A LIGHT WEIGHT INFORMATION SHARING SYSTEM FOR VERSATILE CLOUD ENVIRONMENT

Mr. JALLIPALLI VENKATA BRAHMAIAH

Master of Computer Applications, Qis College of Engineering and Technology, Ongole

Abstract: Cloud computing emerges as latest technology in the real world applications and with this reputation of Cloud computing, PDAs can store/recuperate singular data from wherever at whatever point. In this manner, the data security issue in adaptable cloud ends up being progressively genuine and balances further headway of versatile cloud. There are huge examinations that have been directed to improve the cloud security. Regardless, a vast segment of them are not relevant for adaptable cloud since mobile phones simply have limited enrolling resources and power. Courses of action with low computational overhead are in unimaginable necessity for adaptable cloud applications. In this paper, we propose a lightweight data sharing system (LDSS) for versatile Cloud computing. It gets CP-ABE, a passageway control advancement used in regular cloud condition, anyway changes the structure of access control tree to make it sensible for adaptable cloud circumstances. LDSS moves a sweeping portion of the computational genuine access control tree change in CP-ABE from PDAs to outside go-between servers. Furthermore, to diminish the customer disavowal cost, it familiarizes property portrayal fields with realize lazy renouncement, which is a thorny issue in program based CP-ABE structures. The exploratory results show that LDSS can effectively diminish the overhead on the PDA side when customers are sharing data in flexible cloud conditions.

Keywords: *Cloud Computing, Information Security, Light weight data sharing plan.*

I. INTRODUCTION

Cloud computing has various security models to prevent data loss with unauthorized bodies. People are a little bit at a time getting acquainted with another time of data sharing model in which the data is secured on the cloud and the PDAs are used to store/recuperate the data from the cloud. Consistently, mobile phones simply have limited storage space and figuring power. In fact, the cloud has giant proportion of advantages. In such a circumstance, to achieve the classy execution, it is major to use the benefits given by the cloud authority center (CSP) to store and share the data.

Nowadays, unique cloud adaptable applications have been commonly used. In these applications, people (data owners) can exchange their photos, chronicles, reports and diverse records to the cloud and offer these data with different people (data customers) they like to share. CSPs in like manner give data the administrators' convenience to data owners. Since individual data reports are tricky, data owners are allowed to pick whether to make their data records open or should be bestowed to unequivocal data customers. Evidently, data security of the individual fragile data is a noteworthy stress for some data owners. The front line advantage the administrators/get the opportunity to control instruments given by the CSP are either not necessities of data owners. In any case, when people exchange their data archives onto the cloud, they are leaving the data in a spot where is out of their control, and the CSP may watch out for customer data for its business favorable circumstances and moreover extraordinary reasons. Second, people need to send mystery key to each datum customer if they simply need to confer the mixed data to explicit customers, which is ambling. To improve the advantage the board, the data owner can disconnect data customers into different social occasions and send mystery expression to the get-togethers which they have to share the data. In any case, this approach requires fine-grained get the opportunity to control. In the two cases, mystery states the officials is a noteworthy issue.

Plainly, to deal with the above issues, individual unstable data should be mixed before exchanged onto the cloud with the objective that the data is secure against the CSP. Regardless, the data encryption brings new issues. The best technique to give capable access control instrument on ciphertext disentangling with the objective that simply the endorsed customers can get to the plaintext data is trying. Moreover, structure must offer data owners convincing customer advantage the board limit, so they can permit/deny data get to benefits successfully on the data customers. There have been significant examines on the issue of data get the opportunity to order over ciphertext. In these analyzes, they

have the going with customary suppositions. In the first place, the CSP is seen as reasonable and curious. Second, all the unstable data are encoded before exchanged to the Cloud. Third, customer endorsement on explicit data is practiced through encryption/unscrambling key dispersal. Generally speaking, we can parcel these systems into four characterizations: essential ciphertext get the opportunity to control, dynamic access control, get the chance to control subject to totally homomorphic encryption [1][2] and get the opportunity to control reliant on quality based encryption (ABE). All of these proposals are planned for non-flexible cloud condition. They exhaust far reaching proportion of limit and count resources, which are not available for mobile phones. As demonstrated by the test results in [26], the major ABE assignments take any more drawn out time on mobile phones than PC or PCs. It is some place around different occasions longer to execute on a propelled cell phone than a (PC). This infers an encryption errand which takes one moment on a PC will take around thirty minutes to finish on a wireless. Additionally, current courses of action don't handle the customer advantage change issue incredible. Such an action could result in especially high repudiation cost. This isn't material for mobile phones too. Obviously, there is no real plan which can feasibly handle the ensured data sharing issue in adaptable cloud. As the flexible cloud ends up being progressively conspicuous, giving an successful secure data sharing instrument in versatile cloud is in desperate need.

