International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Sharing Files on Cloud Storage Using a Group Key Management Protocol

Kandra Keerthi[1], Mr. A. Murali Mohan Kumar[2]
Master of Computer Applications[1], Associate Professor[2]
Department of MCA[1&2]
Mother Theresa Institute of Computer Applications, Palamaner, Tirupati, India

Article Info

Publication Issue :
Volume 8, Issue 5
September-October-2022

Page Number : 261-266

Article History
Accepted: 10 Oct 2022
Published: 25 Oct 2022

ABSTRACT

Due to the extensive sharing requirements of many enterprises, cloud storage is becoming more and more popular. As cloud computing maintains shared information beyond the trust zone of the owner, expectations and concerns for file security are developing. For cloud file sharing, a Group Key Management Protocol is suggested in this work. In response to network risks via public channel, a hybrid encryption technology-based group key generation technique is given. Additionally, a verification system is used to protect shared files from attacks by group members and cloud providers. Security and performance assessments show that the proposed protocol is effective and safe for data exchange in cloud computing.

Keywords: Advanced Encryption Standards, data storage, Security, Encryption and decryption.

I. INTRODUCTION

Because of the cutting-edge expansion of cloud technologies in use today, rebuilding services in the cloud has become increasingly widespread. Data from numerous clients can be stored on a single physical system, which can be hosted on various virtual machines, in a shared-tenancy cloud computing environment. Under this paradigm, data owners are left defence less and are forced to rely solely on the cloud provider to protect their data because the cloud provider has total control over data storage and administration. Recent allegations claim that Google provided the FBI with all of one user's records after acquiring a search order, but the individual was not made aware of the search until they were detained. Because the cloud provider has complete access to the data, data privacy could be jeopardized if the cloud provider intercepts or modifies the user's data. Encrypting and authenticating shared data is a popular method for ensuring privacy. There are a number of cryptographic systems that allow a third-party auditor to validate file availability while no information about the file is revealed. Similarly, cloud users are unlikely to have a strong conviction in the cloud server's confidentiality. Before uploading their files to the cloud server, cloud users are encouraged to encrypt them using their own keys. The final challenge is to distribute and manage cryptographic keys among valid users without contacting the cloud provider.

II. RELATED WORKS

CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing: With the popularity of cloud storage growing, more people are outsourcing data to cloud servers. On the one hand, there is a substantial degree of data duplication present with the rapidly expanding cloud data volume. However, with a deduplication cloud storage solution, the cloud server only keeps one copy of the outsourced data, and if that copy is lost or corrupted, there will be irreparable loss. File deduplication and integrity auditing are crucial because of this, and the issue of how to accomplish both securely and effectively in academia and industry must be promptly resolved. We present a deduplication cloud storage with public cloud auditing that preserves secrecy (CPDA). To begin with, our CPDA scheme achieves safe file deduplication on encrypted files, allowing public integrity auditing of the unique copy in the deduplication cloud storage system. Secure authentication tag deduplication is also possible with our CPDA technique. Secondly, our CPDA system uses convergent encryption and random masking techniques to preserve data privacy during the file deduplication and integrity auditing process. Third, our method enables the cloud server to routinely assign various auditing jobs to a third-party auditor, thereby maintaining the integrity of outsourced files, in addition to enabling each data owner to independently initiate integrity audits of their own files. Finally, numerical analyses and simulation experiments show how effective and secure our approach is..

Audit-Free Cloud Storage via Deniable Attribute-Based Encryption: The use of cloud storage is becoming more common. Many cloud storage encryption strategies have been proposed to safeguard data from individuals who do not have access because of the importance of privacy. In actuality, some authorities (i.e., coercers) may force cloud storage providers to expose user secrets or confidential data on the cloud, thereby completely evading storage encryption techniques. We propose our proposal for a new cloud storage encryption system in this work, which allows cloud storage providers to generate convincing false user secrets to safeguard user privacy. Because coercers have no way of knowing if secrets collected are accurate or not, cloud storage providers ensure that user privacy is maintained.

Securing Outsourced Data in the Multi-Authority Cloud with Fine-Grained Access Control and Efficient Attribute Revocation: Data outsourcing is a potential service that would keep data owners' data on a cloud storage provider. Since the cloud cannot be completely trusted, data access control has become a challenging problem in the cloud storage system (CSS). With an attribute authority in charge of managing attributes and dispersing keys, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a workable approach for ensuring access control in the CSS. In this work, we introduce a new Multi-Authority CP-ABE scheme that allows the access policy to be written as any kind of tree, as opposed to the matrix used by other approaches. The policy's tree-like structure makes our strategy more flexible. As a result, activities such as encryption, decryption, and attribute revocation are faster. Under the conventional assumption, our method is also proven to be secure. It can withstand a user collusion attack, and attribute revocation ensures both forward and backward security. Our system is highly efficient, based on simulation results.

