it would take no less than 30 a few moments on an top level machine [10]. In this way, regardless of the fact that the protection of the details and generate can be stored by using these general techniques, the computational expense is still tremendous and unfeasible.

3. SECURE CLOUD STORAGE WITH ABE

In this section, we discuss about outsourced ABE and its procedure implementation and design. Secure data outsourcing is an emerging concept in real time cloud data sharing. Conventionally propose ABE with Anony attribute control and Anony attribute control-F to allow cloud service providers to provide access privileges and control users based on their identity and knower information in out sourced cloud as shown in figure 3.

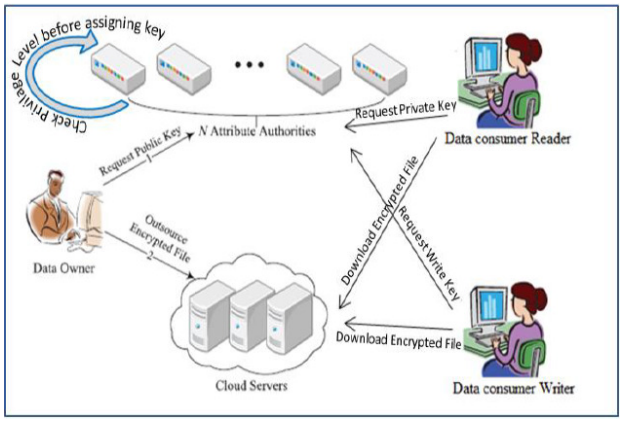

Figure 3: Anony and AnonyControl-F implementation procedure.

This schema is able to provide user's privacy against single user authority in possibility of individual founded information [1]. Partially data enclosed with Anony Attribute Control and no information in Anony Attribute Control-F then multi authority based encryption achieves AnonyControl sequences. Following steps are helpful for development of AnonyControl F-measure in outsourced data in cloud.

a) **Registration with Social Authentication:** Specifically more number of peoples were registered to contribute their working procedure in cloud data sharing and also add some more friends for uploading, downloading required files.

b) **Attribute Based Encryption:** Utilizing for every node encrypts information store. After encrypted information and again the re-encoded the same information is utilizing for fine-grain idea utilizing client information transferred. The quality in feature based protection has been proposed to secure the distributed storage with ABE [20][21][22]. In such encryption conspire, a character is seen as an arrangement of illustrative features, and decoding is conceivable if a decrypt or's personality has a few representations with the one indicated in the encrypted text.

c) **Multi Authority:** This group-authority collaborative system is displayed in which every user has its user id and they can cooperate with every key generator (authority) utilizing different code representations. We will probably accomplish a group-authority CP-ABE which accomplishes the privacy as characterized above; assurances the security of Data Consumers" personality data [7][8][14]; and endures dependent attacks on the authorities to process individual security concerns.

Anony Attribute Control-F directly measures privacy of Anony Attribute Control but extra computational communication overhead is incurred by oblivious transfer data in distributed cloud environment. Supporting user revocation is an emerging concept in real time cloud application development.

