ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

An Approach for Secure Information Sharing Scheme in Mobile Cloud Computing

Prashanth S[1], Bharath M[2], Harshitha Gowda C L[3], Akshatha S R[4].

Department of ISE, SJB Institute of Technology, Bengaluru, India.

ABSTRACT: With the advent of distributed computing, cell phones can store/recover individual data from anyplace whenever. Subsequently, the data security issue in portable cloud turns out to be so much extreme that it keeps us from advance versatile cloud improvement. There are critical investigations that have been done to build the cloud security. Nonetheless, because of constrained registering the greater part of them are not pertinent for versatile cloud. Arrangements with low computational overhead are in extraordinary requirement for portable cloud applications. In this paper, we propose a lightweight data sharing plan (LDSS) for portable distributed computing. It receives CP-ABE, in typical cloud condition, however changes the structure of access control tree to make it appropriate for portable cloud situations. LDSS utilizes outer servers to perform superior figuring for getting to control tree change in CP-ABE from cell phones. The trial comes about demonstrate that time taken for encryption of record concerning number of traits differs relying upon the quantity of characteristics.

KEYWORDS: Mobile Cloud Computing, Data Encryption, Access Control, User Revocation.

I. INTRODUCTION

Mobile Cloud Computing (MCC) is the mix of appropriated figuring, flexible preparing and remote frameworks to pass on rich computational resources for convenient customers, compose heads, and furthermore circulated registering providers. An authoritative goal of MCC is to engage execution of rich adaptable applications on a lot of mobile phones, with a rich customer experience. MCC gives business opportunities to versatile framework executives and also cloud providers. More comprehensively, MCC can be portrayed as "a rich adaptable figuring development that utilization bound together adaptable resources of varied fogs and framework propels toward unhindered helpfulness, storing, and transportability to serve an extensive number of mobile phones wherever, at whatever point through the channel of Ethernet or Internet paying little regard to heterogeneous conditions and stages in light of the remuneration as-you-use run the show.

Nowadays, unique cloud convenient applications have been extensively used. In these applications, people (data proprietors) can exchange their photos, accounts, chronicles and distinctive archives to the cloud and offer these data with different people (data customers) they get a kick out of the opportunity to share. CSPs in like manner give data organization helpfulness to data proprietors. Since singular data reports are sensitive, data proprietors are allowed to pick whether to make their data records open or should be granted to specific data customers. Doubtlessly, data security of the individual delicate data is a noteworthy stress for some data proprietors.

The best in class advantage organization/get the chance to control frameworks gave by the CSP are either not sufficient or not particularly accommodating. They can't meet each one of the requirements of data proprietors. At first, when people exchange their data archives onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may watch out for customer data for its business focal points or possibly extraordinary reasons. Second, people need to send mystery word to each datum customer if they simply need to impart the mixed data to particular customers, which is to a great degree awkward. To revise the advantage organization, the data proprietor can segment data customers into different social events and send mystery key to the get-togethers which they have to share the data. In any case, this approach requires fine-grained get the chance to control. In the two cases, mystery key organization is a noteworthy issue.

The following areas portray about the related work, proposed technique, results and exchange and conclusion.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

II. RELATED WORK

In this area, we center around crafted by ciphertext get to control plans which are firmly identified with our exploration.

Access control is an essential instrument of information security insurance to guarantee that information must be gained by real clients. There has been considerable research on the issues of information get to control in the cloud, generally concentrating on get to control over ciphertext. Regularly, the cloud is viewed as legitimate and inquisitive. Delicate information must be encoded before sending to the cloud.

Client approval is accomplished through key conveyance. The exploration can be by and large isolated into four zones: basic ciphertext get to control, various leveled get to control, get to control in view of completely homomorphic encryption [1][2] and get to control in light of quality based encryption (ABE).

Straight forward ciphertext get to control alludes to that after information record encryption, the encryption keys are disseminated secury to accomplish approval for trusted clients [3]. To decrease the overhead of enormous client key dissemination, Skillen and Mannan [4] composed a framework called Mobiflage that empowers PDE (conceivably deniable encryption) on cell phones by covering up scrambled volumes by means of irregular information on a gadget's outer stockpiling. Nonetheless, the framework needs to acquire substantial measure of data of keys. [5] obtains the entrance control technique utilized as a part of ordinary circulated stockpiling [4][6][12][14], isolating clients into various gatherings as indicated by get to rights and dole out various keys to gatherings. This diminishes the overhead of key administration, however it can't fulfill the interest for fine-grained get to control.

Various leveled get to control has great execution in lessening the overhead of key appropriation in ciphertextaccess control [7]. Subsequently, there are considerable research on ciphertext get to control [8][9][10][11] in light of various leveled get to control technique. In progressive access control technique, keys can be gotten from private keys and an open token table. Notwithstanding, the task on token table is confounded and produces high cost. Additionally, the token table is put away in the cloud. Its protection and security can't be ensured [12].