Comments on "Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing": putting into practise a novel attribute-based encryption (ABE) architecture that enables a verifiable outsourcing of the challenging encryption process to an encryption service provider

(ESP). We demonstrate that, despite the authors' promises that users can inspect the outputs of outsourced encryption, the Ma et al proposal fails to provide the verifiability property for outsourced encryption, which is the most crucial security goal that a verifiable computing method should accomplish. We show that the ESP can return forged intermediate encrypted text to the user without being noticed by demonstrating realistic attacks.

III. Methodology

In proposed scheme, The verification system protects shared data against cloud providers and group members colluding to attack them. The suggested protocol is secure and efficient for data exchange in cloud computing, according to security and performance evaluations. A group key generation strategy based on hybrid encryption technology is presented in response to network threats via public channel.

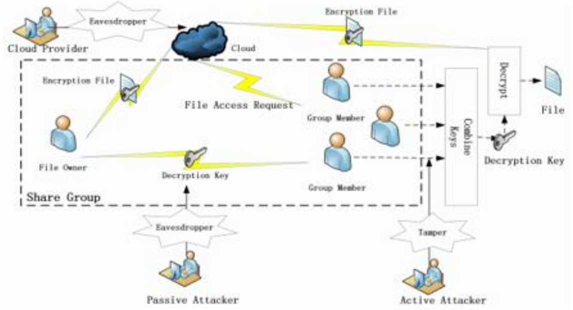


Figure 1: Block diagram of proposed method

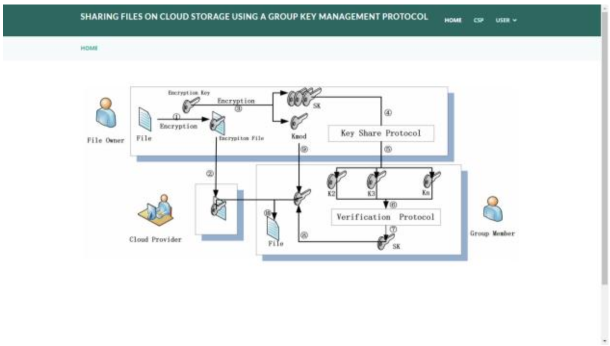
IV. Implementation

Group Key Management Protocol is used to protect the data from attackers known as Cloud Server Providers and group members as part of this project's implementation. Installing necessary software packages is necessary before we can start the process. Additionally, we must specify the issue's resolution, develop and the user interface, and then execute the user, admin, and Cloud Server Providers modules that are listed in the Results and Discussion section below, which also includes screenshots.

V. Results and Discussion

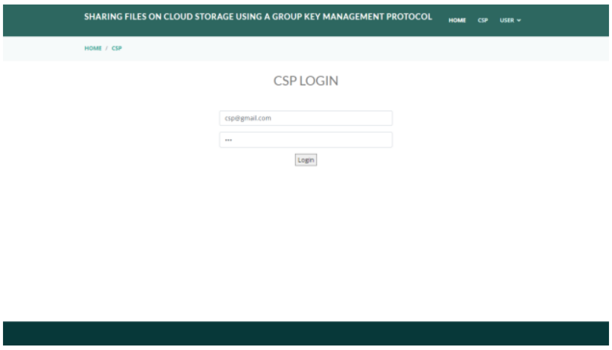
The following images will visually depict the process of our project.

Home page: In this home page we can see the logo designing of our website.



Start: This page is like a starting step to continue the process of project.

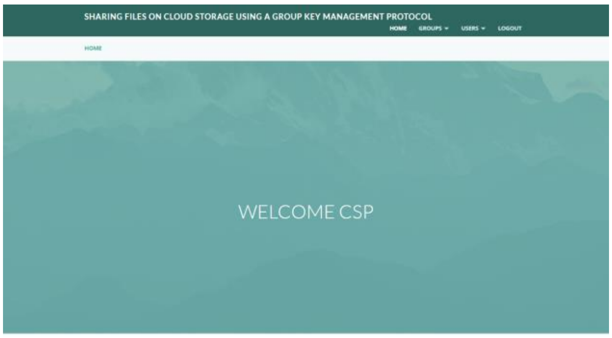
Csp login page: Login with the valid credentials only.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
CSP
USER
HOME / CSP
CSP LOGIN
Login

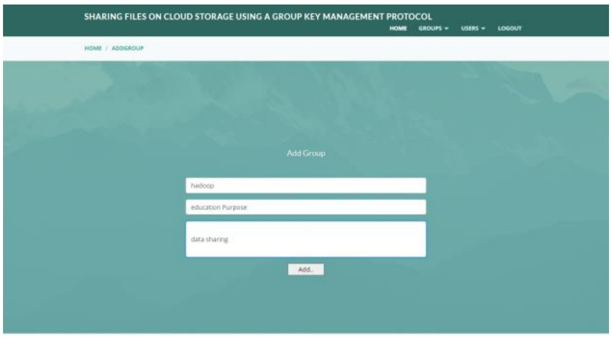
csp@gmail.com

...

