A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

V. Kruthika, MCA, M.Sc.,M.Phil.,B. Ed.,
Assistant Professor
PG &Research Department of Computer Science and Applications
Vivekanandha College of Arts and Sciences for Women (Autonomous)

J. Valarmathi, MCA, M.Phil.,
Assitant Professor
PG &Research Department of Computer Science and Applications
Vivekanandha College of Arts and Sciences for Women (Autonomous)

***Abstract*:- With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.**

I.INTRODUCTION

Cloud computing means storing data and accessing that data from the Internet instead of Using Traditional hardware for most of the operations. More than 50% of IT companies have moved their Business to the cloud. Sharing of data over the cloud is the new trend that is being set on. The amount of data generated on a day to day life is increasing and to store that all of the data in traditional hardware is not possible because of limited storage capacity. Therefore, transferring the data to the cloud is a necessity where the user can get unlimited storage. Security of that data over is the next big concern for most of us. After uploading the data to the cloud use loses its control over that data.

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. Therefore, privacy of the personal sensitive data is a big concern for many data owners. When any of the people upload the data onto the cloud they are leaving their data in a place where monitoring

over that data is out of their control, the cloud service provider can also spy on the personal data of the users. When someone has to share data over the data they have to share the password to each and every user for accessing the encrypted data which is cumbersome. Therefore, to solve this problem data should be encrypted before uploading it onto the cloud which can be safe from everyone.

Now the data encryption part brings some new problems such as we have to provide an efficient encryption algorithm such that if the data Is in encrypted format it cannot be easily to get break or get accessed by any exploiters. The next big concern is time consumption for encryption. Traditional Hardware with big configuration can encrypt data in short amount of time but limited resource devices suffer from this problem. They require more amount of time of encryption and decryption. So, an efficient crypto system is to be proposed which can worked equally or heterogeneously on all of the devices.

II.RELATED WORK

Attribute-based encryption (ABE) is proposed by Sahai and Waters. Attribute-based encryption (ABE) is a moderately late approach that re-evaluates the idea of public key cryptography. Attribute-based encryption is also referred to as ABE is a sort of public-key encryption wherein the secret key of a person and the cipher-text is established upon attributes. In an ABE, a person’s keys and cipher-texts are labeled with units of descriptive attributes and a symmetric key can decrypt a selected cipher-text only if there's a match between the attributes of the cipher-text and the person’s key. It reduces the quantity of key used and hence makes encryption and decryption technique faster

III.EXISTING SYSTEM

With 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. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data. 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. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

Disadvantages

There is no proper mechanism for providing the security for data that is presented in the mobile cloud.2.user authentication and revocation cost will be high.

IV.PROPOSED SYSTEM

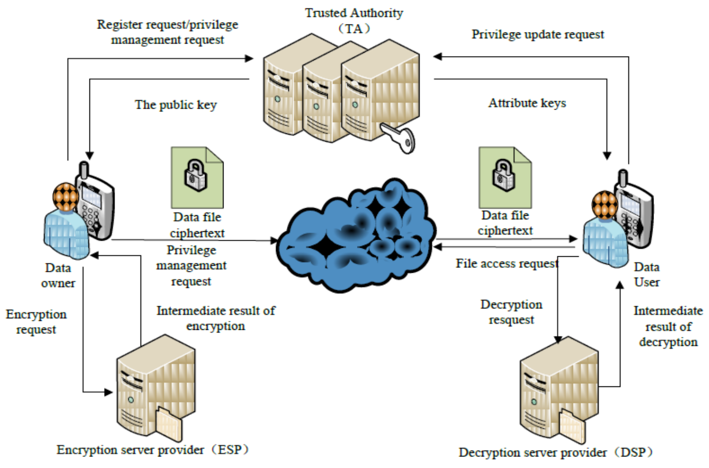
Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. However, the data encryption brings new problems. How to provide efficient access control mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owner's effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data access control over cipher text. In these researches, they have the following common assumptions. First, the CSP is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE). Allthese proposals are designed for non-mobile cloud environment.

OTP which will be matched with key In our proposed system data is encrypted before uploading to the cloud. Combination of Attribute Based Encryption and Byte Rotation Algorithm are used for the encryption of the data. ABE will help to identify the attributes of the data and BREA will perform matrix operations on the block of the data to be encrypted. After performing encryption operation, a random key is generated alongside the encrypted data. Data will be send in encrypted format to respective user. To decrypt this data receiver has to enter the One Time Password generated using ABE algorithm

Advantages

We are providing methods for efficient access of the data. Performance has been increased with the reduced cost.

