IMPLEMENTING AN EFFICIENT METHOD FOR SHARING DATA IN MOBILE CLOUD COMPUTING

D.Kousalya
B.Tech , Department of CSE, Narayana Engineering College Gudur, Affiliated to JNTUA, India
Kousalya824@gmail.com

V.Naga Bhaskar Rao,
Assistant Professor *Department of CSE, Narayana Engineering College Gudur, Affiliated to JNTUA, India Vnbr80@gmail.com*

G.Prasanna
B.Tech Department of CSE, Narayana Engineering College Gudur, Affiliated to JNTUA, India
g.prasanna82972gmail.com

A.Jyothi Parimala
B.Tech Department of CSE, Narayana Engineering College Gudur, Affiliated to JNTUA, India
jyothi50698@gmail.com

ABSTRACT

Now cloud computing is very popular for mobile devices to store, retrieve and access that information from anywhere at any time. The data security problem is becoming an additional issue to prevent further development of the mobile cloud. As they have limited resources and resources. we introduce a weak data sharing system (LDSS) for a laptop. It acquires access technology used in a common cloud environment known as CP-ABE, in moving cloud environments that transform the building. The LDSS distributes a large portion of the computational access control transformation in CP-ABE from mobile devices to external proxy servers. However, to reduce the user relinquishment cost, it introduces attribute description fields , which is a perplexing issue in program based CP-ABE systems.

Keywords: *I*– CP-ABE, Data Sharing Scheme, Cloud computing.

1. INTRODUCTION

Mobile devices are become more popular by the development of cloud computing, people became familiar to share data and stored on the cloud ,which are used to retrieve the data[1] .The cloud has large amount of resources and it requires limited space and power[2]. In such a plot, it is crucial to use the resources provided by the cloud service provider (CSP) to achieve high performance which is used to store and share the data[3].

Cloud mobile applications plays vital role and it is used worldwide to share, store and retrieve the data. In these applications, owner of the data can upload any photos, videos, documents and other files to the cloud and share these data with other users. CSPs provides security for the data by preventing the users from manipulating and data management functionality from data owners. Data owners are allowed to set to make their data files public (every one) or can only be shared with certain or fixed data users, as the personal data files are responsive to modify[3]. Distinctly, we can say that it is considerably a immense challenge for many data owners for the privacy of the flexible data which is easy to modify.

However the futuristic access management and control mechanisms provided by the CSP are not supposed to be convenient, suitable and sufficient. It is highly difficult and impossible to meet the requirements of data owners. CSP may act as a secret agent on user and owner data for its economic concerns and for other reasons when data files are uploaded by the people onto the cloud, they are supposed to leave the data where it can be flexible to change and modify. It is very awkward if people are willing to share the encrypted data they need to send password to certain people to whom they want to share. The data should be divide into different groups by the data owner which is easier to send password to the particular groups[5]. Proceed towards requires simple access control. It is difficult to manage the password in both cases.

To secure the data against the CSP provider, data which can be flexible to change should be encrypted before uploading onto the cloud. It face critical problem like how to provide efficient access and easy management mechanisms on decryption which provide plain text to access only the authorized users. System provides data owners large and efficient management capability of the users, which allows to permit/cancel data access benefits on the data users. CSP is considered not to be biased and irregular .The data that is flexible to change must encrypt before uploading to the Cloud and by using the encryption/decryption key distribution we can control the user authorization. There are four categories of approaches like, simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE)[6]. These are designed for system cloud environment which have huge amount of storage and computational overhead resources and these are not available for mobile devices. ABE scheme takes prolonged time on mobile devices compared to systems and it takes more than 27 times to execute on a android than a computer. So computers take one minute and androids take half an hour to complete encrypt the data.It reduces the high cost and it is not suitable for smart phones. So we can say that is no way to sharing the secure data problem in mobile cloud. In this paper we use a Lightweight Data Sharing Scheme (LDSS) to share the secure data for mobile cloud computing. There some contributions like We adopt a CP-ABE algorithm based on ABE method called LDSS to manage access control over decrypted text.

To reduce the revocation overhead problem, we introduced the decryption. At last, the data shared based on LDSS ,it can reduce the overhead on the user side and less cost on server side[7]. This is an advantage to at an[8] untrusted server in the presence of transactional updates that run directly on the database, and develop the first solutions to this problem.

2 .LITERATURE SURVEY

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

Authors Chenglin Shen, Heng He Description: This paper describes that Mobile device has limited storage and limited computing resources so data can be stored on mobile cloud computing. Any user can upload data on that cloud also anyone can access that data, so there is security issue related to that data so, it need to provide security to that data to prevent from unauthorized user. In this paper, design LDSS-CP-ABE algorithm for provide security to the mobile cloud computing.

2. How to build a trusted database system on un trusted storage. Authors: Maheshwari U, Vingralek R, Shapiro W.Description:In this Paper, It can identify the problem ensuring trustworthiness of data are

increasingly accessed by resourceconstrained mobile devices for which the processing cost must be minimized. this paper, re-encryption mechanism is

3. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. Authors: Cong Wang, KuiRen, Shucheng Yu Description :In this paper, It investigate the problem of secure and efficient similarity search over outsourced cloud data.In this any user can upload data on cloud and also achieves the usable and privacy assured similarity search over outsourced cloud data.

