Journal of Theoretical and Applied Information Technology
31st July 2017. Vol.95. No 14

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

FINE GRAINED MULTI ACCESS CONTROL VIA GROUP SHARING IN DISTRIBUTED CLOUD DATA

RANJEETH KUMAR M[1], N.SRINIVASU[2], LOKANATHA C. REDDY[3]
[1] Research Scholar, Dept. of CSE, KL University, Guntur, A.P., India
[2] Professor, Dept. of CSE, KL University, Guntur, A.P., India
[3] Professor, Dept. of CS, School of Science & Technology, Dravidian University, Kuppam, A.P., India

E-mail: [1]maduri.ranjith@gmail.com, [2]srinivasu28@kluniversity.in, [3]lokanathar@yahoo.com

ABSTRACT

Distributed cloud data storage is an advanced and empirical concept in present days for out sourcing of data in cloud. 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. SABE 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. Protected data transmission among users should be effective in as well as flexible in order to support access control policy models with secure team communication, selective and hierarchal data transfer control in sharing. So in this paper we propose and develop Transmitted Team Key Management (TTKM), where each client (user) in group shares a secret trust key owner with subsequent rekeying for data sharing join or departure of users requires only broadcast message between data sharing in cloud. We analyze the privacy of proposed TTKM schema and compare with existing SABE security schema's in distributed data sharing. We also provide real time secure cloud setup with suitable server configurations based on service domain IP-address and service domain. Our experimental results show effective data access control with authorized security considerations.

Keywords: *Access Control, Pyramid Structure, Distributed Cloud Storage, Transmitted Team Key Management, Privacy Model.*

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. 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].

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

Figure 1: Distributed Cloud Infrastructure Framework.

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 untrusted data storage service provider instead of described and feasible server with specified large amount of users in cloud computing.

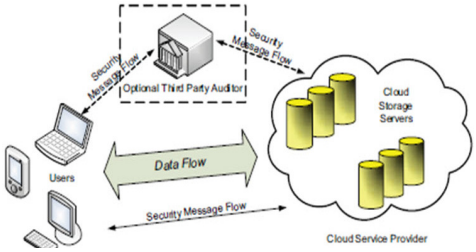

Figure 2: Ensuring data storage security in distributed cloud computing.

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]. Conventionally, Scalable Attribute Based Encryption for access control in cloud computing used for cipher text-policy attribute based encryption with hierarchal structure of system users and to achieve scalable flexible and fine grained access control policy. This schema provides full support for hierarchal user grant, file creation and user revocation in cloud computing. It is has hierarchal structure to improve scalable and flexible fine grained access control of hierarchal attribute based encryption. SABE is single key sharing process between different user's data sharing. SBAE is not accessible for Group Key Management to support security between different users in cloud data sharing. There are more number of approaches proposes for group key management, those centralized approaches use single key trust key to update and distribute share group keys in cloud data sharing. A Transmitted Team Key Management (TTKM) address above problems in group data sharing. In this schema each user in team shares a secret server based trusted key with subsequent rekeying to communicate or relieve of different users require only one broadcast message and also no change to secret key shares with existing users. This schema is flexible, efficient and privacy in cloud data sharing. This approach maintain use of secure private communication when rekeying takes a place either among different users between server and persisting group user. Following are contributions are our proposed approach:

1. Introduce TTKM using formalization methodology.
2. Analysis of TTKM
3. Comparison of Security and Complexity of our proposed approach with existing schemas.
4. Empirical performance of our proposed approach with SABE.

By using real time server setup environment, we need to deploy security considerations to stored data in distributed environment. By using private domain service maintenance for cloud storage and usage of services, we can built our own cloud with individual IP address and domain registration and also provide private security to each individual client present in cloud data sharing. Remaining sections of this paper organized as follows: Section 2 describes related work with literature review on security in cloud computing.. Section 3 formal to

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

implement Scalable Attribute Based Encryption implementation with design. Section 4 formalizes TTKM implementation and design procedure. 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 TTKM 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. , X. Jia, K. Ren, and B. Zhang [4] 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], 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] 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 and B. Rich waters,[2] 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, O. Pandey, A. Sahai, and B. Rich waters,[3] 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 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

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

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. SABE SECURE 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.

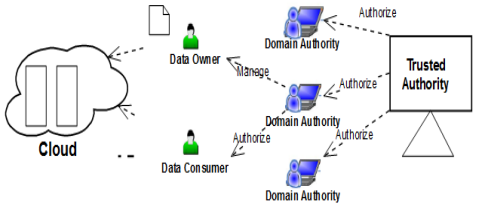

Figure 3: Proposed approach implementation procedure.

a. System Design: As depicted in fig 3, 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 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:

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

$$VK_0 = (\gamma_1, \gamma_1, g^{\delta}) \quad (2)$$

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:

