IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 9, September 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109066 |

Data Privacy and Implications in Cloud Computing

Mr.A.M.Rangaraj[1], Mr.K.Raghavendra[2], Mr.D.Devarajulu[3]

Associate Professor, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, India[1]

MCA Student, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, India[2]

MCA Student, Department of MCA, Sri Venkateswara College of Engineering and Technology, Chittoor, India[3]

ABSTRACT: With the popularity of cloud computing, mobile devices can store and retrieve personal information from anywhere at any time. Consequently, the data security problem in mobile loud becomes more severe and prevents further development of mobile cloud. There are substantial studies have been conducted to improve the cloud security. Most of them are not applicable for mobile cloud since mobile devices has limited computing resources and power. Solutions with low computational overhead are in great need for mobile computing cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. Cloud has been around for two decades and it consists of the vast amount of data from all over the world. Most of the people at a personal level and organization level have moved their data to the cloud and share data across all-around the world. The main challenge faced by everyone is to share the data all over the world or at organization all level securely without giving away the important data to any exploiters. To overcome the challenge to share the data securely over the cloud, an efficient data encryption algorithm for encrypting data before sending it to the cloud. In this proposed we are using a combination of Attribute-Based Encryption and Byte Rotation Encryption Algorithm for encrypting the data before sending it to the cloud. This will help the user to securely store and share the data in encrypted form

KEYWORDS: Mobile cloud computing, Data Encryption, Access control, User Revocation Etc…

.

I. INTRODUCTION

Withtheimprovementofcloudcomputingthepopularityofsmartmobiledevices, people are gradually getting into answer a 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 their sources provided by the cloud service provider (CSP) to store and share the data. Nowadays, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also provide data management functionality for data owners. 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. Clearly, data privacy of the personal sensitive data is a big concern for many data owners. The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or Not very convenient. They cannot meet all the requirements of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which are very cumber, some. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data.

This paper is organized in five sections. After this introduction, in Section II, Existing System discussed of the paper, section III about the Proposed System of the paper, Section IV about Modules, as well as the novel feature of the proposed method. Finally, Sections V and VI provide the Simulation Results and the Conclusions, respectively.

II. EXISTING SYSTEM

With the continuous growth in development of cloud computing people are getting adept and 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109066 |

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 their sources 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 their sources provided by the cloud service provider to store and share the data.

Disadvantages:

1. There is no proper mechanism to provide the security for the data presented in the mobile cloud.
2. User authentication and revocation cost will be high.

III. PROPOSED SYSTEM

The architecture of the proposed system is shown in the figure which shows the users and the operations involved. The detailed description of the architecture is explained as follows:

- **Nodes :** The User is responsible for uploading and sharing its personal data on the cloud.
- **On-line and Off-line Services:** In On-line Service data will encrypted and directly transfer to the respective user. In Off-line Service if there is no Internet Connection the data will get encrypted first and then it will get stored in Main Server. Until the system does not come on-line the data will not be shared over the cloud
- **Cloud Service Provider:** Cloud service provider is responsible for providing all the required services to its users according to their demands.
- **Encryption and Decryption:** Here we are using the combination of ABE and BRE algorithm to encrypt and decrypt the files.
- **File Upload and Download:** the files which are uploaded on cloud are encrypted form. Users

ARCHITECTURE DIAGRAM

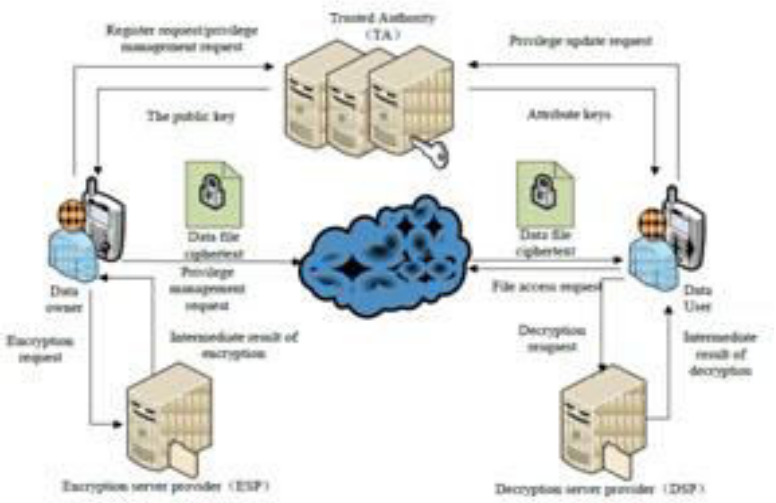

Fig.1: Application design

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109066 |

Up loader

The Main Responsibility of the Up loader is to upload a Document to the cloud storage. And view the files what the different up loaders uploaded. To download that document up loader has to get a key from the Authority.

Authority:

The Authority people is able to view the list of up loader, users in this case he has the another option if he need to add the up loader he need to add otherwise delete and also he is able to give the keys for the requests from the user and up loader

User:

The user can able to view the files if he wants to download the file he need to send the request to Authority after receiving the key he need to download.

IV. MODULES

1. Owner
2. Authority
3. User

Owner:

The Main Responsibility of the owner is to upload a Document to the cloud storage. And view the files what the different owner uploaded. To download that document owner have to get a key from the Authority.

Authority:

The Authority people is able to view the list of owner, users in this case he has the another option if he need to add the owner he need to add otherwise delete and also he is able to give the keys for the requests from the user and owner.

User:

The user can able to view the files if he wants to download the file he need to send the request to Authority after receiving the key he need to download.

V. SIMULATION RESULTS

1. **Home Page (Authority Login)**

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109066 |

2. **Data Owner**

3. **Data Owner Login**

4. **Up Load File**

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109066 |

5. **Authority Login**

6. **User Login**

7. **Downloads**

VI. CONCLUSION

In recent years, many studies on access control in cloud are totally based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices 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 over head from mobile devices on to proxy servers, thus it can help in solving the secure data sharing problem in mobile cloud. The experimental results show states that LDSS can ensures data privacy in mobile cloud and reduce the overload on users' side in mobile cloud. In future work, we will design the new approaches to ensure data integrity. To further tap the potential of mobile cloud, and also ensure how to do cipher text retrieval over existing data sharing schemes.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109066 |

REFERENCES

1. Gentry C, Halevi S. Implementing gentry's fully-homo morphic encryption scheme. in: AdvancesinCryptology–EUROCRYPT2019.Berlin,Heidelberg.
2. Brakerski Z, Vaikuntanathan V. Efficient fully homom orphic encryption from (standard) LWE.in:ProceedingofIEEESymposiumonFoundationsofComputerScience.California, USA.
3. Qihua Wang, Hongxia Jin."Data leakage mitigation for discretionary access controlling collaboration clouds ".the16thACM Symposium on Access Control Models and Technologies.
4. Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium.
5. Wang W, LiZ, Owens R, etal. Secure and efficient access to outsource data. in: Proceeding s of the 2019 ACM workshop on Cloud computing security. Chicago, USA.
6. Maheshwari U, Vingralek R, Shapiro W. How to build a trusted data base system on untrusted storage. In : Proceeding s of the 4th conference on Symposium on Operating System Design & Implementation.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details