IJSEAT International Journal of Science Engineering and Advance Technology

A LDSS-CP-ABE Algorithm to Migrate Major Computation Overhead from Mobile Devices on to Proxy Server

[1]G. Satya Teja, [2]D. Shravani

[1]PG scholar, Dept of CSE, KIET College, East Godavari (District), Andhra Pradesh-533461, INDIA

[2]Asst Professor, Dept of CSE, KIET College, East Godavari (District), Andhra Pradesh-533461

ABSTRACT:

Cloud has hugequantity of resources. In such a situation, to attain the acceptable presentation, it is indispensable to usage the possessionsdelivered by the cloud service provider (CSP) to stock and segment the data. At the moment, many cloud mobile claims have been extensivelycastoff. In these claims, data owners can upload their photos, videos, documents and other files to the cloud and segment these data with other data users they like to stake. Explanations with stumpy computational overhead are in prodigious need for mobile cloud applications. In this paper, we recommend a lightweight data sharing scheme (LDSS) for mobile cloud computing. The investigational results show that LDSS can confirm data concealment in mobile cloud and decrease the overhead on users' side in mobile cloud.

KEYWORDS: cloud, encryption, privacy.

INTRODUCTION:

We recommend a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment. We proposal an algorithm called LDSS-CP-ABE created on Attribute-Based Encryption (ABE) system to suggestion competent access control over cipher text. We practice substitution servers for encryption and decryption processes. Computational concentrated processes in ABE are showed on proxy servers, which importantly decrease the computational slide on client side mobile devices[1,2,3]. Temporarily, in LDSS-CP-ABE, in instruction to up hold data confidentiality, a form quality is also additional to the admission construction. The decryption key arrangement is adapted so that it can be sent to the substitution servers in a safe way. We present indolent re-encryption and account arena of qualities to shrink the cancelation overhead when commerce with the user cancelation problematic[4,5,6]. Lastly, we contrivance a data sharing example outline based on LDSS. The experimentations show that LDSS can importantly condense the overhead on the client side, which only presents a negligible extra cost on the server side. Such amethod is helpful to tool a truthful data distribution safety scheme on mobile devices. The consequences also demonstration that LDSS has healthier presentation likened to the current ABE based admission control arrangements over cipher text.

LITERATURE SURVEY:

2.1] Kan Yang, XiaohuaJia, Kui Ren, Bo Zhang, RuitaoXie [7] Ciphertext-policy attribute-based encryption (CP-ABE) is a capable method for access control of scrambled data. Though, due to the inadequacy of decryption and cancelation, prevailing CP-ABE structures cannot be straightfunctional to hypothesis a data access controller structure for multi expert cloud storage systems, anywhere operators may clutch attributes from many authorities. In this paper, we proposition data entrée mechanism for multiauthority cloud storage (DAC-MACS), an operative and secure data access control arrangement with well-organized decryption and with drawal[8.9].

2.2] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje [10] Users, recognized by attributes, mighteasilyelect a substitution who can re-encrypt a cipher text connected with a convinced access strategy to additional one with a dissimilar access strategy. The planned arrangement is showed choosy construction preferred plaintext protected and master key secure deprived of chance prophecies. Also, we mature additional kind of key giving competence in our scheme and also deliberate some connected issues counting a sturdier safety model and requests[11,12].

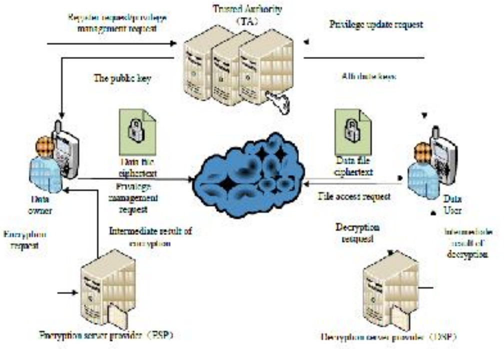
PROBLEM DEFINITION:

When people upload their data files on the cloud, they are departure the data in a place where is out of their mechanism, and the CSP may emissary on user data for its marketable safeties and/or other reasons. Public have to send watch word to each data user if they only want to stake the encoded data with convinced users, which is very unwieldy. To abridge the honor organization, the data owner can split data users into dissimilar collections and direct password to the groups which they want to segment the data. Though, this method necessitates fine-grained access control. In all the cases, password management is a giantconcern.

