NEW HORIZON
COLLEGE OF ENGINEERING

Project Phase 2
Academic Year (2022-23)
Authentication key generator for data sharing on the cloud.
13/05/2023

Team Members

- **1NH19CS047 – Esikala Nithish Mani Krishna**
- **1NH19CS053 – Gangireddy Ramyasri**
- **1NH19CS056 – Gundre sai sruthi**

Guided By
Dr. Santhosh Krishna B V
Associate Professor
Dept. of CSE, NHCE

TABLE OF CONTENTS

ABSTRACT

- With the help of a sizable quantity of virtual storage, cloud computing provides services through the Internet on demand. The primary benefit of cloud computing is that it relieves users of the need to invest in pricey computer equipment. Lower expenses are related with infrastructure. Researchers are looking at new, relevant technologies as a result of recent breakthroughs in cloud computing and other sectors. Due to its accessibility and scalability for computer operations, both private users and companies upload their software, data, and services into the cloud storage.
- Online data interchange for increased productivity and efficiency is one of today's most significant requirements. Owners of this data can keep and distribute the info online. This study aims to provide a secure key for online data sharing for users that includes cloud computing technologies and crypto algorithm principles. Data owners would ideally like to keep their data/files online in an encrypted way, delegate decryption rights for some of these to users, and maintain the ability to withdraw access at any moment.

INTRODUCTION

- Online data sharing for increased productivity and efficiency is one of the primary requirements today for any organization. However, protecting online data is critical to the success of the cloud, which leads to the requirement of efficient and secure cryptographic schemes for the same.
- Data owners would ideally want to store their data/files online in an encrypted manner, and delegate decryption rights for some of these to users, while retaining the power to revoke access at any point of time.
- An efficient solution in this regard would be one that allows users to decrypt multiple classes of data using a single key of constant size that can be efficiently broadcast to multiple users.
- This project proposes to build a Secure key for online data sharing for the users which incorporates technology of cloud computing, crypto algorithm concepts.

Problem Statement

This project proposes to build a Secure key for online data sharing for the users which incorporates technology of cloud computing, crypto algorithm concepts.

OBJECTIVES

The objective of this project is to develop a secure and efficient system that can prevent unauthorized access to sensitive data stored in the cloud. The project aims to use the cloud computing technology to enhance the performance, scalability and availability of the system, while ensuring the confidentiality and integrity of the data through the use of KAC algorithm.

Literature Survey

Sl. No	Title of the Journal	Authors	Summary	Drawbacks
[1]	Spice–simple privacy preserving identity management for cloud environment	Sherman SM Chow, Yi Jun He	This paper introduces SPICE, the first digital identity management system that may meet these requirements as well as other desirable qualities	Authentication mechanisms
[2]	Privacy preserving public auditing for secure cloud storage	Cong Wang, Sherman S.-M. Chow	paper generalise the findings such that the TPA may audit numerous users concurrently and efficiently.	Lack of efficient encryption method.

Literature Survey

Sl. No	Title of the Journal	Authors	Summary	Drawbacks
[3]	Dynamic secure cloud storage with provenance	Sherman SM Chow, Cheng Kang Chu	The topic of developing a secure cloud storage system that supports dynamic users and data provenance is addressed in this study.	Security gurantee during the encryption
[4]	Key aggregate cryptosystem for scalable data sharing in cloud storage	Cheng-Kang Chu, Sherman SM Chow	In this article, we demonstrate how to safely, efficiently, and flexibly exchange data in cloud storage with others.	Generation of key through mail.

Literature Survey

Sl. No	Title of the Journal	Authors	Summary	Drawbacks
[5]	Collusion resistant broadcast encryption with short ciphertexts and private keys	Dan Boneh, Craig Gentry	In this report they discussed about the key broadcast encryption systems.	Efficient algorithms discussion

Inference Of Literature

After reviewing 20 base papers and main 5 base papers which are related to the project that there are some drawbacks in base papers.

The main drawbacks such as

- Authentication mechanisms
- Lack of efficient encryption method.
- Security gurantee during the encryption
- Generation of key through mail.