Full homomorphic encryption calculation can work specifically on the ciphertext. Its working outcomes are the same with working on plaintext and afterward encoding the information. [13] utilizes full homomorphic encryption calculation to do tasks, for example, recovery and count specifically on ciphertext. It can tackle the issue that the cloud is dishonest essentially in light of the fact that all information refresh activities and client benefit change tasks should be possible straightforwardly on ciphertext. In any case, this encryption plot is excessively perplexing, making it impossible to execute in commonsense applications.

Quality based encryption calculation is gotten from character based encryption. It inserts decoding rules in the encryption calculation, which keeps away from visit key circulation. Lai et al [14] and Bethencourt et al [15] proposed key-strategy quality based encryption (KP-ABE) and ciphertext-approach trait based encryption (CP-ABE). In down to earth applications, CP-ABE has been widely examined [16][17][18] since it is like part based access control (RBAC) conspire [19]. In CP-ABE, the ownership of one quality key implies that the key proprietor possesses relating characteristic, and trait keys can't be recovered once they are disseminated. Thus, when an information client's trait is renounced, how to guarantee information security turns into a troublesome issue [14]. Characteristic based intermediary re-encryption (ABPRE) was proposed by Liang et al [16] to take care of this issue. In any case, in their answer, when a client's trait is disavowed, every other client who claim this quality will lose this property in the meantime, which can't fulfill fine-grained get to control needs. Tian et al [20] join CP-ABE and open key cryptography to accomplish ciphertext get to control. Notwithstanding, it conveys high cost to information proprietors. Di Vimercati et al [21] add a period stamp to credits to constrain the utilization of ascribe keys to manage quality disavowal issue. In any case, in this situation, information clients need to intermittently apply for trait keys and the clients' characteristic can't be disavowed before the time stamp terminates. Yu et al [19] propose some work of repudiation can be outsourced to CSP, though CSP ought to have a specific believability, and access control approach that contains "or" relationship or "limit" relationship isn't upheld. Yu et al [21] additionally proposed a plan to address the distributed computing testing that keep delicate client information private against untrusted servers by misusing and remarkably consolidating methods of quality based encryption (ABE), intermediary re-encryption, and lethargic re-encryption. Yang et al. [22] proposed a novel plan that empowering proficient access control with dynamic approach refreshing for enormous information in the cloud that concentrating on building up an outsourced strategy refreshing technique for ABE frameworks. It likewise composed arrangement refreshing calculations for various sorts of access strategies.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

III. PROPOSED WORK

We propose LDSS, a structure of lightweight information sharing plan in portable cloud (see Fig. 1). It has the accompanying six parts.

1. Data Owner (DO): DO transfers information to the versatile cloud and offer it with companions. DO decide the entrance control strategies.
2. Data User (DU): DU recovers information from the versatile cloud.
3. Trust Authority (TA): TA is in charge of creating and appropriating quality keys.
4. Encryption Service Provider (ESP): ESP gives information encryption activities to DO.
5. Decryption Service Provider (DSP): DSP gives information unscrambling tasks to DU.

Cloud Service Provider (CSP): CSP stores the information for DO. It steadfastly executes the tasks asked for by DO, while it might look over information that DO have put away in the cloud.

As appeared in Fig. 1, a DO sends information to the cloud. Since the cloud isn't solid, information must be scrambled before it is transferred. The DO characterizes get to control arrangement as access control tree (allude to Definition 2 in Section 3.2) on information documents to dole out which properties a DU ought to acquire on the off chance that he needs to get to a specific information record. In LDSS, information documents are altogether scrambled with the symmetric encryption instrument, and the symmetric key for information encryption is likewise encoded utilizing characteristic based encryption (ABE).

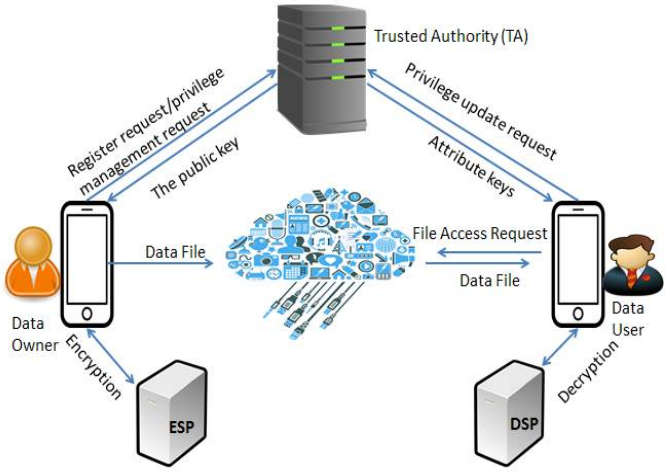


Figure 1: System Architecture

The entrance control strategy is installed in the ciphertext of the symmetric key. Just a DU who gets property keys that fulfill the entrance control approach can unscramble the ciphertext and recover the symmetric key. As the encryption and unscrambling are both computationally escalated, they present overwhelming weight for versatile clients. To calm the overhead on the customer side cell phones, encryption specialist co-op (ESP) and decoding specialist organization (DSP) are utilized. Both the encryption specialist co-op and the unscrambling specialist organization are additionally semi-trusted. We adjust the customary CP-ABE calculation and outline a LDSS-CP-ABE calculation to guarantee the information security while outsourcing computational assignments to ESP and DSP.

