A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

Mr. M.Sainath. Vidya Jyothi institute of technology, Hyderabad, India

Mr. M.Ratnakar. Vidya Jyothi institute of technology, Hyderabad, India

Mr. M.Karthik Reddy. Vidya Jyothi institute of technology, Hyderabad, India

Mr. P.RaviTeja. Vidya Jyothi institute of technology, Hyderabad, India

Ms. P.Sandhya (Assistant professor). Vidya Jyothi institute of technology, Hyderabad, India

Abstract - Because of the widespread adoption of cloud computing, mobile devices may now store and access personal data from any location at any time. As a result, the data security issue in the mobile cloud becomes increasingly serious. And is becoming increasingly severe, impeding the growth of mobile cloud. There are several studies available. that have been carried out in order to increase cloud security However, the most of them aren’t. Because mobile devices have low computational resources, they are ideal for mobile cloud. Power. Mobile cloud solutions with reduced computational overhead are in high demand. Applications. We propose a lightweight data sharing strategy (LDSS) for mobile devices in this study. Cloud computing is a term that refers to the use of It uses CP-ABE, an access control method often used in cloud computing. However, the structure of the access control tree is changed to make it suitable for mobile cloud. LDSS relocates a significant chunk of the computationally demanding access control tree. In CP-ABE, mobile devices are transformed into external proxy servers. In addition, to It provides attribute description fields to implement lazy revocation, which is a tricky issue in program-based CP-ABE systems, to lower the user revocation cost. First and foremost, the CSP is seen as trustworthy and inquisitive. Second, all important information is encrypted. prior to uploading to the cloud Third, user authorization for specific data is obtained via Key distribution for encryption and decryption We may categories these techniques into four categories in general. access control based on simple ciphertext, hierarchical access control, and access control based on Access control based on attribute-based encryption and completely homomorphic encryption (ABE). All of these suggestions are intended for use in a non-mobile cloud context. They eat a lot of food Mobile devices lack the storage and computing capacity that desktop computers.

1. INTRODUCTION

1.1 Introduction

People are progressively becoming acclimated to a new era of data sharing model in which data is kept on the cloud and mobile devices are used to store/retrieve data from the cloud, thanks to the rise of cloud computing and the popularity of smart mobile devices. Mobile devices often have limited storage space and processing power. The cloud, on the other hand, has a massive quantity of resources. In such a circumstance, it is critical to employ the cloud service provider's (CSP) capabilities to store and exchange data in order to achieve optimal performance. Various cloud-based mobile applications are now commonly utilized. People (data owners) can use these programmed to upload images, videos, documents, and other things. They like to share their data on the cloud with other individuals (data users). CSPs also give data owners the ability to govern their data. Due to the sensitivity of personal data files, data owners have the option of making their files public or just sharing them with selected data users. Data privacy of personal sensitive data is obviously a major concern for many data owners. The CSP's state-of-the-art privilege management and access control techniques are either insufficient or inconvenient. They are unable to address all of the needs of data owners. To begin with, when users transfer their data files to the cloud, they are doing it in a secure manner. placing the data at a location outside their control, and the CSP may monitor user data for commercial and/or other reasons. Second, if people only want to share encrypted data with certain users, they must transmit passwords to each data user, which is inconvenient.

The data owner can divide data users into multiple groups and send passwords to the groups with which they wish to share the data to make permission management easier. This method, however, necessitates fine-grained access control. Password management is a major concern in both scenarios.

To address the aforementioned issues, it appears that personal sensitive data should be encrypted before being transferred to the cloud, ensuring that the data is safe from the CSP. However, They use up a lot of storage and processing power, which isn't available on mobile devices. The fundamental ABE processes take substantially longer on mobile devices than on laptops or desktop computers, according to the experimental results in [26]. A smart phone takes at least 27 times longer to run than a computer (PC). This implies that a one-minute encryption procedure on a PC will take nearly half an hour to complete on a mobile device. Furthermore, present methods do not adequately address the issue of user privilege changes. A large revocation cost might come from such a procedure. This also does not apply to mobile devices. Clearly, In the mobile cloud, there is no adequate solution that can successfully tackle the safe data exchange problem. As the mobile cloud grows in popularity, it is becoming increasingly important to provide an effective and secure data exchange method.