V.ARCHITECTURE DIAGRAM PROPOSED SYSTEM ALGORITHM:


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 resquest
Intermediate result of decryption
Encryption server provider（ESP）
Decryption server provider（DSP）

Step-1: Start
Step-2: Accept the data from the user.
Step-3: The Attributes of the data from the users' formats are obtained by the Attribute-Based Encryption.
Step-4: With the help of these Attributes, Random Key is generated, and type of data is obtained for encryption by BRE algorithm.
Step-5: The data is converted into equal number of blocks and N x N matrix will be generated on the basis of these blocks.
Step-6: Based on no. of blocks, pool of threads will be created.
Step-7: Run the threads in multi core system to create encrypted data in short amount of time.
Step-8: A secret key is generated in order to open the encrypted file which is stored in the cloud.
Step-9: The secret key is shared to the user via email or mobile number of the authorized user. This key will be used to decrypt the encrypted file

VI. IMPLEMENTATION

This period of the venture is critical in light of the fact that at this stage the hypothetical plan is changed over into functional one. This stage is a basic stage since this stage require exceptionally exact arranging and need the learning of existing framework and its detriments. The execution stage ought to be created by considering every one of the prerequisites, imperatives. The new framework ought to be successful and work appropriately

ADMIN MODULES

1.Text Encryption and Decryption
2.Image Encryption and decryption
3.Text request
4.Image request

SERVER SIDE

5.View encrypted data
6.View user request
7.Provide password

1.Text Encryption and Decryption:

In this module user encrypted the plain text to encrypted format and uploaded to the cloud. The encryption is done by using a password. Only using this password only any one can decrypt the text. The user upload the password also include with encrypted data. The trusted authority id responsible for passing the password to the requested user

2.Image Encryption and decryption:

Like the same as the image encryption is also done. And the encrypted images and password will also be uploaded to the cloud. The trusted authority id responsible for passing the password to the requested user

3.Text request:

Any user can view the file uploaded in the server. All the files are in encrypted format. User cant view the files without know the password. For view the file first user need to request the password to Trusted Authority The Authority check the user and provide the password for valid user.

4.Image request Image:

Request is also same as the Text Request. The list of images can view in the application. But user can only view the images after getting the password from trusted authority

5.View Encrypted Data:

The user uploaded encrypted data can be view in the server side. The trusted authority act as server they have the responsibility to provide password for the requested user.

6.View user request:

After user view the encrypted data they can request the password for encrypted data. This user request can be view in the Truste.

*7.**Provide password:***

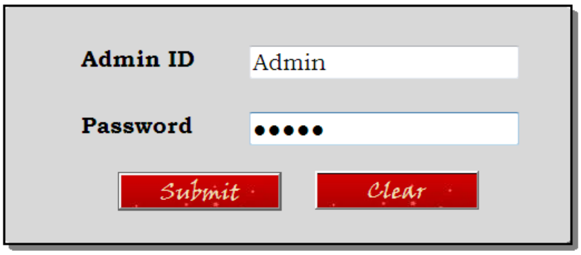
After view the request Trusted authority validating the user and if the user is valid the Trusted authority provide password for the requested file via email. Using this password user can decrypt the file.

VII.RESULT

Data owners inscribe the information having a particular get right of entry to action this that one handiest input users whose attributes accomplish the get admission to program may well purchase the analogous private decryption key from a trusted authority.

In CP-ABE is taken into account as a bright solid get right of entry to keep an eye on operation for goods distribution situation no centralized depended on third violence exists, case in point, detract computing, vagrant detailed networks (MANET), Peer-to-Peer (P2P) networks. In the most term situation, on the one cup attributes are allocated to purchasers as institute of your art CP-ABE schemes, on the disparate gold a wholly unique personality(ID) is maintaining every single shopper. That is, the two attributes and the ID are planted right into a purchaser' sinner most key.

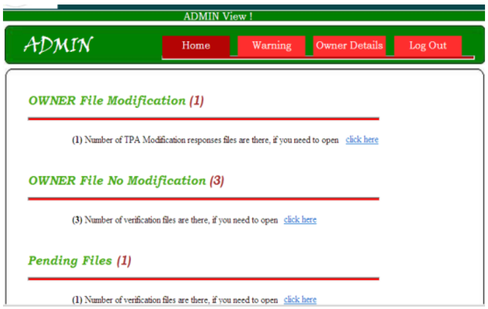
Encryption set of rules whole caboodle by waltz: initially, define trace literals in conjunctive/disjunctive reasonable forms as an blame organization to involve the recipients of one's objective categorize; moment, nullify pirated users byincorporating their identities in the direction of through to the Ciphertext



Admin ID: Admin

Password: ●●●●●

Fig 1: Admin Login



ADMIN View !