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

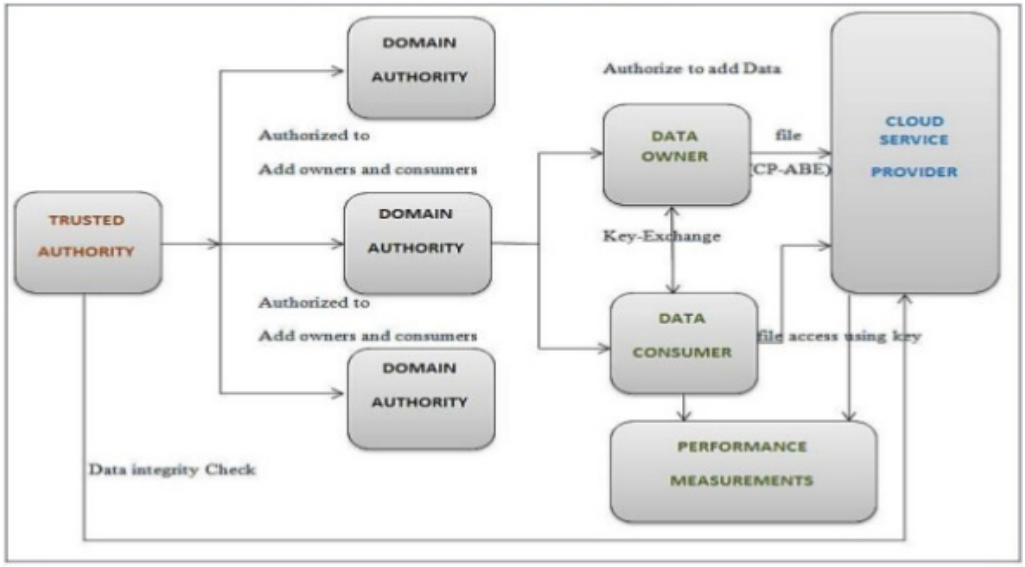

Figure 4: Proposed Approach Implementation Procedure.

4. SYSTEM DESIGN & IMPLEMENTATION

Procedures of cloud computing under consider five following steps: Cloud Service Provider, User's Data, Data Consumers based o their attributes, Domain Authorities with attributes and Trusted Authority for users.

a. **System Design:** As depicted in fig 4, CSP controls overall cloud to provide information with security and storage service. Data entrepreneurs secure their information in terms of data files and then store them into cloud for information discussing into other information customers. To access their data files information customers decrypt information submitted from information entrepreneurs. Each information owner or information consumer administrated by sector power, Domain power managed by reliable sector power provider [15][19].

b. SABE schema Implementation: The suggested SABE schema totally expands ABE to handle chart structure of the program customers shown in figure 5. Remember suggested approach program design comprises multiple sector regulators, reliable regulators with numerous customers corresponding to information consumers and information owners. Trusted regulators maintain, managing and spread program factors with master private important factors as well as approve parent sector regulators. So sector power is responsible for assigning secrets of subordinate regulators at each level of description with feasible reflection of information based on its sector.

Main operations of SABE are as follows: we are ready to develop following steps to implement scalable access control environment to share user's data into different domain authorities.
System Setup, Domain Authority, User Grant, File Creation, User Revocation, File Access and File Deletion. Procedure of developing these steps achieved as follows:
System Setup: Cloud distributed environment trusted authority achieves implementation procedure to create public key (PK) parameters and Victim Key (VK_0). PK will store data as public to visible data to all persons in same time VK_0 will be secret to data sharing. Setup d=2 → (PK, VK0), where d is depth measure of key structure store in procedure. Implementation procedure selects bilinear group B of unique

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

order p with generator g and then random exponents $\delta, \gamma_i \in Z_p, \forall_i \{1,2\}$. To support generated key design with proper structure of depth d and i is the range from 1 to d. The procedure for PK and VK_0 is as follows:

$$PK = (B, g, h_1 = g^{\gamma_1}, f_1 = g^{1/\gamma_1},$$
$$h_2 = g^{\gamma 2}, f_2 = g^{1/\gamma 2}, e(g,g)\delta)$$
$$VK_0 = (\gamma_1, \gamma_1, g^{\delta})$$

Main Level Domain permission Authority: Main attribute domain authority conceive with unique representation i.e. ID and recursive attribute set $\square = \{C_0, C_1, C_2, C_3, ...C_m\}$ where $C_i = \{c_0, c_1, c_2, ..., c_m\}$ with $a_{i,j,}$ it is being able to generate j^{th} attribute in C_i and n_i being presentation of all the attributes in C_i then create Domain Authority(DA) as follows:

$$VK_i = (\square, D = g^{\frac{(\delta + r^{\{\mu\}})}{\gamma_1}}, D_{i,j} = g^{r_i^{\{\mu\}}}.H(c_{i,j})^{r_{i,j}^{\{\mu\}}}$$
$$D'_{i,j} = g^{r_{i,j}^{\{\mu\}}} for \rightarrow (0 \le i \le m), (1 \le j \le n_i),$$
$$E_i = g^{\frac{(r^{\{\mu\}} + r_i^{\{\mu\}})}{\gamma_2}} for \rightarrow (1 \le i \le m))$$

In the above victim key reflection Ei is for interpretation from $r^{\{\mu\}}$ of Ci at the converting components Ei and Ei' can be used in decryption process.

