IJSEAT International Journal of Science Engineering and Advance Technology

Mobile Cloud Computing System Using Lightweight Secure Data Sharing Scheme

[1]Kola Naga Lakshmi, [2]K.V.V.L. Madhuri
[1]Final year student, MCA, [2]Assistant Professor
[1,2]Dept. of computer science, IDEAL College of Art & science.,
Viduyutnagar, Kakinada, E.g.dt, Ap, India.

ABSTRACT:

We propose a lightweight data sharing scheme (LDSS) for mobilecloud computing. It receives CP-ABE, an entrance control innovation utilized in typical cloud condition, yet changes the structure of access control tree to make it appropriate for mobile cloud situations. LDSS moves a substantial bit of the computational serious access control tree change in CP-ABE from cell phones to outer intermediary servers. Moreover, to lessen the client revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems.

KEYWORDS: private keys, re-encryption, symmetric key.**1] INTRODUCTION:**

Regularly, cell phones just have restricted extra room and figuring power. Despite what might be expected, the cloud has colossal measure of assets. In such a situation, to accomplish the tasteful execution, it is fundamental to utilize the assets given by the cloud service provider (CSP) to store and share the data.

These days, different cloud mobile applications have been broadly utilized. In these applications, individuals (dataowners) can transfer their photographs, recordings, reports and different documents to the cloud and offer these data with other individuals (data clients) they like to share. CSPs additionally give data the executives usefulness to dataowners. Since individual data records are touchy, dataowners are permitted to pick whether to make their data documents open or must be imparted to explicit data clients. Unmistakably, data protection of the individual touchy data is a major worry for some dataowners.

2] LITERATURE SURVEY:

[1] Cong Wang we research the issue of secure and proficient comparability look over re-appropriated cloud data. Comparability look is a crucial and incredible asset broadly utilized in plaintext data recovery, however has not been very investigated in the scrambled data space. Our instrument structure first endeavors a stifling method to assemble capacity effective similitude watchword set from a given record accumulation, with alter separate as the closeness metric. In view of that, we at that point manufacture a private trie-navigate seeking list, and show it effectively accomplishes the characterized similitude look usefulness with consistent hunt time unpredictability. We formally demonstrate the protection saving assurance of the proposed system under thorough security treatment.

[2] Kan Yang we plan an entrance control structure for cloud storage frameworks that accomplishes fine-grained get to control dependent on an adjusted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach. In the proposed plan, a productive characteristic repudiation technique is proposed to adapt to the dynamic changes of clients' entrance benefits in huge scale frameworks. The investigation demonstrates that the proposed access control conspire is provably secure in the irregular prophet model and effective to be connected into training.

3] PROBLEM DEFINTION:

When all is said in done, we can isolate these methodologies into four classes: straightforward ciphertext get to control, various leveled get to control, get to control dependent on completely homomorphic encryption and access control dependent on attribute based encryption (ABE). Every one of these proposition are intended for non-mobile cloud condition

Tysowski et al. considered a particular cloud computing condition where data are gotten to by asset compelled cell phones, and proposed novel adjustments to ABE, which allocated the higher computational overhead of cryptographic activities to the cloud supplier and brought down the all-out correspondence cost for the mobile client.

4] PROPOSED APPROACH:

We propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment.

The main contributions of LDSS are as follows:

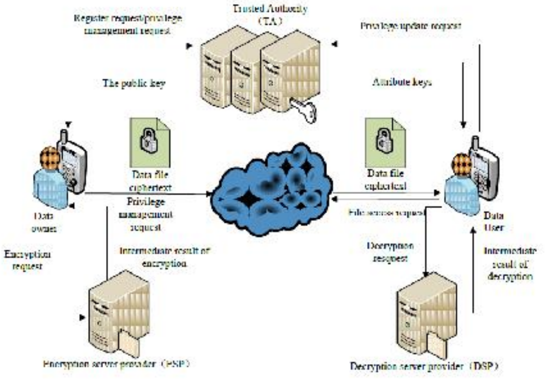
We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext.

We use proxy servers for encryption and decryption operations. In our approach, computational intensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on client side mobile devices. Meanwhile, in LDSS-CP-ABE, in order to maintain data privacy, a version attribute is also added to the access structure. The decryption key format is modified so that it can be sent to the proxy servers in a secure way.

We introduce lazy re-encryption and description field of attributes to reduce the revocation overhead when dealing with the user revocation problem.

Finally, we implement a data sharing prototype framework based on LDSS.

5] SYSTEM ARCHITECTURE:


Register request/privilege management request
Trusted Authority (TA)
Privilege update request
The public key
Attribute keys
Data file ciphertext
Data file ciphertext
Privilege management request
Data owner
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)

6] PROPOSED METHODOLOGY:

System Framework:

The advancement of cloud computing and the ubiquity of keen cell phones, individuals are bit by bit getting acclimated with another period of data sharing model in which the data is put away on the cloud and the cell phones are utilized to store/recover the data from the cloud. In these applications, individuals (dataowners) can transfer their records and different documents to the cloud and offer thesedata with other individuals (data clients) they like to share. CSPs additionally give data the board usefulness to dataowners. Since individual data documents are delicate, dataowners are permitted to pick whether to make their data records open or must be imparted to explicit data clients. Unmistakably, data security of the individual delicate data is a major worry for some dataowners. We propose LDSS, a system of lightweight data sharing plan in mobile cloud. It has the accompanying six segments. (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):

At the point when the dataowner (DO) registers on TA, TA runs the algorithm Setup() to produce an open key PK and an ace key MK. PK is sent to DO while MK is kept on TA itself. DO characterizes its own characteristic set and doles out credits to its contacts. All these data will be sent to TA and the cloud. TA and the cloud get the data and store it. DO transfers data to the mobile cloud and offer it with companions. DO decides the entrance control strategies. DO sendsdata to the cloud. Since the cloud isn't tenable, data must be encoded before it is transferred. The DO characterizes get to control approach as access control tree on data documents to allot which attributes a DU ought to acquire on the off chance that he needs to get to a specific data record.