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

$$VK_i = (\square, D = g^{\frac{(\delta + r^{\{\mu\}})}{\gamma_1}}, D_{i,j} = g^{r_i^{\{\mu\}}}.H(c_{i,j})^{r_{i,j}^{\{\mu\}}},$$
$$D'_{i,j} = g^{r_{i,j}^{\{\mu\}}} for \rightarrow (0 \le i \le m), (1 \le j \le n_i),$$
$$E_i = g^{\frac{(r^{\{\mu\}} + r_i^{\{\mu\}})}{\gamma_2}} for \rightarrow (1 \le i \le m)) \quad (3)$$

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:

$$VK_{i+1} = (\tilde{\square}, \tilde{D} = D_i f_1^{\tilde{r}^{\{\mu\}}}, \tilde{D}_{i,j} = D_{i,j} g_1^{\tilde{r}^{\{\mu\}}}.H(c_{i,j})^{\tilde{r}_{i,j}^{\{\mu\}}},$$
$$\tilde{D}'_{i,j} = D'_{i,j} g^{\tilde{r}_{i,j}^{\{\mu\}}} for \rightarrow c_{i,j} \in \tilde{\square},$$
$$\tilde{E}_i = E_i f_2^{\tilde{r}^{\{\mu\}} + \tilde{r}_i^{\{\mu\}}} for \rightarrow C_i \in \tilde{\square}) \quad (4)$$

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.

4. SYSTEM DESIGN & IMPLEMENTATION

In this section, we formally express TTKM and its implementation procedure and key management schema with defined users in group which has hold Individual Subscription Token (ISP) with common group key. TTKM definition as follows:

Transmitted Team Key Management (TTKM) Exposed with two leafs like 1. A key Server (Svr) and 2. Group Members (Usrs), a convenient broadcast from single server (Svr) to all the Usrs. Procedure of TTKM achieves as follows:

ParamGen Svr takes as input a warranty parameter k and outputs a fit of nation parameters

Param, which includes the dwelling KS of vacant time signature values.

TkDeliv Svr sends each Usr an deserted subscription least possible (IST) on a secluded channel.

KeyGen Svr chooses a shared accumulation key K $ KS. Based on the ISTs of Usrs, Svr computes a reside of values PubInfo. Svr keeps K confidential, and broadcasts at the hand of the word channel

PubInfo to generally tell lock stock and barrel members Usr.

KeyDer Usr uses its IST and PubInfo to count one by one the shared lock stock and barrel key K.

Update When the shared everyone K cut back no longer be secondhand (e.g., when there is a culmination of group dynamics one as unite and ceasing to exist of lock stock and barrel users), Svr generates polished group key K" and PubInfo", earlier broadcasts the dressed to the teeth PubInfo to the group. Each Usr uses its IST and the new PubInfo" to count one by one the dressy shared group key K". We re-gather the system after-words the Update phase a dressy "session". The Update phase is furthermore called a rekeying phase.

Svr picks randomly generated key $K \in KS$ as the shared team key, then svr chooses N random strings $a_1, a_2, ..., a_N \in \{0,1\}$. Svr creates an $n \times (N+1)$F -matrix.

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

$$Z = \begin{pmatrix} 1 & z_{1,1} & z_{1,2} & z_{1,N} \\ 1 & z_{2,1} & z_{2,2} & z_{2,N} \\ & & & \\ 1 & z_{n,1} & z_{n,2} & z_{n,N} \end{pmatrix} \quad (5)$$

In the above equation $a_{i,j} = H(ist_i \,||\, a_j), 1 \le i \le n, 1 \le j \le N$.

By using non-zero evaluation with solution of matrix nontrivial by construction of uniformly generated random keys by Svr for clause access control vector generation.

Based on individual subscription token Svr constructs (N+1) dimensional with vector representation. Based on above operations like KeyGen, PubInfo KeyDer update all the KeyGen then Svr runs all the phases with respect to current group users, creates new group and broadcast all the keys based on PubInfo of multiple users as shown in below figure.

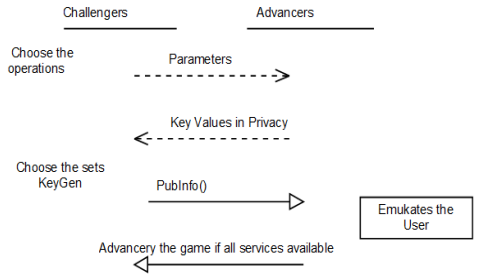

Figure 4: TTKM procedure with group sharing in cloud.

Suppose Svr runs an Update past to serve Param for another diffuse gathering time signature K", and a yesteryear kind of thing Usr is no in a superior way a gathering part at the heels of the Update stage. Let K be a horse and buggy day shared gathering key which can be left to the imagination by Usr mutually token IST. A TTKM is ahead key securing if a foe mutually learning of IST, K, and the beautiful PubInfo can't get the dressed to the teeth key K" from an unreasonable esteem in the key-space KS by all of non-negligible happening [6][7]. Essentially, a TTKM schedule is in dance to a different tune key securing if another bunch part Usr at the heels of the Update stage can't recall anything roughly the yesterday gathering keys. Consider the entanglement in multi key disclosure sharing mid multi users in unsound sourced front page new TTKM was not support travail flexibility in key sharing to multi users

5. REAL TIME PRIVACY FOR CLOUD STORAGE

In this section we discuss about real time cloud set environment with real time security in data storage and sharing between different clients. In real time cloud setup environment, we need to maintain privacy for registered users using basic private setting whenever user enters into registered cloud setup environment. Excluding this, we also maintain application privacy for storage data based on user access control as public and private scenarios. For efficient data storage sharing between different users in cloud, we implement SHA (Secure Hash Algorithm) to provide security to data and share encrypted data to all the available users present in real time environment. Sample real time cloud set up environment as shown in figure 5.