In this research, we suggest a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing to overcome this issue.

1.2 Objective

Because of the widespread adoption of cloud computing, mobile devices may now store and access personal data from any location at any time. As a result, the data security issue in mobile cloud is becoming increasingly serious, impeding the growth of mobile cloud. There have been several research undertaken in order to enhance cloud security. However, because mobile devices have limited processing capabilities and power, the majority of them are not suitable for mobile cloud. Mobile cloud applications require solutions with a low computational overhead. We propose a lightweight data sharing strategy (LDSS) for mobile cloud computing in this study. It uses CP-ABE, an access control technique often used in cloud environments, but modifies the access control tree's structure to make it suited for mobile cloud. environments. LDSS offloads a considerable chunk of the CP-computationally ABE's costly access control tree transformation to external proxy servers. It also includes attribute description fields to implement lazy revocation, which is a tricky issue in program-based CP-ABE systems, to lower the cost of user revocation. The results of the experiments reveal that when users share data in mobile cloud settings, LDSS may efficiently minimize the overhead on the mobile device side..

2. Literature Survey

Review of access control models for cloud computing:

In the cloud, the connection between users and resources is fluid, and service providers and customers are rarely in the same security domain. In an open cloud computing environment, where each resource node may not be familiar, or even know each other, identity-based security (e.g., discretionary or obligatory access control models) cannot be applied. In most cases, users are recognized by their qualities or features rather than by established identities. Cross domain authentication frequently necessitates the use of a dynamic access control method. We will focus on three main kinds of access control mechanisms for cloud computing in this paper: Role-based models, attribute-based encryption models, and multi-tenancy models are the three types of models. We'll go over the existing research on the subject. each of the aforementioned access control models and their variations (technical methods, features, application, advantages and disadvantages), and indicate future research objectives for building access control models for cloud computing systems.

On Implementing Deniable Storage Encryption for Mobile Devices:

Encryption is an excellent way to protect data secrecy. In other cases, this is insufficient since users may be forced to provide their decryption keys. The data must be disguised in this situation so that its mere existence may be denied. To overcome this challenge, steganographic methods and deniable encryption algorithms have been developed. We investigate the feasibility and efficacy of deniable storage encryption for mobile devices, given the rapid growth of smartphones and tablets. We assess known difficulties and identify new ones that might jeopardize plausibly deniable encryption (PDE) in a mobile setting. To overcome these challenges, we created Mucilage, a technology that allows PDE on mobile devices by encrypting volumes and concealing them behind random data on the device's external storage. We apply what we've learned from recognized difficulties with deniable encryption on desktops to create novel defenses for threats unique to mobile devices. Deniable file systems with no impact on performance; efficient storage with no data growth; and restriction/prevention of known sources of leakage and disclosure are all key elements of Mucilage. To evaluate the feasibility and performance of Mucilage, we present a proof-of-concept implementation for the Android OS. We also construct a list of recommended practices that users should adhere to in order to prevent additional types of leakage and cooperation that might jeopardize deniability.

Secure and Efficient Access to Outsourced Data:

Cloud computing is crucial for providing safe and efficient access to massive amounts of outsourced data. We suggest a solution for solving this problem in owner-write-users-read applications in this work. We suggest encrypting each data block with a distinct key in order to enable flexible cryptography-based access control. The owner just has to keep a few secrets after implementing key derivation procedures. The key derivation technique employing hash functions will result in relatively little compute cost, according to the analysis. To prevent revoked users from accessing updated data blocks, we recommend using over-encryption and/or lazy revocation. We create systems to handle both outsourced data updates and changes in user access privileges. We look into the above and the safety of the proposed technique, as well as strategies for improving data access efficiency, are being investigated.

