International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-409 PAGE NO: 2781-2785

DEVELOP DUPLICATION SYSTEM DATA IN CLOUD

Kalimuthu G[#1], Mrs. K. Renuka[*2]

[#]*Student, M.Sc Computer Science,*
Rathinam College of Arts and Science, Coimbatore,
Tamil Nadu, India -641021 *hamseabdiali.mit20@rathinam.in*

[*]*Head of the Department, Department of Computer Science,*
Rathinam College of Arts and Science, Coimbatore,
Tamil Nadu, India -641021. *hod.csc@rathinam.in*

Abstract - **Meanwhile, cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay- per-use manner. Access control is paramount as it is the first line of defense that prevents unauthorized access to the shared data. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying cipher text-policy, making the computation over encrypted data a very hard problem. The proposed scheme not only achieves scalability due to its hierarchical structure.**

Index Terms – **Cloud Computing, Bandwidth, Sensitive Data, Cipher Text Policy.**

I. INTRODUCTION

In cloud computing, authority accepts the user enrollment and creates some parameters. Cloud service provider (CSP) is the manager of cloud servers and provides multiple services for client. Data owner encrypts and uploads the generated cipher text to CSP. User downloads and decrypts the interested cipher text from CSP. The shared files usually have hierarchical structure. That is, departments of files are divided into a number of hierarchy sub departments located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of cipher text and time cost of encryption could be saved. Presently a day's more number of plans utilized encryption for control the information in Cloud. It empowers clients with restricted computational assets to outsource their expansive calculation workloads to the cloud, and monetarily appreciate the monstrous computational power, data transfer capacity, stockpiling, and even proper programming that can be partaken in a compensation for each utilization way.

We provide the privacy secure in public social cloud computing. In our project we implement hierarchical attribute base security the hierarchy are Cloud authority, Domain authority and users. Cloud authority can only have privilege to create or remove the domain (private cloud authority) in cloud and they can maintain all the details in overall cloud Domain authority can create or remove the users inside the domain this users are called private users. Users are two types private cloud user and public cloud users Private cloud users are depending the domain Public users under cloud authority. Users can upload the files in two ways: Public and Private.

II. SOFTWARE DESCRIPTION

FRONT END

ASP.NET

The system is developed using Visual Basic. NET, which is a very popular Microsoft Product developed by Microsoft Corporation. This is one of the improved languages from basic language. Visual basic. NET includes a variety of open active controls for user interfaces to design application formASP.NET is the multiple documents inter face format (MDI). The user interface is the part of the program that responds to the key press and mouse clicks. The action is referred to as events of the form and controls in the form. ASP.NET provides vast properties and methods for each control, which helps to utilize all those, functions for record manipulations. Menu driven is one of the most effective controls in the ASP.NET. In this menu driven the menu names in a program appear in the menu bar when the user selects a menu, that menu open. Each menu usually contains items arranged in a vertical list. These items are often grouped into functional groups with menu parameters. When the user selects a menu item, that item appears highlighted; pressing enter or releasing the mouse button opens that item. Each item should have a unique access character for users to choose commands with keyboards. The user reaches the menu or menu item by pressing alt key and access character. Short cuts are also useful to the user these keys are faster than access character in that the user only needs to enter a shortcut to execute the corresponding menu item.

1) **BACK END**
2) **SQL SERVER 2005**

Microsoft SQL Server 2005 is a full-featured relational database management system (RDBMS) that offers a variety of administrative tools to ease the burdens of database development, maintenance and administration.

Enterprise Manager is the main administrative console for SQL Server installations. It provides you with a graphical "birds-eye" view of all of the SQL Server installations on our network.

Query Analyzer offers a quick and dirty method for performing queries against any of our SQL Server databases. It is a great way to quickly pull information out of a database in response to a user request, test queries before implementing them in other applications, create/modify stored procedures and execute administrative tasks.

SQL Profiler provides a window into the inner workings of your database. SQL Profiler allows you to capture and replay system "traces" that log various activities. It is a great tool for optimizing databases with performance issues or troubleshooting particular problems.

Service Manager is used to control the MS SQL Server (the main SQL Server process), MSDTC (Microsoft Distributed Transaction Coordinator) and SQL Server Agent processes. An icon for this service normally resides in the system tray of machines running SQL Server.

III. SYSTEM STUDY

EXISTING SYSTEM:

Existing system can't secure computation outsourcing data. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing. Ordinary data encryption techniques can't secure cloud underlying plaintext data. Making the computation over encrypted data a very hard problem. Complex of access control policies. Cipher-texts are not encrypted to one particular user as in traditional public key cryptography. Assigning multiple valuesto the same attribute.