To address this issue, in this paper, we propose a Lightweight Data Sharing Scheme (LDSS) for versatile distributed computing condition. The primary commitments of LDSS are as per the following:

(1) We plan a calculation called LDSS-CP-ABE dependent on Attribute-Based Encryption (ABE) technique to offer proficient access power over ciphertext.

(2) We use intermediary servers for encryption and unscrambling tasks. In our methodology, computational serious tasks in ABE are directed on intermediary servers, which significantly diminish the computational overhead on customer side cell phones. Then, in LDSS-CP-ABE, so as to keep up information security, an adaptation credit is additionally added to the entrance structure. The decoding key configuration is changed with the goal that it tends to be sent to the intermediary servers secury.

(3) We present languid re-encryption and depiction field of ascribes to decrease the renouncement overhead when managing the client disavowal issue.

(4) Finally, we execute information sharing model system dependent on LDSS. The tests demonstrate that LDSS can extraordinarily decrease the overhead on the customer side, which just presents a negligible extra expense on the server side. Such a methodology is valuable to actualize reasonable information sharing security plot on cell phones. The outcomes likewise demonstrate that LDSS has better execution contrasted with the current ABE based access control conspires over ciphertext.

II RELATED WORK

a). Attribute-based fine-grained access control with efficient revocation in cloud storage systems

A cloud storage service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. To address this challenge, traditional methods usually require the data owner to encrypt the data and deliver decryption keys to authorized users. These methods, however, normally involve complicated key management and high overhead on data owner. In this paper, we design an access control framework for cloud storage systems that achieves fine-grained access control based on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach. In the proposed scheme, an efficient attribute revocation method is proposed to cope with the dynamic changes of users' access privileges in large-scale systems. The analysis shows that the proposed access control scheme is provably secure in the random oracle model and efficient to be applied into practice.

b). Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data

As the data produced by individuals and enterprises that need to be stored and utilized are rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. However, as sensitive cloud data may have to be encrypted before outsourcing, which obsoletes the traditional data utilization service based on plaintext keyword search, how to enable privacy-assured utilization mechanisms for outsourced cloud data is thus of paramount importance. Considering the large number of on-demand data users and huge amount of outsourced data files in cloud, the problem is particularly challenging, as it is extremely difficult to meet also the practical requirements of performance, system usability, and high-level user searching experiences. In this paper, we investigate the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. Our mechanism design first exploits a suppressing technique to build storage-efficient similarity keyword set from a given document collection, with edit distance as the similarity metric. Based on that, we then build a private trie-traverse searching index, and show it correctly achieves the defined similarity search functionality with constant search time complexity. We formally prove the privacy-preserving guarantee of the proposed mechanism

under rigorous security treatment. To demonstrate the generality of our mechanism and further enrich the application spectrum, we also show our new construction naturally supports fuzzy search, a previously studied notion aiming only to tolerate typos and representation inconsistencies in the user searching input. The extensive experiments on Amazon cloud platform with real data set further demonstrate the validity and practicality of the proposed mechanism.

c). DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems

Data access control is an effective way to ensure data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising technique for access control of encrypted data. However, due to the inefficiency of decryption and revocation, existing CP-ABE schemes cannot be directly applied to construct a data access control scheme for multiauthority cloud storage systems, where users may hold attributes from multiple authorities. In this paper, we propose data access control for multiauthority cloud storage (DAC-MACS), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multiauthority CP-ABE scheme with efficient decryption, and also design an efficient attribute revocation method that can achieve both forward security and backward security. We further propose an extensive data access control scheme (EDAC-MACS), which is secure under weaker security assumptions.

III PROPOSED SYSTEM

We propose LDSS, a framework of lightweight data-sharing scheme in mobile cloud (see Fig. 1). It has the following six components.

(1) Data Owner (DO): DO upload data to the mobile cloud and share it with friends. DO determine the access control policies.

(2) Data User (DU): DU retrieves data from the mobile cloud.

(3) Trust Authority (TA): TA is responsible for generating and distributing attribute keys.

(4) Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

(5) Decryption Service Provider (DSP): DSP provides data decryption operations for DU.

(6) Cloud Service Provider (CSP): CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO have stored in the cloud.