3. OVERVIEW OF THESYSTEM

3.1 Existing System

• Various cloud-based mobile applications are now commonly utilized. People (data owners) can use these programmed to upload images, videos, documents, and other things. They like to share their data on the cloud with other individuals (data users). CSPs are also offer data owners with data management functionality Due to the sensitivity of personal data files, Data owners have the option of making their files public or simply sharing them with others. with certain data users Clearly, the privacy of personal sensitive data is a major worry for many people. There are several data owners. Privilege management and access control technologies that are cutting-edge The CSP's services are either insufficient or inconvenient. They won't be able to satisfy all of the demands. data owners' requirements To begin with, when users transfer their data files to the cloud, they are doing it in a secure manner. leaving the data in an uncontrollable location, and the CSP may eavesdrop on user data for its own purpose’s Commercial interests and/or other factors may be at play. Second, each data must have a password sent to it. If a user only wants to exchange encrypted data with specific users, this is a time-consuming process. The data owner might separate data users into multiple groups to make permission management easier. Then give the passwords to the parties with whom they wish to share the information However, this strategy is ineffective. Fine-grained access control is required. Password management is a major concern in both scenarios.

3.1.1 Disadvantages of Existing System

• When consumers upload their data files to the cloud, they are handing over control of their data to a third party, and the CSP may monitor user data for commercial and/or other reasons.

2. If people only want to share encrypted material with a few others, they must transmit a password to each of them, which is inconvenient.

3.2 Proposed System

Personal sensitive data should be encrypted before being uploaded to the cloud to ensure that it is safe from CSPs. However, data encryption introduces new issues. It's difficult to create an effective access control system for ciphertext decoding so that only authorized users have access to plaintext data. In addition, the system must allow the data owner to control user privileges effectively. First and foremost, the CSP is seen as trustworthy and inquisitive. Second, before being uploaded to the Cloud, all sensitive data is encrypted. Third, user authorization for particular data is accomplished by the provision of encryption/decryption keys. In general, these systems may be divided into four categories: basic ciphertext access control, hierarchical access control, completely homomorphic encryption access control, and attribute-based encryption access control. (ABE). All of these ideas are geared for a non-mobile cloud environment. They use up a lot of storage and processing power, which isn't available on mobile devices.

Advantages of Proposed System

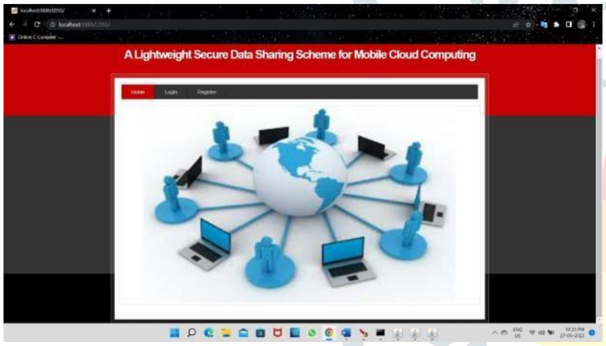
Reduce the processing burden on client-side mobile devices by a significant amount.

When dealing with the user revocation problem, employ lazy re-encryption and the description field of attributes to decrease revocation costs.

3.3 Proposed System Design

In this project work, I used five modules and each module has own functions, such as:

1. Data Owner (DO)
2. Data User (DU)
3. Trust Authority (TA)
4. Encryption Service Provider (ESP)


A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing
Home
Login
Register

5. Decryption Service Provider (DSP)
6. Cloud Service Provider (CSP)

3.3.1 Data Owner

DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies.

3.3.2 Data User

DU retrieves data from the mobile cloud.