User Grant: When customers signify as u and new subordinate sector power denoted as DA_{i+1} wants to be a part of in to system for giving authorization to other customer present immediately reasoning data discussing with possible connections created by managing the domain authority. Create User using victim key proceeding attribute set using create domain authority procedure with secret key as follows:

$$VK_{i+1} = (\tilde{\square}, \tilde{D} = D.f_1^{\tilde{r}^{\{\mu\}}}, \tilde{D}_{i,j} = D_{i,j}.g_1^{\tilde{r}^{\{\mu\}}}.H(c_{i,j})^{\tilde{r}_{i,j}^{\{\mu\}}},$$
$$\tilde{D}'_{i,j} = D'_{i,j}.g^{\tilde{r}_{i,j}^{\{\mu\}}} for \rightarrow c_{i,j} \in \tilde{\square},$$
$$\tilde{E}_i = E_i.f_2^{\tilde{r}^{\{\mu\}} + \tilde{r}_i^{\{\mu\}}} for \rightarrow C_i \in \tilde{\square})$$

The newly generated secret key VK_{i+1} for key structure $\tilde{\square}$, it is equivalent received key from trusted authority.

Data file Creation: To guard information saved on the reasoning, a information proprietor first encrypts information and then stores the secured information on the reasoning. Before posting file into reasoning prepared by information proprietor as follows: Pick file exclusive id, arbitrarily select symmetrical information security using Encryption and then decrypt with Decryption process, describes shrub accessibility framework [18][19].

User Revocation: Whenever there is a person to be suspended, the system must make sure the suspended customer cannot connect to the associated information any more. One way to resolve this problem is to re-encrypt all the associated information used to be utilized by the suspended customer, but we must also ensure that the other users who still can get rights to these information can accessibility them properly. SABE gets the advantage of ABE in efficient customer cancellation.

File Deletion: Encrypted information can be removed only at the demand of the information proprietor. To remove an secured computer file, the information proprietor delivers the file's exclusive ID and its trademark on this ID to the reasoning. Only upon successful confirmation of the information proprietor and the demand, the reasoning removes the information file.

5. EXPERIMENTAL SETUP

In this section, we analyze theoretical computation of complexity of proposed schema at each operation. Then we implement an SABE based on CP-ABE and also defines series of experiments to evaluate performance of our proposed schema with comparison of outsource Annoy ABE. Theoretical implementation already discussed in above section with feasible implementation.

Performance Evaluation: We have implemented multi level SABE based on CP-ABE which is pair based cryptography. Experimental setup conducted on laptop with I3 processor 4GB RAM running Windows Operating system successfully. It's implementation as follows:

SABE Setup: Generates a public key PK and Victim key operates VK_0.

SABE Key Gen: Generates key structure using PK and VK_0, usually supported depth of key structure maintain in between 1 and 2.

SABE-KeyDel: In Domain authority, some parts are private keys to new users in DA_{i+1} in its

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

domain presentation. Delegated key is equivalent to generated private keys by Root Authority in data access control.

SABE KeyUp: Firstly generate PK with attributes; while users decide to change PK in data sharing then usually generates updated PK with new attributes.

SABE Enc: Do encryption on files under an access tree policy specified in developed procedure.

SABE Dec: Using private keys and then decrypts a file.

Following figure 5 shows proposed system setup to maintain key structure using different parameters with respect to time. This figure achieves only performance of proposed approach only because of drawback in ABE as suitable maintenance of privates key with their depths. Performance w.r.t to Maintain Key Structure with different paradigms i.e., they are key generation time with number of attributes and second one is key generation time with subset of attributes.