Figure 5: Own cloud registration with server.

We register with some basic details to our developed own cloud, then our cloud store our details in the form of .hc format for security to data and share those files securely to other users present in cloud storage environment. In this way, we need to maintain secure formations in cloud environment.

6. EXPERIMENTAL SETUP

In this section, we construct our own developed cloud set up using JDK and NETBEANS latest version and then deploy into some domain registered formations. We also maintain individual security to all the users present in cloud with suitable data sharing. 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 Anony ABE. Theoretical implementation already discussed in above section with feasible implementation.

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

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:

Comparison w.r.t to Existing Schemas: In this section we present to compare TTKM with SABE theoretically because of lack summaries in group data sharing in real time cloud data sharing. SABE only performs single key distribution for uploaded files in cloud. So TTKM performs effective efficiency in generation of multiple keys with representation of multi user data sharing.

Implementation of TTKM with respect to Usrs:

In this area we analyze the computational performance of TTKM. We imitate the KeyGen stage at Svr and the KeyDer stage at Usrs. In the research, we vary both the dimensions of the actual primary field Fq and the dimensions of the group of Usrs, and measure the Svr-side and Usr-side calculations time. To stress on the mathematics functions, we do not depend the here we are at hashing functions in the research. As shown in figure 5, the common calculation time improves normally as the dimension of the best area improves. The actual operating time relies upon on the best area that is selected and the way area mathematics.

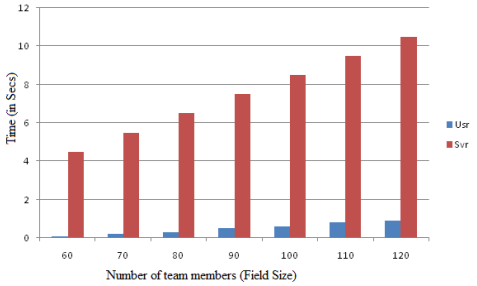

Figure 6: Dimensionality based data sharing in cloud with field size with group members.

Fig. 6 reviews the TTKM operating time at Svr and Usr for set area measures (in bits) 64, 80, 96 and 112, with the dimensions of the team varying from 10 to 200 members. The important time is averaged over 20 versions. It demonstrates the TTKM rekeying process operates fast on Svr when there are thousands of Usrs in the team. It takes less than two minutes for Svr to produce new PubInfo when there are up to 200 Usrs and when the best area is large enough.

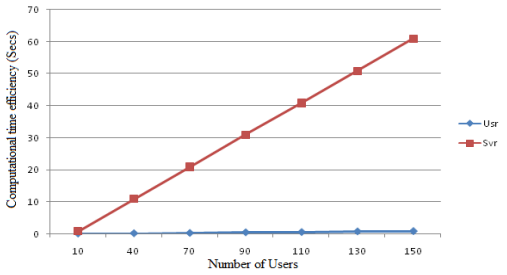

Figure 7: Computational time at Usr and Svr with group users in file computation.

Both figures show that it takes very little here we are at a Usr to obtain the distributed team key, and a practically short time frame for the Svr to generate the key and the transmitted rekeying information, when the actual limited field and the team size are both considerably large.

7. CONCLUSION

In this document, we have suggested a new TTKM schema, which is managed by a trusted key server, and allows any legitimate customer in the team to get you a distributed team key on its own from transmitted public details. The plan reduces the utilization of private peer-to-peer communication programs, and only uses a transmitted route to provide new rekeying messages when the team key needs to be modified. The interaction expense is straight line with the number of customers in the team. The plan uses only effective hash functions and straight line geometry over finite areas in calculations, and does not require any security plan. It is protected in that even a computationally unbounded attacker cannot get the distributed team key without a valid symbol from the key server. The key derivation is effective for any team participant. We also implement own cloud set up with security using open source software and hardware's in distributed data storage. The experimental results show that the creation of the rekeying details takes a short time period on a laptop or computer for a team of countless numbers of associates. If we are increase users in local host based service in data sharing then storage is takes high for both data sharing and security maintained. So our own setup maintain server for storage and security maintenance in real time data sharing with individual privacy in data sharing. 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. As further improvement of proposed approach into

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

key-aggregated cryptographic in multi data sharing in cloud.

REFRENCES:

[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.

[6] 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.

[7] 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.

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

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

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

[11] 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.

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

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

[14] 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.

[15] 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.

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

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

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

[22] 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.

[23] Ning Shang #, Mohamed Nabeel #, Elisa Bertino #, Xukai Zou, “Broadcast Group Key Management with Access Control Vectors”, IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16–30, 2000.