Data User (DU):

DU logins onto the framework and sends, an approval solicitation to TA. The approval demand incorporates attribute keys (SK) which DU as of now has. TA acknowledges the approval solicitation and checks the solicitation and a produce property keys (SK) for DU. DU sends a solicitation for data to the cloud.Cloud gets the solicitation and checks if the DU meets the entrance necessity. DU gets the ciphertext, which incorporates ciphertext of data documents and ciphertext of the symmetric key. DU decode the ciphertext of the symmetric key with the help of DSP. DU utilizes the symmetric key to unscramble the ciphertext of data documents.

Trusted Authority:

To make LDSS plausible by and by, a confided in power (TA) is presented. It is mindful of creating open and private keys, and dispersing ascribe keys to clients. With this system, clients can share and access data without monitoring the encryption and decoding tasks. We expect TA is altogether believable, and a believed channel exists between the TA and each client. The way that a believed channel exists doesn't imply that the data can be shared through the confided in channel, for the data can be in a substantial sum. TA is just used to exchange keys (in a little sum) safely between clients. Furthermore, it's mentioned that TA is online all the time since data clients may get to data whenever and need TA to refresh quality 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 the request; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.

LDSS POLICY ATTRIBUTE BASED ALGORITHM:

INPUT: DO,TA,PK,MK,M,K,CT,SK

Step1:in system initialize the data owner registers on TA, TA to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA.

Step2: DO defines its own attribute set and assigns attributes to its contacts. All these information will be sent to TA and the cloud.

Step3: DO selects a file uploaded and encrypts it using a symmetric key *K*, generating ciphertext *C*.

Step4: DO uploads C, CT and access control policy to the cloud.

Step5: DU logins onto the system and sends, an authorization request to TA.

Step6: TA generate attribute keys for DU.

Step7: DU sends a request for data to the cloud.

Step8: Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses the request, otherwise it sends the ciphertext to DU.

Step9: DU uses the symmetric key to decrypt the ciphertext of data files.

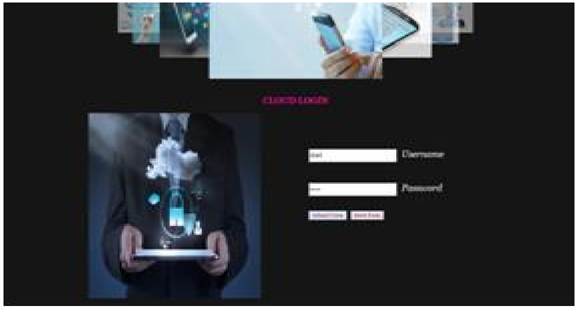
Step10: DO informs TA and the cloud that one attribute has been revoked from a specific DU.

Step11: TA and the cloud update the information of DU in database.

Enhancement:

Proposing present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext-policy attribute-based hybrid encryption

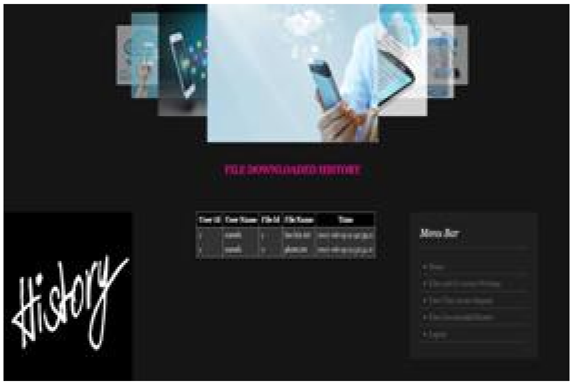
8] RESULTS:



CLOUD LOGIN

Username

Password



FILE DOWNLOADED HISTORY

User Id	User Name	File Id	File Name	Time
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

9] CONCLUSION:
As of late, numerous examinations on access control in cloud depend on attribute-based encryption algorithm (ABE). Nonetheless, customary ABE isn't reasonable for mobile cloud since it is computationally escalated 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, along these lines it can take care of the safe data sharing issue in mobile cloud.

10] 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, 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.

[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: 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.

[13] 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.

[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 Data, 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.

Ms. Kola Naga Lakshmi is a student of PG department of computer science in IDEAL college of Art & Sciences, Kakinada. Presently she is in final year MASTER COMPUTER APPLICATION (MCA) in this college and affiliated to Adikavinannaya University, Rajamahendravaram, Andhra pradesh. She received her BSC (CS) from VSR DEGREE COLLEGE Yeleswaram in the year of 2016. Her area of interest includes cloud computing, and web designing all current trends and techniques in computer science.

Ms. K.V.V.L MADHURI is presently working as Assistant Professor in P.G Department of Computer science, Ideal college of Arts & sciences, Kakinada. She obtained her M.Sc in computer science from Andhra University. Her areas of interest include Software Engineering, Data base management system, Computer networks etc.