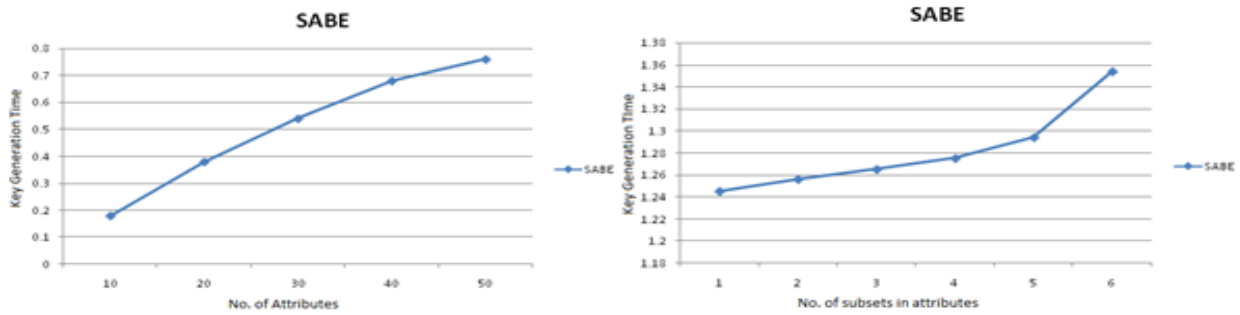

Figure 5: Tests on system setup and top-level sector power allow. (a) Top-level sector power allow (the variety of subsets in the key framework is 1); (a) top-level sector power allow (the count of features in the key framework is 50).

This procedure performed with command line SABE-KeyGen is determined by the variety of subsets and features in the key framework creation. This process is conducted only one sub set present in key framework, expenses previously improved based on variety of features improved. Practical implementation of key update, data encryption and decryption assigned based on attributes added to the domain authority.

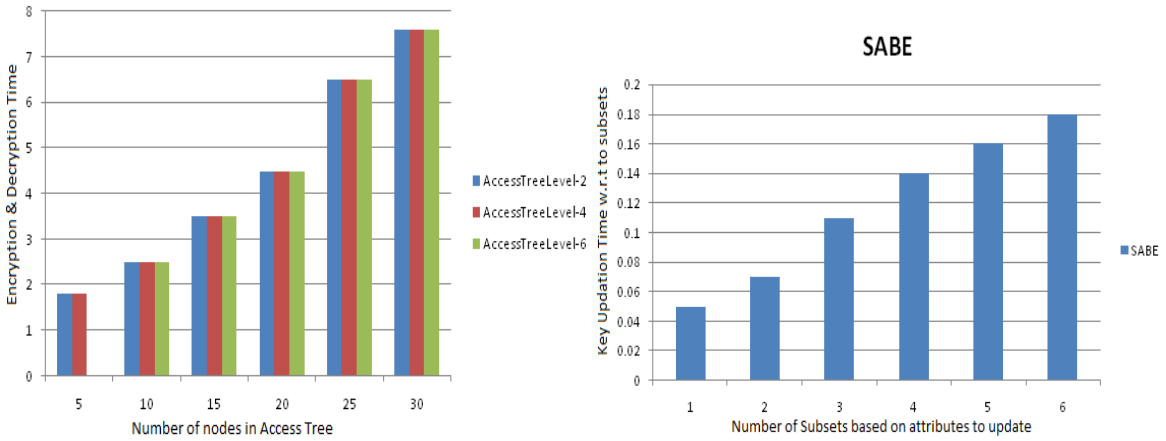

Figure 6: Experiments setup on file encryption & decryption, a) Encrypt/Decrypt file operations based on access tree based on attributes b) key update generation time with sub set attributes achieved in access tree operations.