OWNER File Modification (1)

(1) Number of TPA Modification responses files are there, if you need to open click here

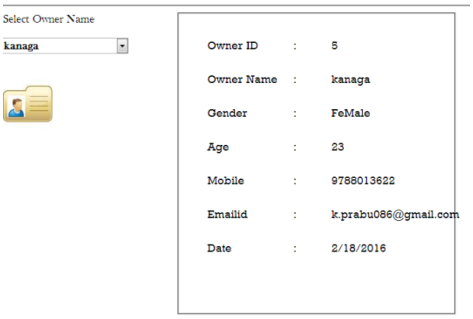
OWNER File No Modification (3)

(3) Number of verification files are there, if you need to open click here

Pending Files (1)

(1) Number of verification files are there, if you need to open click here

Fig 2: Admin Home

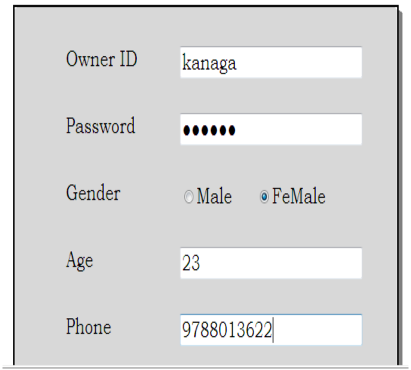


Select Owner Name

kanaga

Owner ID	:	5
Owner Name	:	kanaga
Gender	:	FeMale
Age	:	23
Mobile	:	9788013622
Emailid	:	k.prabu086@gmail.com
Date	:	2/18/2016

Fig 3:Owner Details



Owner ID: kanaga

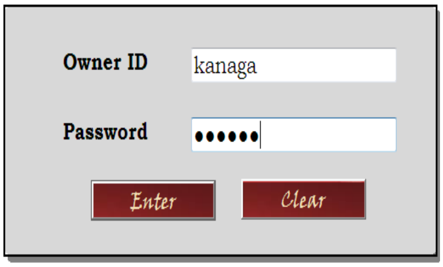
Password: ●●●●●●

Gender: ○ Male ● FeMale

Age: 23

Phone: 9788013622

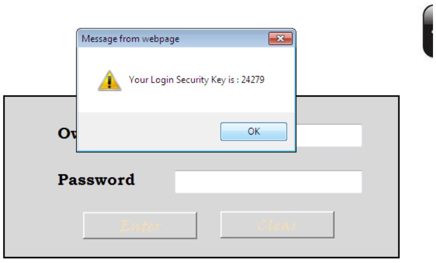
Fig 4: Owner Registration



Owner ID: kanaga

Password: ●●●●●●

Fig 5:Owner Login

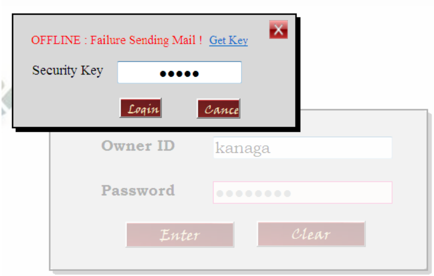


Message from webpage

Your Login Security Key is : 24279

OK

Fig 6:Owner Received Security key



OFFLINE : Failure Sending Mail ! Get Key

Security Key •••••

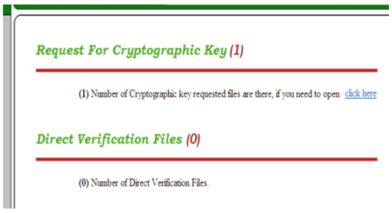
Login Cance

Owner ID kanaga

Password ••••••••

Enter Clear

Fig 7: Owner Received key offline



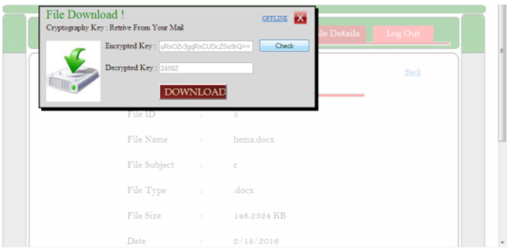
Request For Cryptographic Key (1)

(1) Number of Cryptographic key requested files are there, if you need to open click here

Direct Verification Files (0)

(0) Number of Direct Verification Files.