3.3.3 Trust Authority

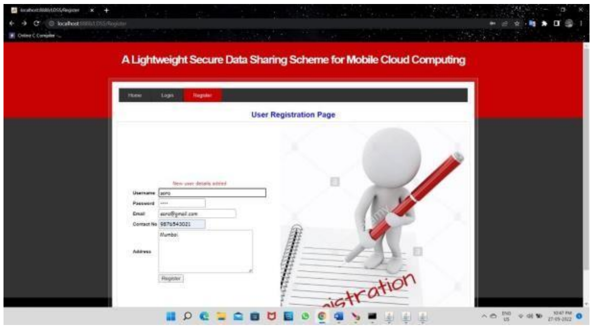
TA is responsible for generating and distributing attribute keys.

3.3.4 Encryption Service Provider

ESP provides data encryption operations for DO.

3.3.5 Encryption Service Provider

ESP provides data encryption operations for DO.


A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing
Home
Login
Register
User Registration Page
Register
registration

New user details added

Username: aoro
Password: ····
Email: aoro@gmail.com
Contact No: 9876543021
Address: Mumbai

3.3.6 Decryption Service Provider (DSP)

DSP provides data decryption operations for DU.

3.3.7 Cloud Service Provider (CSP)

4 Architecture

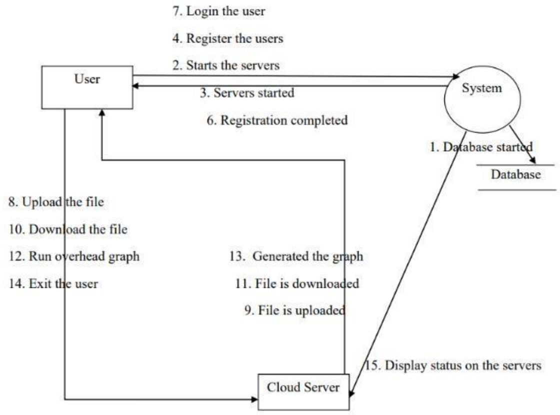


Fig 1: Frame work of Project

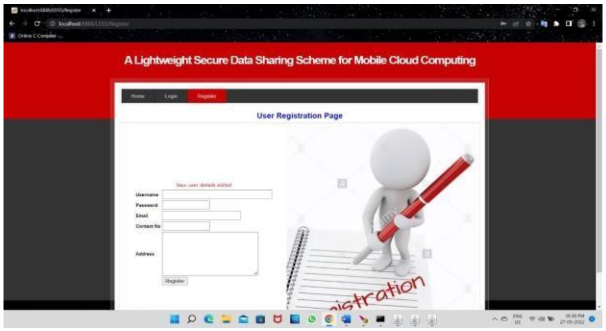
.

5 RESULTS SCREEN SHOTS

Home Page:

Upload File Page:

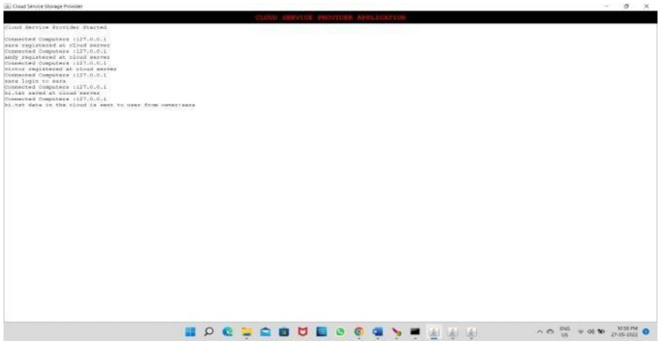
Upload Data:


A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing
Home
Login
Register
User Registration Page
Register
registration

New user details added

Username
Password
Email
Contact No
Address

Data Screen:

