© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Achieving an Effective Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

S R V Durga Bhavani[1], Dr. K V V S Narayana Murthy[2], Dr. D. Mohan Reddy[3]

[1]PG Scholar, Department of Computer Science and Engineering, Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram, East Godavari District, Andhra Pradesh, India
[2]Professor, Computer Science and Engineering, Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram, East Godavari District, Andhra Pradesh, India
[3]Professor & Principal, Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram, East Godavari District, Andhra Pradesh, India

ABSTRACT

Mobile device has restricted capacity and constrained computing resources so data can be put away on mobile cloud processing .Any client can transfer data on that cloud additionally anybody can get to that data, so there is security issue identified with that data in this way, we have to give security to that data to keep from unapproved client. Presently a day, the cloud computing turns out to be better known however the security isn't given in productive way. The issues identified with security is expands step by step. A few algorithms are intended to give security to cloud computing however those are not proficient for portable cloud computing so we outline LDSS-CP-ABE algorithm for give security to the mobile cloud computing. LDSS moves major computational overhead from portable customer side devices utilizing intermediary servers. Likewise we can utilize lethargic re-encryption technique which can lessen tedious process. Lightweight secure data sharing plan can decrease the computational overhead on the customer side mobile device when clients are sharing their data on portable cloud. Likewise we utilize the AES (Advance Standard Encryption) algorithm for data encryption and unscrambling reason.

Keywords : Mobile Cloud Computing, Data Encryption, Access control, User revocation.

I. INTRODUCTION

In cloud computing gigantic measure of data store on cloud by utilizing diverse brilliant devices or computer. Cloud computing implies, capacity of data and application on remote server and getting to them by means of web as opposed to sparing and introducing them on your own devices and PCs. As the mobile device has restricted storage room we utilize the mobile cloud computing for putting away data. Portable cloud computing are only mobile computing + cloud computing. Step by step fame and utilization of mobile devices are expanded quickly, so individuals can utilize new time to store data on cloud and store/recover that data by utilizing mobile devices. As the mobile device have restricted algorithm power and capacity the cloud contain colossal measure of assets so it is fundamental to utilize the cloud assets gave by cloud service provider(CSP) to store and offer data. Presently a day's numerous utilization of cloud portable has broadly utilized. Individuals (Data Owner) can share data. For instance: content, video, and sound on mobile cloud and individuals (Data User) who need to data can recover it. As data owner chose the data which shared is open or private. Plainly for data owner touchy data protection is real concern.

CSP (Cloud Service Provider) can't meet all prerequisite of data owner. To begin with when data owner needs to store data on cloud, data owner can isolate number of clients into gathering and offer the secret key to that gathering which is data owner needs to send however in this approach administration of watchword is huge issue. Distinctive algorithm are concocted or exhibit for giving security to cloud yet it isn't reasonable for mobile cloud computing, so utilize LDSS for giving security to data put away on portable cloud. The principle advantage of portable cloud computing and our proposed framework is to decreased computational overhead on customer side mobile device and give security to data on mobile cloud. Clearly, individual delicate data ought to be encoded before transferred onto the cloud with the goal that the data is secure against the Cloud Service Provider. The data encryption brings new issues. Instructions to give get to control component on figure content decryption with the goal that lone the approved clients can get to the plaintext data is testing. Likewise, framework offer data owner's viable client benefit administration ability, so they can allow data gets to benefits effortlessly on the data clients. In these explores, they have the accompanying normal presumptions. Initially, the CSP is viewed as genuine and inquisitive. Second, all the delicate data is encoded before transferred to the Cloud. Third, client approval on specific data is accomplished through encryption/ unscrambling key dissemination. As a rule, we can partition these methodologies into four classes: straightforward figure content access control, progressive access control, get to control in view of completely homomorphism encryption and access control in light of attribute based encryption (ABE). At long last, we actualize an data sharing model system in view of LDSS and furthermore utilized the AES(Advance Encryption Standard) algorithm for motivation behind encryption of data which are transferred on mobile cloud computing.

II. Literature Survey

1] A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing.

Authors: ChenglinShen, Heng He

Description: This paper describes that Mobile device has constrained capacity and restricted registering assets so data can be put away on mobile cloud computing .Any client can transfer data on that cloud likewise anybody can get to that data, so there is security issue identified with that data thus, it have to give security to that data to keep from unapproved client. In this paper, outline LDSS-CP-ABE algorithm for give security to the portable cloud computing.