Fig 8: Owner Home Page



File Download !

Cryptography Key : Retrive From Your Mail

Encrypted Key : uRsOZv3gqRxCUDcZ5io9rQ==

Decrypted Key : 24562

Check

DOWNLOAD

File ID : 5

File Name : hema.docx

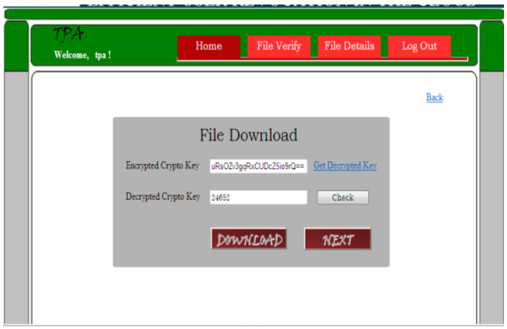
File Subject : c

File Type : .docx

File Size : 146.2324 KB

Date : 2/18/2016

Fig 8: Key Verification



File Download

Encrypted Crypto Key uRsOZv3gqRxCUDcZ5io9rQ== Get Decrypted Key

Decrypted Crypto Key 24652 Check

DOWNLOAD NEXT

Fig 9: File download

VIII. CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE isnot suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do cipher text retrieval over existing data sharing schemes.

REFERENCES

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

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

[3] Qihua Wang, HongxiaJin. "Data leakage mitigationfor discertionary access control in collaborationclouds".the 16th ACM Symposium on AccessControl Models and Technologies (SACMAT),pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan.OnImplementing Deniable Storage Encryption forMobile Devices.the 20th Annual Network andDistributed System Security Symposium (NDSS),Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficientaccess to outsourced data. in: Proceedings of the2009 ACM workshop on Cloud computing security.Chicago, USA: ACM pp. 55-66, 2009.

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

[7] Kan Yang, XiaohuaJia, KuiRen: Attribute-basedfine-grained access control with efficient revocationin cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8] G. Anuprabhavathi, R. Rajmohan, Energy-efficientand cost-effective resource provisioning frameworkfor map reduce workloads using dcc algorithm,International Journal of Engineering ScienceInvention Research & Development, Vol 2, issue 9,pp. 623-628, 2016.

[9] Crampton J, Martin K, Wild P. On key assignmentfor hierarchical access control.in: Computer SecurityFoundations Workshop. IEEE press, pp. 14-111,2006.

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

[11] Cong Wang, KuiRen, Shucheng Yu, andKarthikMahendraRajeUrs.Achieving Usable andPrivacy-assured Similarity Search over OutsourcedCloud Data. IEEE INFOCOM 2012, Orlando,Florida, March 25-30, 2012

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

[13] Kan Yang, XiaohuaJia, KuiRen, Bo Zhang,RuitaoXie: DAC-MACS: Effective Data AccessControl for Multiauthority Cloud Storage Systems.IEEE Transactions on Information Forensics andSecurity, Vol. 8, No. 11, pp.1790-1801, 2013.

[14] Stehlé D, Steinfeld R. Faster fully homomorphicencryption. in: Proceedings of 16th InternationalConference on the Theory and Application ofCryptology and Information Security. Singapore:Springer press, pp.377-394, 2010.

[15] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fullysecure key-policy attribute-based encryption withconstant-size ciphertexts and fast decryption. In:Proceedings of the 9th ACM symposium onInformation, Computer and CommunicationsSecurity (ASIACCS), pp. 239-248, Jun. 2014.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al.Attribute based proxy re-encryption with delegatingcapabilities. in: Proceedings of the 4th InternationalSymposium on Information, Computer andCommunications Security. New York, NY, USA:ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secureatrribute-based systems. in: Proceedings of the 13thACM Conference on Computer andCommunications Security. New York, USA: ACMpress, pp. 99-112, 2006.

[18] Yu S., Wang C., Ren K., et al. Attribute based datasharing with attribute revocation. in: Proceedings ofthe 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. Rolebasedaccess control models. Computer, 29(2): 38-47, 1996.

[20] Tian X X, Wang X L, Zhou A Y. DSP REEncryption:A flexible mechanism for access controlenforcement management in DaaS. in: Proceedingsof IEEE International Conference on CloudComputing. IEEE press, pp.25-32, 2009

[21] M Swarnamala, M Pajany, Smart Cloud SecurityBack-up System for High Recurrent Data in CloudStorage", IJSRSET, vol 3 (2), 2017, pp 82-85.