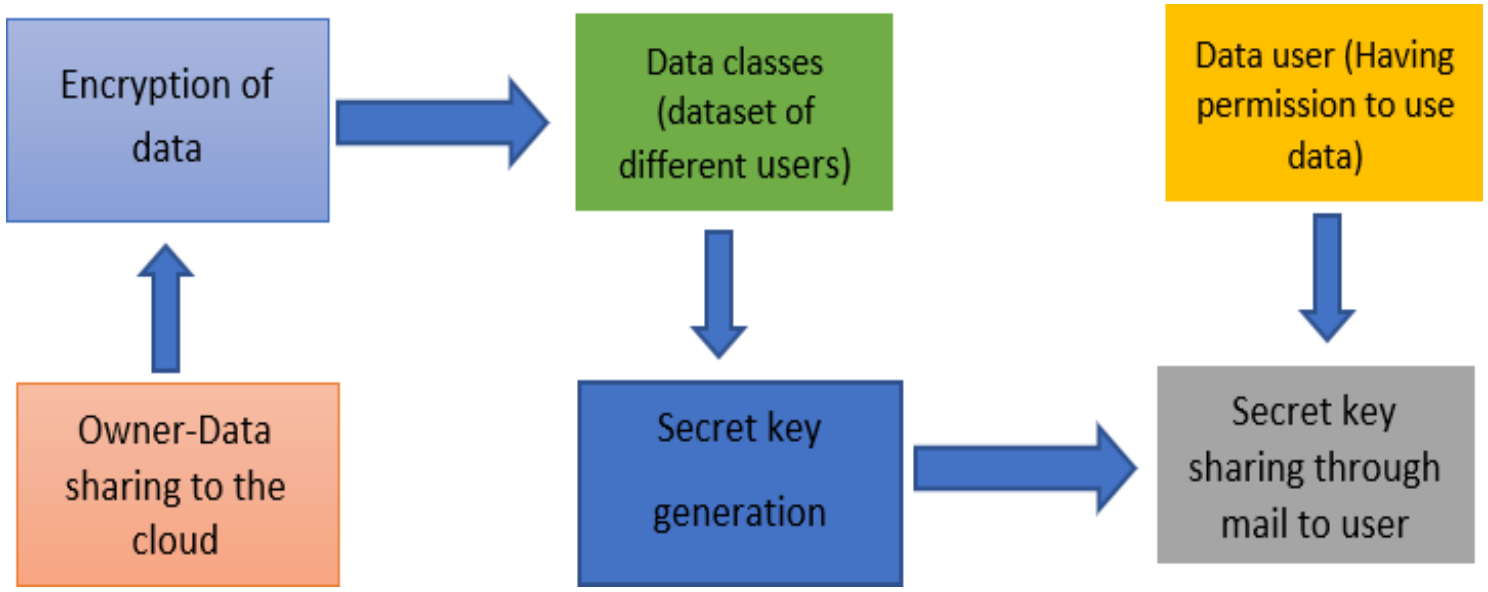
These are the main drawbacks of the previous project which we been reviewed.

Proposed system

The newly proposed ideas in the project are

- Sharing of the files to users by generating aggregate key through mail.
- Multiple key generation.
- Encryption of data while owner uploading the file in to the cloud and decryption of data when user download the file.
- For key generations we are using the cryptosystems algorithms to be more secure for data and this will be more efficient.

Sequence Diagram



EXPLAINATION

Data Owner

- Registration
- Data owner can login only using secrete key sent by cloud.
- Data owner upload their files with cloud in an encrypted format.

Data user

- Registration
- Data user can search uploaded files by using file key.
- Data user also can login only using secrete key sent by the cloud.
- User can download requested files from cloud by using third party generated private and aggregate key.

Cloud

- Cloud can view user's file request.
- It request third party to send corresponding file to the user.

TPA

- It will send private key and aggregate key to user's email.
- we can show all file details.