2] How to fabricate a trusted database framework on untrusted capacity.

Authors: Maheshwari U, Vingralek R, Shapiro W.

Description: In this Paper, It can recognize the issue of guaranteeing dependability of data at an untrusted server within the sight of value-based updates that run specifically on the database, and build up the principal answers for this issue.

3] Achieving Usable and Privacy-guaranteed Similarity Search over Outsourced Cloud Data.

Authors: Cong Wang, KuiRen, Shucheng Yu

Description: In this paper, it examines the issue of secure and proficient comparability seeks over outsourced cloud data. In this any client can transfer data on cloud and furthermore accomplishes the usable and protection guaranteed similitude look over outsourced cloud data.

4] An adaptable component for get to control authorization administration in DaaS. In: Proceedings of IEEE International Conference on Cloud Computing.

Authors: Tian X, Wang X L, Zhou A Y.

Description: In this paper, First present a way to deal with executes the adaptable access control authorization administration by applying a DSP re-encryption instrument additionally this re-encryption component is utilized more than once.

5] Hybrid trait and re-encryption-based key administration for secure and mobile portable applications in mists.

Authors: P. K. Tysowski and M. A.Hasan

Description: Cloud-based data is progressively gotten to by asset compelled mobile devices for which the handling cost must be minimized. In this paper, re-encryption component is performed alternatively.

III. Methods and Techniques Used

1) LDSS (Lightweight secure data sharing scheme):

In Proposed System, we utilize LDSS-CP-ABE algorithm, this algorithm outlined utilizing following techniques.

i. Setup (A, V) - It produce the private master key and public key on set of properties An of the data owner and adaptation trait V.

ii. KeyGen (Au, MK) - It is utilized to produce property keys SK for data client in view of quality set An and master key MK.

iii. Encryption (K, PK,T)- Based on symmetric key K, Public key PK and Access Control tree T create figure content CT.

iv. Decryption (CT, T, SK) - Attribute Key SK and Access control tree. It unscrambles figure content CT.

LDSS is only the one sort of procedure which gives security to the lightweight data sharing plan on portable cloud. In LDSS it utilizes quality based encryption which has another two subparts that is:

• CP-ABE:-Cipher text policy Attribute based Encryption.

• KP-ABE:-Key Policy Attribute based Encryption.

In our System, We utilize the CP-ABE (Cipher Policy – Attribute based Encryption). CP-ABE gives the encryption of data system.

2) AES (Advanced Encryption Standard):

i. To survey the general structure of AES and to concentrate especially on the four stages utilized as a part of each round of AES: (1) byte substitution, (2) move lines, (3) blend sections, and (4) include round key

ii. AES is a block cipher with a block length of 128 bits.

iii. AES takes into consideration three distinctive key lengths: 128, 192, or 256 bits. The greater part of our talk will expect that the key length is 128 bits. Encryption comprises of the 10 rounds of preparing for 128-bit keys, 12 rounds of handling for 192-bit keys, and 14 rounds of preparing for 256-bit keys.

IV. Proposed System

In Proposed system, we describe the LDSS system design. First, we refer the overview of LDSS (Lightweight secure data sharing scheme), and then we present LDSS-CP-ABE algorithm and system operations.

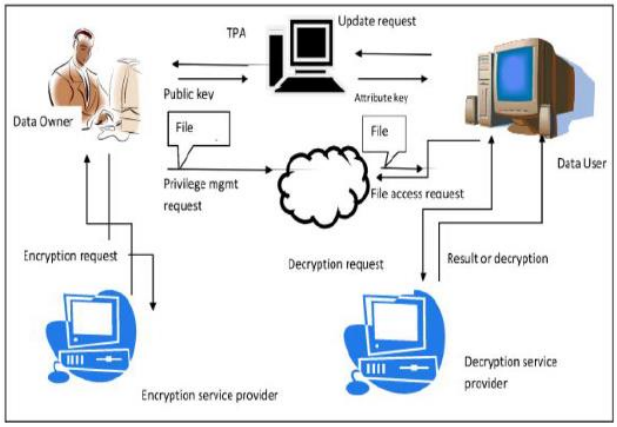

Fig 1. A lightweight data-sharing scheme (LDSS) framework

In Proposed system, we develop the Architecture of LDSS by using 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)

Firstly DO send data to the cloud. Since the cloud isn't believable, data must be encoded before it is transferred. The DO characterizes get to control approach as access control tree which strategies are, for example, read the data, compose the data. Data documents to relegate which qualities a DU ought to acquire on the off chance that he needs to get to a specific data record. In LDSS, data records are altogether encoded utilizing symmetric encryption system, and the symmetric key for data encryption is additionally scrambled utilizing attribute based encryption (ABE).