User revocation basically consists two operations i.e. Key Update with new features (attributes) and Data Encryption/Decryption; Key update is generalized with Keyup command in SABE for operations effective utilization. Domain authority assigns new attributes to the user authority; O (1) is the average time complexity in new attributes added to subset of private keys analyzed with subsets. SABE-Rec is used to encrypt and decrypt file with different access tree levels in real time application development. Procedure for key update and file encryption and decryption shown in figure

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6 with subset attributes and newly added features by domain authority. We can see effective performance of proposed approach with representative attributes in real time cloud development.

6. CONCLUSION

In this document we introduce to implement SABE approach for analyze and flexible, realizing scalable and dependable attribute access control in distributed cloud environment with computational implementation. The SABE incorporates pyramid structure of systematic user's implementation by improving outcome delegation procedure to ABE. SABE not only supports relevant attributes (features) due to flexibility attribute set combinations with data user removable revocation because of multiple analyzed attributes with newly added attributes to upload file. Finally our proposed schema conducted theoretical and practical experimental setup and evaluation, it shows efficiency in user revocation and computational over a head with existing schemas.

REFERENCES

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

[2] 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. 13thCCS*, 2006, pp. 89–98.

[4] 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.

[5] 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.

[6] 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.

[7] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen,"Securely Outsourcing Attribute-Based Encryption with Check ability", proceedings in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 8, AUGUST 2014.

[8] Zhiguo Wan, Jun'e Liu, and Robert H. Deng," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[9] B. Barbara, "Salesforce.com: Raising the level of networking," *Inf. Today*, vol. 27, pp. 45–45, 2010.

[10] J. Bell, Hosting EnterpriseData in the Cloud—Part 9: InvestmentValue Zetta, Tech. Rep., 2010.

[11] A. Ross, "Technical perspective: A chilly sense of security," *Commun. ACM*, vol. 52, pp. 90–90, 2009.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 2010*, 2010, pp. 534–542.

[13] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc. ESORICS*, Saint Malo, France, 2009.

[14] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Acvances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457–473.

[15] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.

[16] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Comput. Syst.*, vol. 25, pp. 599–616, 2009.

[17] M.J. Atallah and K.B. Frikken, ''Securely Outsourcing Linear Algebra Computations,'' in Proc. 5th ACM Symp. ASIACCS, 2010, pp. 48-59.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[18]C. Wang, K. Ren, and J. Wang, ‘‘Secure and Practical Outsourcing of Linear Programming in Cloud Computing,’’ in Proc. IEEE INFOCOM, 2011, pp. 820-828.

[19]K.-M. Chung, Y.Kalai, F.-H. Liu, and R. Raz, ‘‘MemoryDelegation,’’ in Proc. Adv. Cryptol.-CRYPTO, LNCS 6841, P. Rogaway, Ed., Berlin, 2011, pp. 151-168, Springer-Verlag.

[20]J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, ‘‘Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption,’’ in Proc. 18th ESORICS, 2013, pp. 592-609.

[21]J. Lai, R. Deng, C. Guan, and J. Weng, ‘‘Attribute-based Encryption with Verifiable Outsourced Decryption,’’ IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.

[22]R. Canetti, B. Riva, and G. Rothblum, ‘‘Two Protocols for Delegation of Computation,’’ in Proc. Inf. Theor. Security, LNCS 7412, A. Smith, Ed., Berlin, Germany, 2012, pp. 37-61, Springer-Verlag.

[23]X. Chen, J. Li, J.Ma, Q. Tang, andW. Lou, ‘‘NewAlgorithms for Secure Outsourcing of Modular Exponentiations,’’ in Proc. ESORICS, LNCS 7459, S. Foresti, M. Yung, and F. Martinelli, Eds., Berlin, Germany, 2012, pp. 541-556, Springer-Verlag.

[24]Rao, B. Thirumala. "A Study on Data Storage Security Issues in Cloud Computing." *Procedia Computer Science* 92 (2016): 128-135.

[25]Vurukonda, Naresh, B. Thirumala Rao, and B. Tirapathi Reddy. "A Secured Cloud Data Storage with Access Privileges." *International Journal of Electrical and Computer Engineering (IJECE)* 6.5 (2016).