IV. PRELIMINARIES AND ASSUMPTIONS

In this section, we tend to 1st in brief gift the technique preliminaries closely associated with LDSS, then gift the system model and a few security assumptions in

$$k = h(0) = \sum_{s=1} y_{i_s} \prod_{\substack{j=1 \\ j \neq s}} \frac{\square x_i}{x_{i_s} - x_{ij}}$$

Since $x1$, $x2$,...,xn is public, we can get Lagrange Coefficients in advance:

$$\lambda_s = \prod_{\substack{j=1 \\ j \neq s}}^{t} \frac{-x_{i_j}}{x_{i_s} - x_{i_j}}$$

Thus, the formula to recover the secret k can be put in a simpler way:

$$k = \sum_{s=1}^{t} \lambda_s y_{i_s}$$

V. ALGORITHEM

To better illustrate LDSS-CP-ABE rule, we first define the subsequent terms.

Definition 1: Attribute An attribute defines the access privilege for a particular data file. Attributes are assigned to knowledge users by knowledge owners. a knowledge user will have multiple attributes corresponding to multiple knowledge files. A knowledge owner will define a collection of attributes for its knowledge files. The data accesses ar managed by access management policy nominative by knowledge house owners.

Function 1: Setup()

INPUT: The attribute set A , the version attribute V.
OUTPUT: The master key MK, the public key PK.

1. Construct a p-order bilinear group G_0 of generator g and a bilinear mapping $e : G_0 * G_0 = G_1$.
2. Randomly choose $a,b \in Z_p$ and calculate g^b , $e(g, g)^a$.
3. For each attribute a_i in A, randomly choose $t_i \in Z_p$, and calculate $X_i = g^{t_i}$.
4. For V, randomly choose $t_v \in Z_p$, and calculate $X_v = g^{t_v}$.
5. Return the master key MK and the public key PK, Wherein $MK=\{a,b\}$, $PK=\{ G_0, g , g^b, e(g,g)^a, \{X_i\}^k_{1,i=} X_v\}$.

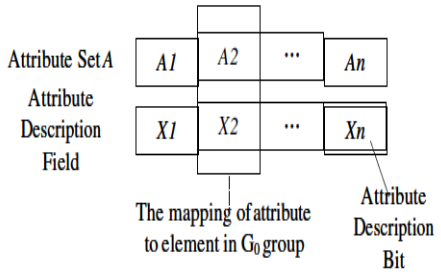
Definition 2: Access management Tree Access management tree is that the specific expression of access control policies, during which the leaf nodes ar attributes, and non-leaf nodes ar relative operators like and, or, n of m threshold. every node in associate access management tree represents a secret, and therefore the secret of a high node are often split into multiple secrets by secret sharing theme and distribute to lower level nodes. Correspondingly, if we know the secrets of leaf nodes, we will deduce the key of non-leaf nodes by calculative recursively from bottom to top.

Function 2: KeyGen()

INPUT: The attribute set A_u, the master key $MK=\{a,b\}$.
OUTPUT: Attribute keys associated with A_u.

1. Randomly choose a parameter $r \in Z_p$, and calculate $SK_r = g^{(a+r)/b}$.
2. For each attribute a_i in A_u, randomly choose $r_i \in Z_p$, and calculate $SK_a = \{g^{r_i}, g^r \cdot X_i^{r_i}\}_{i=1}^{j}$.
3. For V, randomly choose $r_v \in Z_p$, and calculate $SK_v = \{g^{r_v}, g^r \cdot X_v^{r_v}\}$.
4. Return $SK_u = \{SK_r, SK_a, SK_v\}$.

The attribute description field of DO is generated by the TA. Once a knowledge owner registered with tantalum, it sends its own attribute set to tantalum. Tantalum then generates attribute description field, during which every attribute bit represents a value in G0. Tantalum keeps the attribute description field within the DO-PK/MK-information. The attribute description field of DO is shown in sharing scheme we can get:



$$Fx = \prod_{z \in Sx} Fz^{\Delta_{i,S'x}(0)}$$

$$= \prod_{z \in Sx} (e(g,g)^{r \cdot q_z(0)})^{\Delta_{i,S'x}(0)}$$

$$= \prod_{z \in Sx} (e(g,g)^{r \cdot q_{parent(z)}(index(z))})^{\Delta_{i,S'x}(0)}$$