DRAWBACKS OF EXISTING SYSTEM:

The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. The hierarchy structure of shared files hasn't been explored in CP-ABE. Using Cipher text- policy attribute-based encryption to secure the cloud storage part. The authority for file access control in which authorized of all operations on cloud data can bemanaged in the entire manner. To avoid unauthorized information leakage, sensitive data have to be encrypted before outsourcing. Role based encryption is used for encrypting the data based on the authority provided.

THE PROPOSED SYSTEM:

We offer the security of social cloud computing. In this paper we put into practice hierarchical security, Cloud authority, Domain authority and users. Cloud authority can only have a privilege to create or remove the province in cloud and they can preserve all the details in overall cloud Domain authority can create or eliminate the users contained by the domain this users are called private users.

ADVANTAGE OF THE PROPOSED SYSTEM

Two type users will be there. One is private cloud user and another one is public cloud users. Private users are relying on the domain, Public users under cloud authority. User has a two way of uploading files Public and Private. If one file uploaded by private user, file visibility and convenience having only within domain without confirmation. If some file should uploaded by public user's then, file access privileges having all the users If file uploading the private user means file visibility is only within field but file accessibility is who have the secrete key (OTP) means who have license to access the file If the public user upload the private file means that file visibility is public anyone can noticeable the file but who have a privilege like one time password to access they only can file.

IV. SYSTEM DEVELOPMENT

DESCRIPTION OF MODULES:

This project has five main modules to demonstrate the entire process by using the following modules:

1. Cloud Service Provider
2. Data Users Module
3. Private Cloud Module
4. Secure Deduplication System

Modules Description:

Cloud Service Provider

In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud. The S-CSP provides the data outsourcing service and stores data on behalf of the user. To reduce the storage cost, the S-CSP eliminates the storage of redundant data via deduplication and keeps only unique data. In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.

Data Users Module

A user is an entity that wants to outsource data storage to the S-CSP and access the data later. In a storage system supporting deduplication, the user only uploads unique data but does not upload any duplicate data to save the upload bandwidth, which may be owned by the same user or different users. In the authorized deduplication system, each user is issued a set of privileges in the setup of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized deduplication with differential privileges.

Private Cloud Module

Compared with the traditional deduplication architecture in cloud computing, this is a new entity introduced for facilitating users secure usage of cloud service. Specifically, since the computing resources at data user/owner side are restricted and the public cloud is not fully trusted in practice, private cloud is able to provide data user/owner with an execution environment and infrastructure working as an interface between user and the public cloud. The private keys for the privileges are managed by the private cloud, who answers the file token requests from the users. The interface offered by the private cloud allows user to submit files and queries to be securely stored and computed respectively.

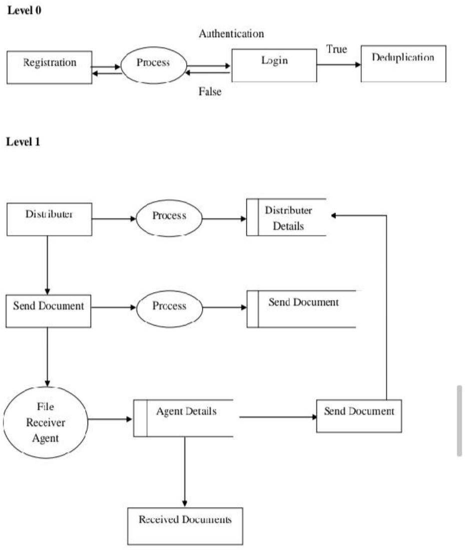
Secure Deduplication System

We consider several types of privacy we need protect, that is, i) enforceability of duplicate-checktoken: There are two types of adversaries, that is, external adversary and internal adversary. As shown below, the external adversary can be viewed as an internal adversary without any privilege.