ALGORITHM

- For this project we are using the Key Aggregate Cryptosystem Algorithm for generating the security while sharing the data.
- We will generate the aggregate key for the people who are accessing the file.
- when the user request for the file cloud will generate the aggregate key.
- When we request the cloud view the user's request and cloud request the third party to send the corresponding file to the user.
- Then third party will send the key to the user's through the mail.

Encryption

Let m be a file to be encrypted
Compute ciphertext as: c

Decryption

Let c be the ciphertext to be decrypted
Compute the plaintext message as : m

Encryption algorithm is used by the owner to upload the encrypted file to the cloud
Decrypted algorithm is used by the user to fetch the required information from desired file which is stored in the cloud.

Requirements

HARDWARE REQUIREMENTS

Processor	: 3.00GHz
RAM	: 8GB
Hard Disk	: 1TB
Input device	: Standard Keyboard and Mouse
Output device	: VGA and High Resolution Monitor

SOFTWARE REQUIREMENTS

Operating system	: Windows XP
IDE	: Netbeans
Data Base	: MYSQL
Code	: Java

Advantages

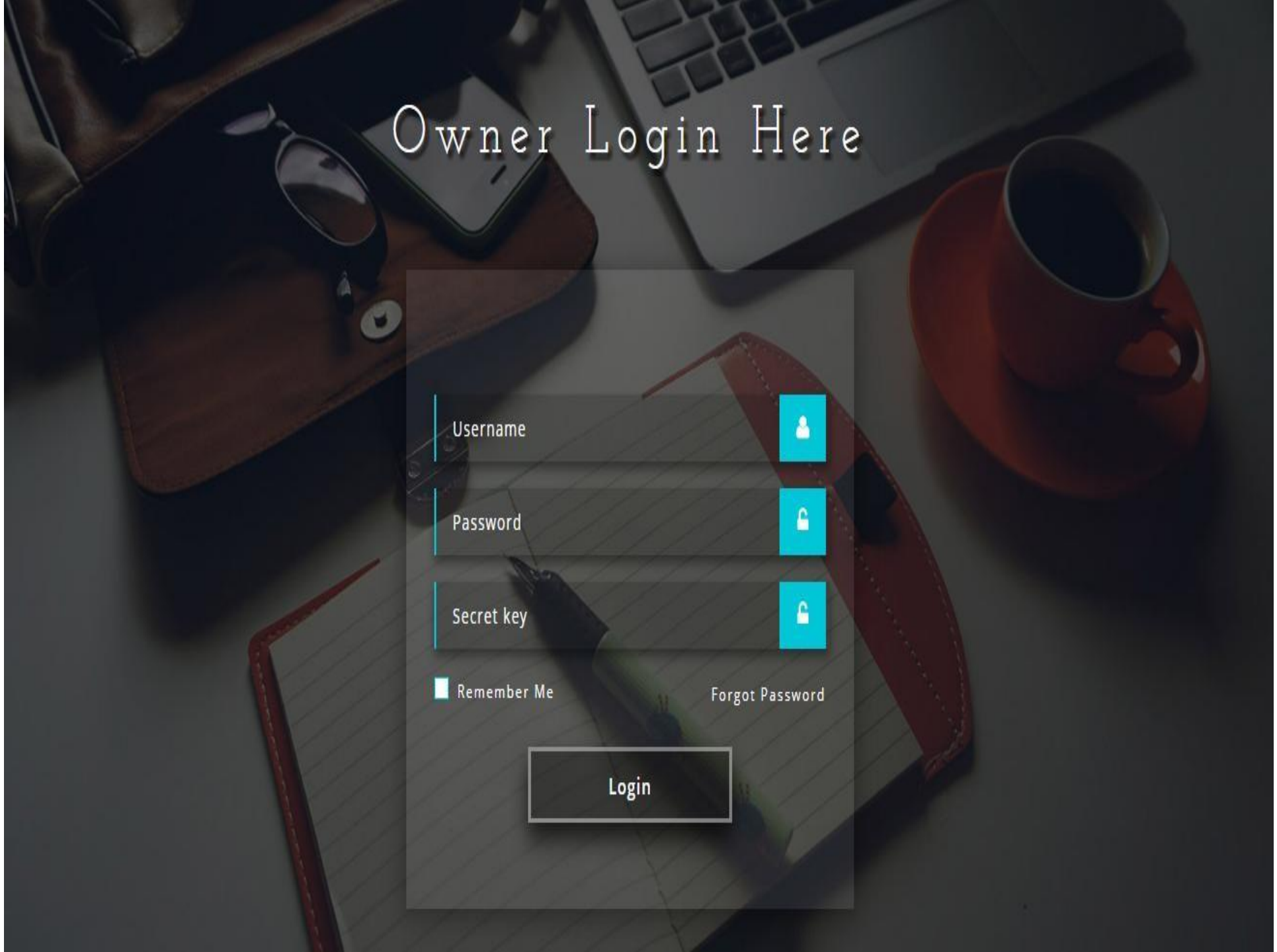
- In this project we can avoid the security issues which we are facing while sharing the files on cloud.
- Improves the economy of the company and reduce the storage and security issues.
- Generation of key generator.

Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud

Search...

Home | Data owner | Data user | TPA | cloud | Registration


User Login Here
LOGIN
MAKE YOURSELF AT HOME
Before proceeding, please ensure that any pop up blocking software is disabled, click here for tips.
EE Helpdesk Tel: 07973 100 292 - option 5
Username
Password
Username
Please fill out this field.
NEW USER?
FORGOT ?
Password
Secret Key
Remember Me
Forgot Password
Login


Owner Login Here
Username
Password
Secret key
Remember Me
Forgot Password
Login

CONCLUSION

- Cloud computing include rapid system implementation, low costs, abundant storage, and simple system access from anywhere at any time As a result, cloud computing is becoming more and more apparent in recent technical developments and a widely utilised computer environment everywhere. Several security and privacy issues make it difficult to use cloud computing.
- The security weaknesses, dangers, and assaults that the cloud already has should be known to all users. If businesses are aware of security threats and attacks, they can adopt the cloud more swiftly.. Utilizing both traditional and cutting-edge techniques and technology, cloud computing. Multiple clouds can be produced using this innovative technique.
- To reduce this security issue in this project we have implement KAC algorithm and we have generating the secret keys ,private keys and all to upload and download the file.

References

1 IDC Enterprise Panel. “It cloud services user survey, What users want from cloud services providers”, august 2008.

2 M. O'Neill, “NIST: The NIST Definition of Cloud Computing” Accessed 2013 September.

3 “Amazon: Amazon Web Services: Overview of Security Processes”, Accessed 2015 November.

4P. Syam Kumar and R. Subramanian, “ An efficient and secure protocol for ensuring data storage security in Cloud Computing”,2011, IJCSI Int. J. Comput. Sci. Issues 8 6, 8.

5B. V. Santhosh Krishna, S. Sharma, K. Devika, Y. Sahana, K. N. Sharanya and C. Indraja, "Review of Fake Product Review Detection Techniques," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 771-776, doi: 10.1109/ICAIS53314.2022.9742735.

6S. Bangari, P. Rachana, N. Gupta, P. S. Sudi and K. K. Baniya, "A Survey on Disease Detection of a potato Leaf Using CNN," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 144-149, doi: 10.1109/ICAIS53314.2022.9742963.

7M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, “ Security and privacy in cloud computing: A survey. In: Semantics Knowledge and Grid ”, 2010 Proceedings of the Sixth International Conference on Nov 1 pp. 105–112. IEEE.

8S. Subashini and V. Kavitha, “ A survey on security issues in service delivery models of cloud computing” J. Netw. Comput. Appl. 34 1, 1–11,2011.

9 B.Meenakshi Sundaram; B Rajalakshmi; Babu Aman Singh; Rachit S Kumar; Rohith Arsha, Disaster Relief Compensation Computational Framework, 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), DOI: 10.1109/ICAIS53314.2022.9742829

THANK YOU