$$= \prod_{z \in Sx} (e(g,g)^{r \cdot q_x(i)})^{\Delta_{i,S'x}(0)}$$

$$= e(g,g)^{r \cdot q_x(0)}$$

$$= e(g,g)^{rs}.$$

PERFORMANCE ANALYSIS

In this section, we tend to appraise the performance of LDSS in terms of process and storage overheads, respectively. Experimental Settings to evaluate the potency of the projected resolution, we conduct many experiments. The take a look at of LDSS is finished on a Core a pair of pair machine, that has a pair of.0GHz central processor with the Linux package (Ubuntu twelve.10) put in. The core formula of LDSS takes advantage of the CPABE tools developed by Bettencourt et al [15]. It's based on 160-bit elliptic curve cluster, CP-ABE tools have 3 basic operations, namely exponentiation and pairing on G0 and mathematical operation on G1. These 3 operations take four.99ms, 4.98ms and 0.58ms severally in our experimental setting.

TABLE 1
COMPUTATIONAL OVERHEAD OF BASIC OPERATIONS OF ABE SCHEMES

Types of Devices	Pairing	Exponentiation	Multiplication
PC	20 ms	5 ms	0.7 ms
Mobile	550 ms	177 ms	26 ms

TABLE 2
COMPUTATIONAL OVERHEAD OF DATA SHARING

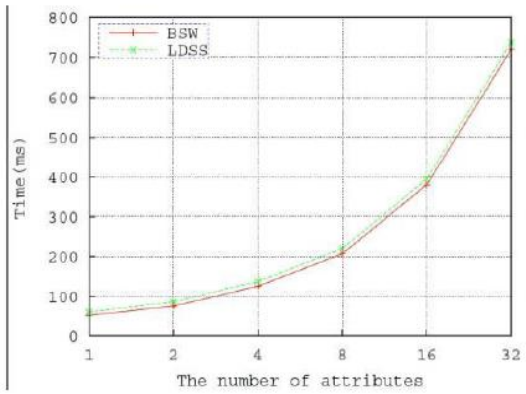
	Exponentiation on G_0	Exponentiation on G_1	Paring on G_0
ESP	$2\|T_a\|$	0	0
DO	3	1	0

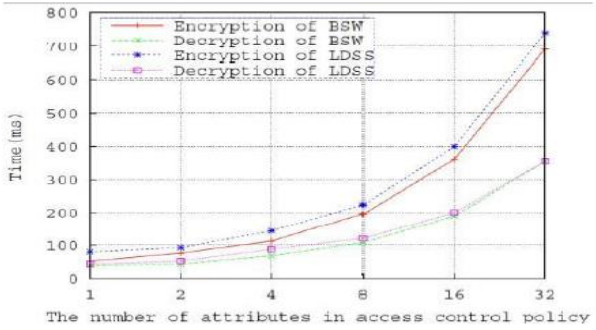
TABLE 3
COMPUTATIONAL OVERHEAD OF DATA ACCESS

	Exponentiation on G_0	Exponentiation on G_1	Paring on G_0
DSP	0	$\|T_a\|$	$2\|T_a\|+1$
DO	0	1	0

Accessing knowledge files

The cost of accessing knowledge files comes from operate Decryption (), that is dead whenever a file is accessed. This operate includes pairing operations on G0, multiplication operations on G0 and operation on G1. the quantity of those 3 forms of operations is all proportional to the quantity of attributes included within the access strategy. The value of accessing knowledge files depends on that one will the secret writing operation. Before introducing DSP, the overhead is on DU. After the introduction of DSP, the value on DU is reduced to a constant worth. The overhead of secret writing is expounded to the number of attributes concerned within the record and the way these attributes square measure combined. Within the worst case, all the attributes keys associated with the access management strategy square measure needed for secret writing. During this case, the overhead of psychic phenomenon and DO is shown bellow.





VI. METHODOLOGY

System Framework:

The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. In these applications, people (data owners) can upload their documents andother files to the cloud and share these data with other people (data users) they like to share. CSPs also provide data management functionality for data owners.

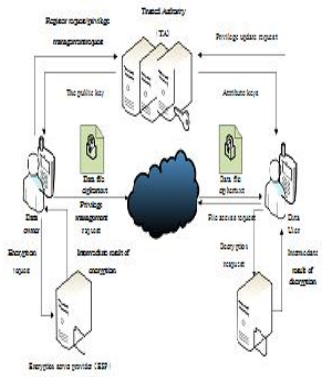


Fig: A lightweight data-sharing scheme (LDSS) framework.

Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners. We propose LDSS, a framework of lightweight data sharing scheme in mobile cloud. It has the following six components. (1)Data Owner (DO) (2) Data User (DU) (3) Trust Authority (TA) (4) Encryption Service Provider (ESP) (5) Decryption Service Provider (DSP) (6) Cloud Service Provider (CSP).

Data Owner (DO):

When the data owner (DO) registers on TA, TA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. DO defines its own attribute set and assigns attributes to its contacts. All these information will be sent to TA and the cloud. TA and the cloud receive the information and store it. DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies. DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file.

Data User (DU):

DU logins onto the system and sends, an authorization request to TA. The authorization request includes attribute keys (SK) which DU already has. TA accepts the authorization request and checks the request and a generate attribute keys (SK)for DU.DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. DU receives the ciphertext, which include ciphertext of data files and ciphertext of the symmetric key. DU decrypt the ciphertext of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the ciphertext of data files.

Trusted Authority:

To make LDSS feasible in practice, a trusted authority (TA) is introduced. It is responsible of generating public and private keys, and distributing attribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TA is entirely credible, and a trusted channel exists between the TA and every user. The fact that a trusted channel exists doesn't mean that the data can be shared through the trusted channel, for the data can be in a large amount. TA is only used to transfer keys (in a small amount) securely between users. In addition, it's requested that TA is online all the time because data users may access data at any time and need TA to update attribute keys.

Cloud Service Provider:

CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that

DO has stored in the cloud.DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses therequest; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.

VII. RESULT

In recent years, several studies on access management in cloud are supported attribute-based secret writing algorithmic rule (ABE). However, ancient ABE isn't appropriate for mobile cloud because it's computationally intensive and mobile devices solely have restricted resources. During this paper, we propose LDSS to handle this issue. It introduces a unique LDSS-CP-ABE algorithmic rule to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure information sharing downside in mobile cloud. The experimental results show that LDSS will guarantee information privacy in mobile cloud and cut back the overhead on users' facet in mobile cloud. Within the future work, we will design new approaches to confirm information integrity. To further faucet the potential of mobile cloud, we'll conjointly study a way to do ciphertext retrieval over existing information sharing schemes.

VIII. CONCLUSION

As of late, numerous investigations on access control in cloud depend on attribute based encryption calculation (ABE). Notwithstanding, customary ABE isn't reasonable for versatile cloud since it is computationally concentrated and cell phones just have restricted assets. In this paper, we propose LDSS to address this issue. It presents a novel LDSS-CP-ABE calculation to move significant calculation overhead from cell phones onto intermediary servers, in this way it can take care of the protected information sharing issue in portable cloud. The test results demonstrate that LDSS can guarantee information security in portable cloud and diminish the overhead on clients' side in versatile cloud. Later on work, we will plan new ways to deal with guarantee information honesty. To additionally tap the capability of portable cloud, we will likewise ponder how to do ciphertext recovery over existing information sharing plans.

IX REFERENCES

[1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Cloud System Security Symposium (NDSS), Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000.

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[9] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[12] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with

constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. NewYork, NY, USA: ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secure atrribute-based systems. in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM press, pp. 99-112, 2006.

[18] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270, 2010.

[19] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 29(2): 38-47, 1996.

[20] Tian X X, Wang X L, Zhou A Y. DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS. in: Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32, 2009

[21] Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data. in: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134, 2007.

[22] Kan Yang, Xiaohua Jia, Kui Ren, Ruitao Xie, Liusheng Huang: Enabling efficient access control with dynamic policy updating for big data in the cloud. INFOCOM 2014, pp.2013-2021, 2014.

[23] Jia W, Zhu H, Cao Z, et al. SDSM: a secure data service mechanism in mobile cloud computing. in: Proceedings of 30th IEEE International Conference on Computer Communications. Shanghai, China: IEEE, pp. 1060-1065, 2011.

[24] D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010.

[25] Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.

[26] Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. in: Proceedings of 8th International Conference on Network and Service Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.

[27] P. K. Tysowski and M. A.Hasan. Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds. IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, Nov. 2013.

[28] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. in: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, pp. 213−229, 2001.

[29] Sahai A, Waters B. Fuzzy identity based encryption. in: Proceedings of the Advances in Cryptology. Aarhus, Denmark: Springer-Verlag, pp.457-473, 2005.

[30] Shamir A. How to share a secret. Communications of the ACM,1979, 22 (11): 612-613.

Authors Profile

Mr. **JALLIPALLI VENKATA BRAHMAIAH** pursuing MCA 3rd year in Qis College and Engineering and Technology in Department of Master of Computer Applications, Ongole.