4. A flexible mechanism for access control enforcement management in DaaS. In: Proceedings of IEEE International Conference on Cloud Computin.Authors:Tian X X, Wang X L, Zhou A Y. Description :In this paper, First present an approach to implement the flexible access control enforcement management by applying a DSP re-encryption mechanism also this re-encryption mechanism is used repeatedly.

5. Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds.

3.PROPOSED WORK

LDSS is proposed, a framework for sharing lightweight data in a moving cloud .It has the following six elements.

(1) Data Owner (DO): DO load data into a mobile cloud and share it with friends. DO determines access control policies.

(2) Data User (DU): DU captures data from the moving cloud.

(3) Trust Authority (TA): The TA is responsible for producing and distributing the key of responsibility**.**

(4) Encryption Service Provider (ESP): ESP provides encryption services for DO.

(5) Decryption Service Provider (DSP): The DSP provides DU data compilation services.

(6) Cloud Service Provider (CSP): CSP stores DO information. It faithfully performs the tasks requested by the DO, while it may seek information DO stored in the cloud.

A DO sends data to the cloud. Since the cloud is unreliable, the data must be encrypted before uploading. DO describes the access control policy in the form of an access control tree in the data files to provide what attributes the DU should acquire if it wants to access a specific data File.

4. RESULTS AND DISCUSSION

In future work, we will develop new ways to ensure data integrity. To advance the power supply in the cloud, we will also learn how to generate maximum returns over existing data sharing systems.

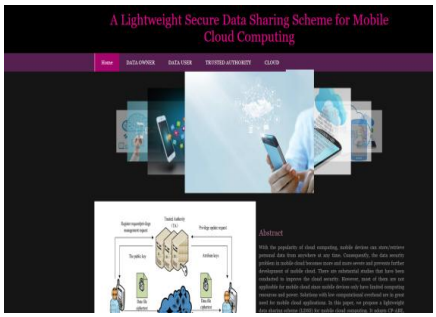

Fig.1:Home Page

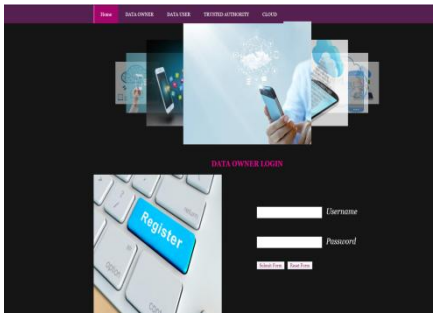

Fig.2:Data Owner Login Page

ISSN: 2278-4632
Vol-10 Issue-5 No. 6 May 2020

After executing it will shows fig1,in home page it shows data owner ,user ,trusted authority &cloud .we must register data owner and then we need login in as shown in fig2

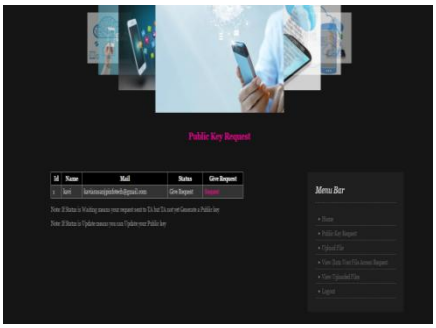

Fig.3:Data Owner with E-mail

Fig.4:Key Generate

After login it shows a waiting request as shown in fig 3 and later we need to login in trusted authority &it will shows the public key is generated ,as show in fig 4.After that we must register with Data User & login with data user as shown below fig 5.

Fig.5 Data User Registration

6. CONCLUSION

In recent years, most cloud access control research is based on the encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because devices contain solid content and only mobile devices have limited resources. This project uses the LDSS to address this issue. Introducing the novel LDSS-CP-ABE algorithm to migrate larger compression from mobile devices to proxy servers, so it can solve a secure data sharing problem in the mobile cloud

REFERENCES

1. AdamSkillen and Mohammad Mannan. On Using Undesirable Encryption for Mobile Device Storage. 20 Year Network and Distributed System Security Symposium (NDSS), February 2013.
2. Brakerski Z, Vaikuntanathan V. Full-length Homomorphic encoding from (standard) LWE. in Proceedings of the IEEE Symposium on the Foundations of Computer Science. California, USA: IEEE press, p. 97-106, Oct. 2011
3. Gentle C, Halevi S. Implementing a fully automated Homoeomorphic writing system. in: Advances in Cryptology-EUROCRYPT 2011. Berlin, Heidelberg: Springer Press, p. 129-148, 2011
4. P Penchalaiah, M Vijay Kumar *etl*, **"***A Research Threshold Efficient Hybrid Encryption Schema for Secure File System***",** International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, **(SCOPUS)** Volume-8, Issue-2S3, Page 888 –891,July 2019
5. Penchalaiah P, Ramesh Reddy K, "Random Multiple Key Streams for Encryption with Added CBC Mode of Operation*", Perspectives in Science (ISSN: 2213-0209), ()*, Volume 8, pp.57-62, April 2016.
6. Penchalaiah P, Ramesh Reddy K, "Secure and Cost Effective Cryptosystem Design Based on Random Multiple Key Streams", *Journal of Information Security Research,(* ISSN: 0976-4143) *DIRF Publisher*, Volume 7, Number 1, pp. 29-40, March 2016
7. Qihua Wang, HongxiaJin. "Data reductions that reduce access control out of the cloud collaboration". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun.
8. Wang W, Li Z, Owens R, et al. Secure and appropriate access to the information entered In: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM p. 55-66, 2009.