PROPOSED APPROACH:

Individual subtle data should be encodedearlier uploaded onto the cloud so that the data is protected in contradiction of the CSP. Though, the data encryption transports new-fangled difficulties. How to deliver effective access control appliance on cipher text decryption so that only the sanctioned users can entrance the plaintext data is inspiring. In count, system necessity proposition data owners active user pleasure organization competence, so they can allowance/withdraw data access rights simply on the data users. There have been considerable investigates on the subject of data access control over cipher text.

SYSTEM ARCHITECTURE:


Trusted Authority (TA)
Register request/privilege management request
Privilege update request
The public key
Attribute keys
Data file ciphertext
Privilege management request
Data owner
Data file ciphertext
File access request
Data User
Encryption request
Intermediate result of encryption
Decryption request
Intermediate result of decryption
Encryption server provider (ESP)
Decryption server provider (DSP)

PROPOSED METHODOLOGY:

ATTRIBUTE:

An attribute expresses the access pleasure for a confident data file. Attributes are dispensed to data users by data owners. A data user can have several attributes conforming to numerous data files. A data owner can describe a set of attributes for its data files. The data admissions are achieved by access control policy stated by data owners[13].

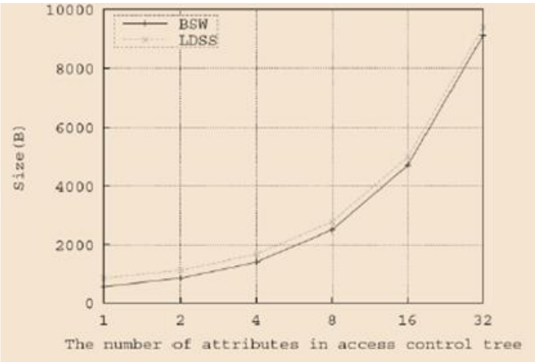
ACCESS CONTROL TREE:

Access control tree is the precise appearance of access control strategies, in which the leaf nodes are qualities, and non-leaf nodes are inter personal operators such as and, or, n of m threshold. Each node in an access control tree signifies a secret, and the secret of a top node can be riven into manifold secrets by secret sharing scheme and allocate to lower level nodes. Congruently, if we distinguish the secrets of leaf nodes, we can infer the secret of non-leaf nodes by scheming recursively from bottom to top[14].

VERSION ATTRIBUTE:

Version attribute is presented in LDSS-CP-ABE algorithm to confirm security. It is an accumulation to the inventive access control tree, establishing a new root node [15].

RESULTS:



The relationship between symmetric key ciphertext and access control policy

EXTENSION WORK:

We include efficient resource consumption auditing with less overhead that should be practical and economically applicable in the semi-trusted cloud environment.

CONCLUSION:

An access control expertise used in usual cloud environment, but variations the structure of access regulator tree to make it appropriate for mobile cloud environments. LDSS transfers a large share of the computational concentrated access control tree transformation in CP-ABE from mobile devices to exterior proxy servers. Additionally, to decrease the user withdrawal cost, it presents attribute description fields to device lazy-revocation, which is a prickly issue in database based CP-ABE systems. The tentative results show that LDSS can efficiently decrease the above on the mobile device side when users are distribution data in mobile cloud surroundings.

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 Distributed 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

Mr. G. Satya Teja is a student of Kakinada Institute of Engineering & Technology, Kakinada. Presently he is pursuing his M.Tech [Software Engineering] from this college and he received his B.Tech from KIET, affiliated to JNT University, Kakinada in the year 2017.

Ms. D. Shravani, well known Author and Excellent Teacher Received M.Tech (CSE) from JNTUK University. She is working as Assistant Professor in Department of Computer Science and Engineering at Kakinada Institute of Engineering and Technology. She has 1 year of teaching experience in Kakinada Institute of Engineering and Technology. Her area of Interest includes Data Warehouse and Data Mining, Internet Of Things and other advances in Computer Applications.