In our proposed framework, data owner, TPA is available on break even with level of specialist. Data owner right off the bat should enroll or login on site then as it only work like a CSP (cloud specialist co-op) at that point he can transfer his own documents on cloud in encoded design. Data client can enlist or login on site for access for records ,After login of data client on cloud server at that point ask for goes to the data owner then data owner choose the favor of documents access to client or not. Data client has affirmation from data owner on the off chance that he endorses the demand of data client. Outsider approval is utilized to monitories the data owners exercises likewise it can check the trustworthiness, solidness of records which are transferred by data owner on mobile cloud computing. Trusted authority (TA) likewise creates the report for data owner. While asking for of data client or the like of data from cloud, data owner select the part for data client and furthermore after endorsement of clients ask for he send the general population key to data client through the email then data client can recover the data from cloud by entering the key on site yet this data it as encryption so to decode that data .Data owner give the private key to data client from mail. At that point by utilizing this key Data User can decode that data. To alleviate the overhead on the customer side mobile devices, encryption service provider (ESP) and decryption service provider (DSP) are utilized. Both the encryption specialist co-op and the unscrambling specialist co-op are additionally semi-trusted. We change the customary CP-ABE algorithm and outline a LDSS-CP-ABE algorithm to guarantee the data security while outsourcing computational undertakings to ESP and DSP, additionally we utilized the AES (Advanced Encryption Standard) algorithm to scramble and decode the general data which is transferred on mobile cloud by data owner.

V. Conclusion

In late year, Attribute Based Encryption (ABE) algorithm utilized for cloud yet mobile device has constrained asset and Attribute Based Encryption is computationally escalated, so ABE isn't reasonable for mobile devices. In this paper we propose LDSS for secure sharing of data on mobile cloud, Also we can utilize Advance Encryption Standard (AES) for perform encryption and unscrambling of data. Proposed framework lessens computational overhead on mobile device. We utilize intermediary servers for encryption and unscrambling additionally decreases time many-sided quality by utilizing sluggish re-encryption strategy. Likewise we allude Third Party Authorization (TPA) for validation reason .By utilizing TPA we can check honesty, solidness, consistency of related documents which are transferred by data owner.

VI. REFERENCES

[1]. 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.

[2]. Kan Yang, XiaohuaJia, KuiRen: "Attribute-based fine-grained access control with efficient revocation in cloud storage systems". ASIACCS 2013, pp. 523-528, 2013.

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

[4]. 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. 350364

[5]. 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

[6]. 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

[7]. Kan Yang, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: "DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems". IEEE

Transactions on Data Forensics and Security, Vol. 8, No. 11, pp.1790 1801, 2013.

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

[9]. 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 Data, Computer and Communications Security" (ASIACCS), pp. 239-248, Jun. 2014.

[10]. ChenglinShen, Heng He. "A Lightweight Secure Data Sharing Scheme for MobileCloud Computing". Ruixuan Li, Member, IEEE 2016.

[11]. 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.

[12]. 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.

[13]. 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.

[14]. 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.

ABOUT AUTHORS:

S.V.R.DURGA BHAVANI is currently pursuing her M.Tech Computer Science & Engineering at Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram.

Dr. K V V S Narayana Murthy is currently working as a Professor in Computer Science and Engineering at Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram. He has an 16 years of teaching experience. His research interests include data mining, Network Security and areas of expertise in DLD, CO, FLAT, CD etc.

Dr. D. MOHAN REDDY received the B.Tech. Degree from Jawaharlal Nehru Technological University, Hyderabad, India and he received the M.E from Anna University, Chennai and Ph.D from Sri Venkateswara University, Tirupati, India. Presently he is working as a Professor & Principal in Amalapuram Institute of Management Sciences and College of Engineering, Mummidivaram. His research areas of interests are power electronic converters & Intelligence Systems.