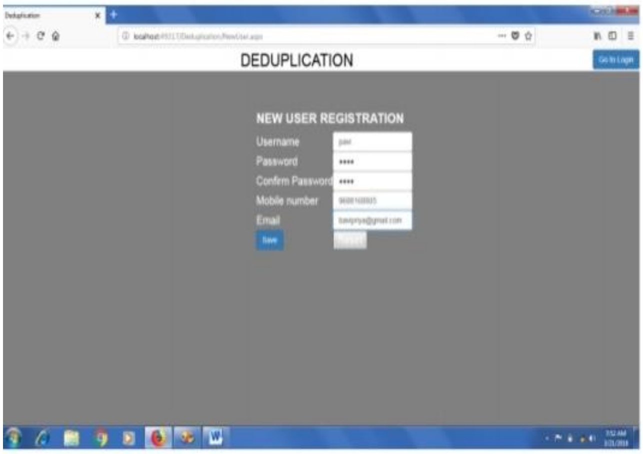
Data Flow Diagram:

IJCS International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SK Research Group of Companies SKRGC Since 2012

http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-409 PAGE NO: 2781-2785



V. OUTPUT SCREENS

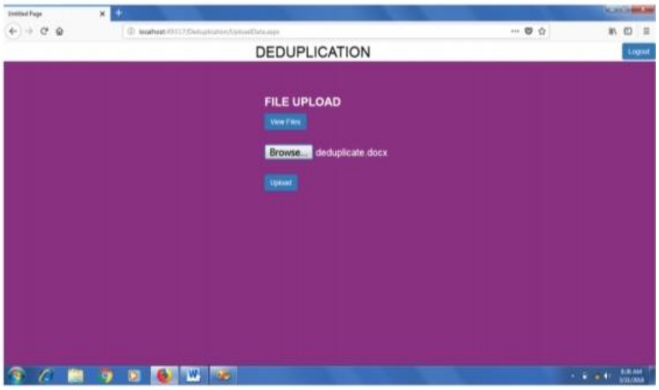


DEDUPLICATION

NEW USER REGISTRATION

Username: pavi
Password: ••••
Confirm Password: ••••
Mobile number: 9698168805
Email: bavipriya@gmail.com

FILE UPLOAD

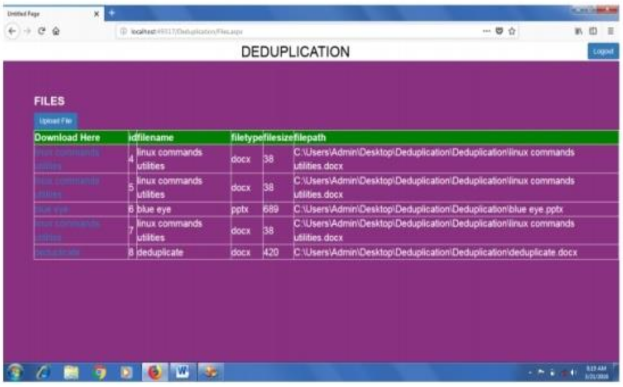


DEDUPLICATION

FILE UPLOAD

deduplicate.docx

VIEW FILES

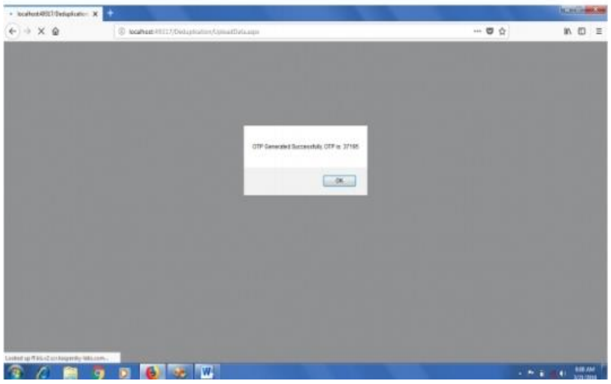


DEDUPLICATION

FILES

Download Here	id	filename	filetype	filesize	filepath
linux commands utilities	4	linux commands utilibes	docx	38	C:\Users\Admin\Desktop\Deduplication\Deduplication\linux commands utilities.docx
linux commands utilities	5	linux commands utilibes	docx	38	C:\Users\Admin\Desktop\Deduplication\Deduplication\linux commands utilities.docx
blue eye	6	blue eye	pptx	689	C:\Users\Admin\Desktop\Deduplication\Deduplication\blue eye.pptx
linux commands utilities	7	linux commands utilibes	docx	38	C:\Users\Admin\Desktop\Deduplication\Deduplication\linux commands utilities.docx
deduplicate	8	deduplicate	docx	420	C:\Users\Admin\Desktop\Deduplication\Deduplication\deduplicate.docx

OTP GENERATION



OTP Generated Successfully OTP is: 37195

VI. CONCLUSION

A semi-anonymous attribute-based privilege control scheme Annoy Control and a fully anonymous attribute-based privilege control scheme Annoy Control-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users‟ identity information. More importantly, our system can tolerate up to N − 2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment.