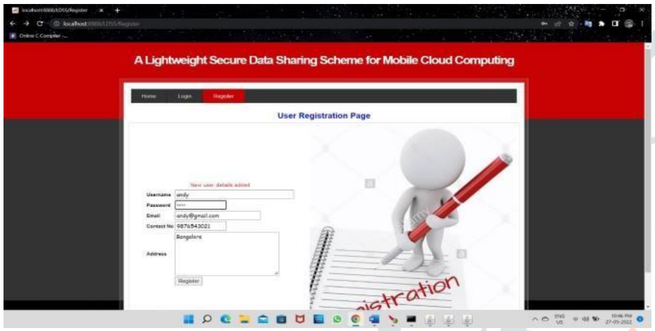


Cloud Service Storage Provider
CLOUD SERVICE PROVIDER APPLICATION

```
Cloud Service Provider Started

Connected Computers :127.0.0.1
sara registered at cloud server
Connected Computers :127.0.0.1
andy registered at cloud server
Connected Computers :127.0.0.1
victor registered at cloud server
Connected Computers :127.0.0.1
sara login to sara
Connected Computers :127.0.0.1
hi.txt saved at cloud server
Connected Computers :127.0.0.1
hi.txt data in the cloud is sent to user from owner:sara
```

Client fill Form:

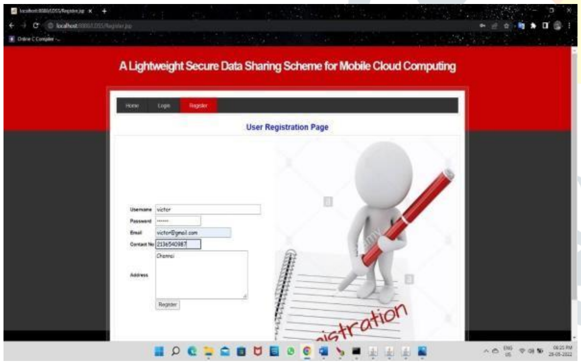


localhost:8888/LDSS/Register
localhost:8888/LDSS/Register
Online C Compiler -...
A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing
Home
Login
Register
User Registration Page
Register
registration

New user details added

Username: andy
Password: ****
Email: andy@gmail.com
Contact No: 9876543021
Address: Bangalore

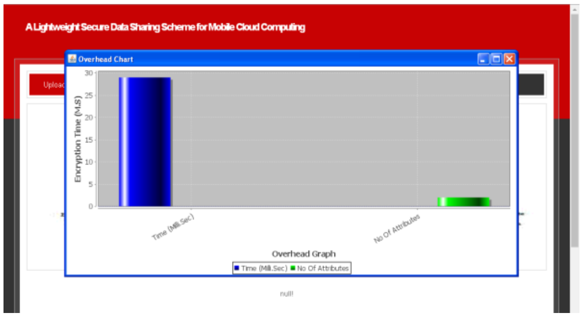
Data:



localhost:8888/LDSS/Register.jsp
localhost:8888/LDSS/Register.jsp
Online C Compiler -...
A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing
Home
Login
Register
User Registration Page
Register
registration

Username: victor
Password: ******
Email: victor@gmail.com
Contact No: 2136540987
Address: Chennai

Graph:



7. CONCLUSION

✓ DC Store is a number of information Virtualized file system that targets the consistency of cloud servers in this project. Through client-side data duplication, interior encoding, and a package share management strategy, DC Store not only delivers store high availability, but also cost reductions. When compared to conventional Virtualized storage systems, our small suggested model of DC Store reveals that DC Store dramatically improves quality and cost effectiveness.

8. References

[1] Core Java Volume I, author – Cay S. Horstmann.

[2] Learning SQL is a book written by Alan Beaulieu. Each chapter of this book teaches you a
[3] key SQL concept or technique, with various illustrations and annotated examples. Exercises at
[4] the end of each chapter allow you to practice the skills you learn.

[5] [3] Android Programming with Kotlin for Beginners by John Horton.

[6] [4] Object Oriented Modeling and Design using UML - The University of Mumbai.

[7] [5] A Craftsman's Guide to Software Structure and Design - Robert C. Martin.

[8] [6] Cloud Computing from Beginning to End by, Ray J Rafaels.