3.1. CP-ABE Algorithm

A ciphertext-arrangement quality based encryption conspires comprises of four calculations: Setup, Encrypt, KeyGen, and Decrypt.

1. Setup (λ, U).The setup calculation takes security parameter and trait universe depiction as info. It yields the general population parameters PK and an ace key MK.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

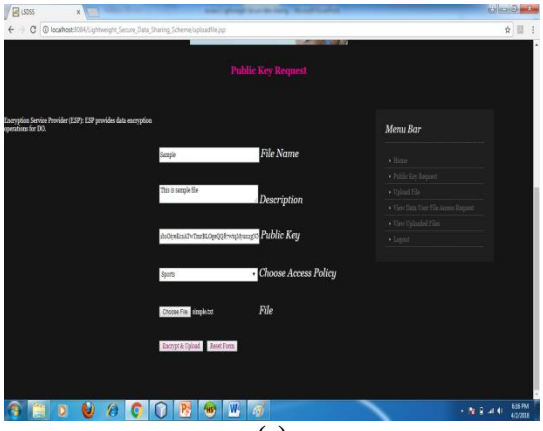
Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

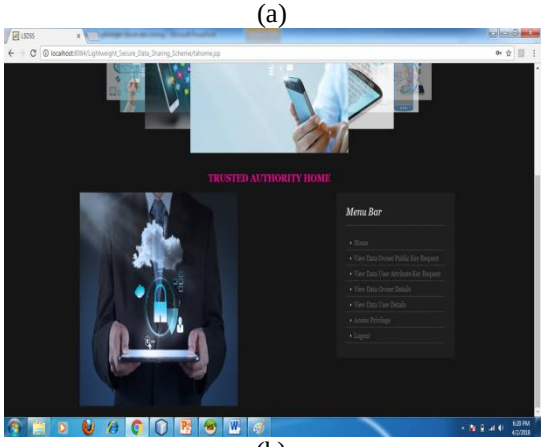
2. Encrypt (PK, M, A). Public parameter, a message M and entrance structure is taken as information for calculating. The calculation will scramble M and deliver a ciphertext CT to such an extent that lone a client that has an arrangement of qualities that fulfills the entrance structure will have the capacity to unscramble the message. We will accept that the ciphertext certainly contains A.
3. Key Generation (MK, S). The key age calculation takes as information the ace key MK and an arrangement of properties S that portray the key. It yields a private key SK.
4. Decrypt (PK, CT, SK). The unscrambling calculation takes as information people in general parameters PK, a ciphertext CT, which contains an entrance arrangement, an, and a private key SK, which is a private key for a set S of traits. In the event that the set S of characteristics fulfills the entrance structure A then the calculation will unscramble the ciphertext and restore a message M.

V. EXPERIMENTAL RESULTS

The intermediate output of the proposed model is shown in Figure below



(a)



(b)

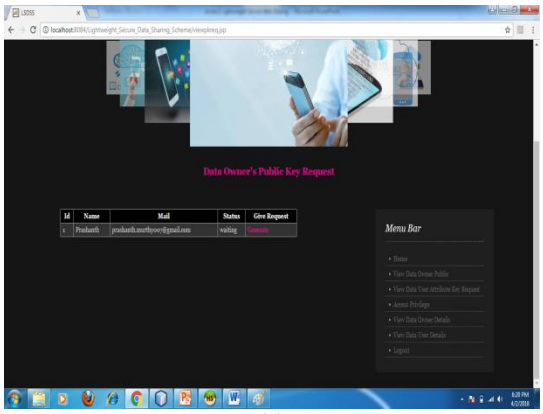
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018



(c)

Figure 2 : Proposed System Outputs

V. CONCLUSION AND FUTURE USE

Lately, numerous investigations on get to control in cloud depend on attribute based encryption calculation (ABE). In any case, customary ABE isn't appropriate for versatile cloud since it is computationally escalated and cell phones just have restricted assets. It presents a novel LDSS-CP-ABE calculation to move significant calculation overhead from cell phones onto intermediary servers, consequently it can take care of the protected information sharing issue in portable cloud. The trial comes about demonstrate that LDSS can guarantee information protection in versatile cloud and lessen the overhead on clients' side in portable cloud. Later on work, we will outline new ways to deal with guarantee information respectability. To additionally tap the capability of versatile cloud, we will likewise consider how to do ciphertext recovery over existing information sharing plans.

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, XiaohuaJia, KuiRen: 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

[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, KuiRen, Shucheng Yu, and KarthikMahendraRajeUrs.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, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: DAC-MACS: 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 key-policy 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. New York, 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, XiaohuaJia, KuiRen, RuitaoXie, Liusheng Huang: Enabling efficient access control with dynamic policy updating for big data in the cloud. INFOCOM 2014, pp.2013-2021, 2014.