Future Work:

Deduplication of files are done for each user bucket. Future enhancement would be to achieve deduplication on the complete cloud storage. Currently, improved technique for storage has been tested only for text files. In future, it can be further extended to support files of other types. Design of an improved technique for storage in Cloud is deduplication technique. Deduplication aids in saving the storage space. This application helps in easy maintenance of data on the cloud platform so that no duplicate files are saved in the Cloud. With the evolution of Cloud computing, storage resources of commodity machines can be efficiently utilized.

REFERENCES:

[1] Lohstroh M, Kim H, Eidson JC et al (2019) On enabling Technologies for the Internet of important things. IEEE Access 7:27244–27256. https://doi.org/10.1109/ACCESS.2019.2901509

[2] Abbas N, Zhang Y, Taherkordi A, Skeie T (2018) Mobile edge computing: a survey. IEEE Internet Things J 5:450–465. https://doi.org/10.1109/JIOT.2017.2750180

[3] Ren J, Zhang D, He S et al (2019) A survey on end-edge-cloud orchestrated network computing paradigms: transparent computing, mobile edge computing, fog computing, and cloudlet. ACM Comput Surv:52. https://doi.org/10.1145/3362031

[4] Zhang P, Liu JK, Richard Yu F et al (2018) A survey on access control in fog computing. IEEE Commun Mag 56:144–149. https://doi.org/10.1109/MCOM.2018.1700333

[5] Menon VG, Jacob S, Joseph S, Almagrabi AO (2019) SDN powered humanoid with edge computing for assisting paralyzed patients. IEEE Internet Things J:1. https://doi.org/10.1109/jiot.2019.2963288

[6] Menon VG, Prathap J (2017) Vehicular fog computing. Int J Veh Telemat Infotain Syst 1:15–23. https://doi.org/10.4018/ijvtis.2017070102

[7] Liu J, Zhang Q (2018) Offloading schemes in Mobile edge computing for ultra-reliable low latency communications. IEEE Access 6:12825–12837. https://doi.org/10.1109/ACCESS.2018.2800032

[8] Li S, Zhang N, Lin S et al (2018) Joint admission control and resource allocation in edge computing for internet of things. IEEE Netw 32:72–79. https://doi.org/10.1109/MNET.2018.1700163

[9] Nadesh RK, Aramudhan M (2018) TRAM-based VM handover with dynamic scheduling for improved QoS of cloud environment. Int J Internet Technol Secur Trans:8. https://doi.org/10.1504/IJITST.2018.093340

[10] Ning Z, Kong X, Xia F et al (2019) Green and sustainable cloud of things: enabling collaborative edge computing. IEEE Commun Mag 57:72–78. https://doi.org/10.1109/MCOM.2018.1700895

[11] Rajesh S, Paul V, Menon VG, Khosravi MR (2019) A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices, pp 1–21

[12] Zhang J, Chen B, Zhao Y et al (2018) Data security and privacy-preserving in edge computing paradigm: survey and open issues. IEEE Access 6:18209–18237. https://doi.org/10.1109/ACCESS.2018.2820162

[13] Nadesh RK, Srinivasa Perumal R, Shynu PG, Sharma G (2018) Enhancing security for end users in cloud computing environment using hybrid encryption technique. Int J Eng Technol 7

[14] Abbasi M, Rafiee M, Khosravi MR et al (2020) An efficient parallel genetic algorithm solution for vehicle routing problem in cloud implementation of the intelligent transportation systems. J Cloud Comput 9.

https://doi.org/10.1186/s13677-020-0157-4

[15] Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42. https://doi.org/10.1016/j.compeleceng.2018.06.006

[16] Jiang S, Jiang T, Wang L (2017) Secure and efficient cloud data Deduplication with ownership management. IEEE Trans Serv Comput 12:532–543. https://doi.org/10.1109/TSC.2017.2771280

[17] Yoon MK (2019) A constant-time chunking algorithm for packet-level deduplication. ICT Express 5:131–135. https://doi.org/10.1016/j.icte.2018.05.005

[18] Wang L, Wang B, Song W et al (2019) Offline privacy preserving proxy re-encryption in mobile cloud computing. Inf Sci (Ny) 71:38–43. https://doi.org/10.1016/j.jksuci.2019.05.007

[19] Wang L, Wang B, Song W, Zhang Z (2019) A key-sharing based secure deduplication scheme in cloud storage. Inf Sci (Ny) 504:48–60.