Csp home page: After successful login the CSP can get the home page.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
USERS
LOGOUT
HOME
WELCOME CSP

Csp add group page: Csp can create groups.

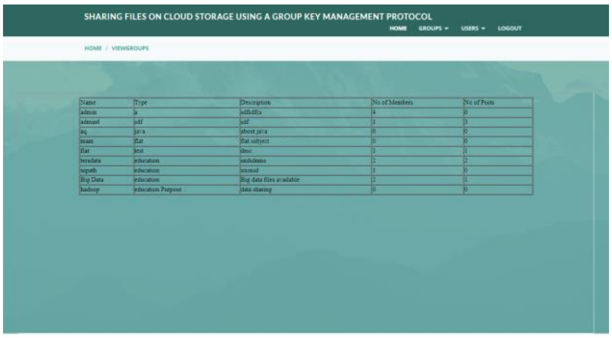

SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
USERS
LOGOUT
HOME / ADDGROUP
Add Group
Add..

hadoop

education Purpose

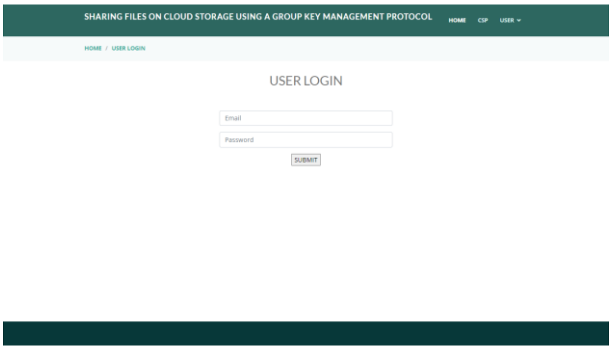
data sharing

View groups page: Csp can view all groups then join in particular group if he is interested view his own groups.

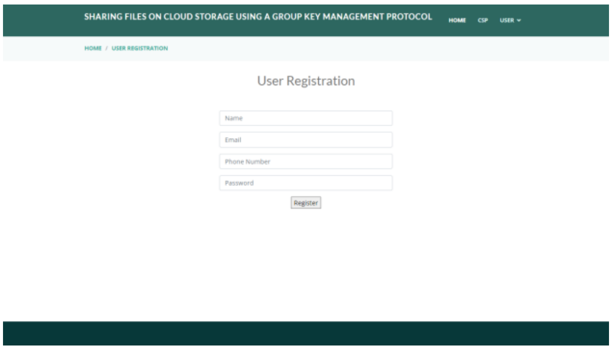

SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
USERS
LOGOUT
HOME / VIEWGROUPS

Name	Type	Description	No of Members	No of Posts
admin	a	sdfsdfcs	4	6
admin6	sdf	sdf	1	3
aq	java	about java	0	0
mani	flat	flat subject	0	0
flat	test	desc	1	1
teradata	education	sndsdnms	2	2
sripath	education	xxxxxd	1	0
Big Data	education	Big data files available	2	1
hadoop	education Purpose	data sharing	0	0

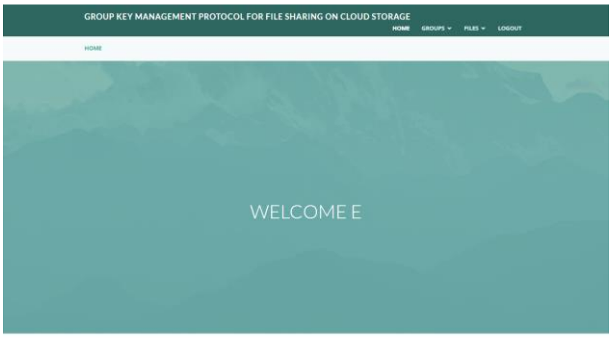
User login page: User having an account he can directly login into the system.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
CSP
USER
HOME / USER LOGIN
USER LOGIN
Email
Password
SUBMIT

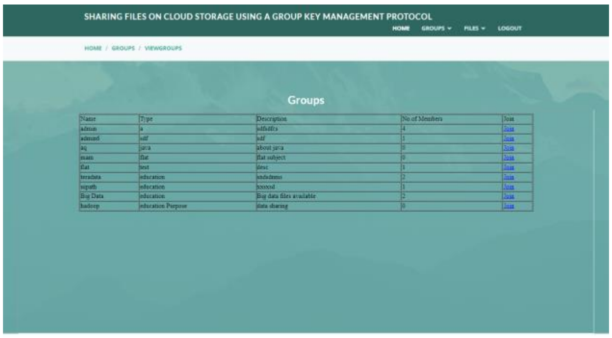
User registration page: If user don't have any account he has to register and login.



User home page: User can access this page by login.


GROUP KEY MANAGEMENT PROTOCOL FOR FILE SHARING ON CLOUD STORAGE
HOME
GROUPS
FILES
LOGOUT
HOME
WELCOME E

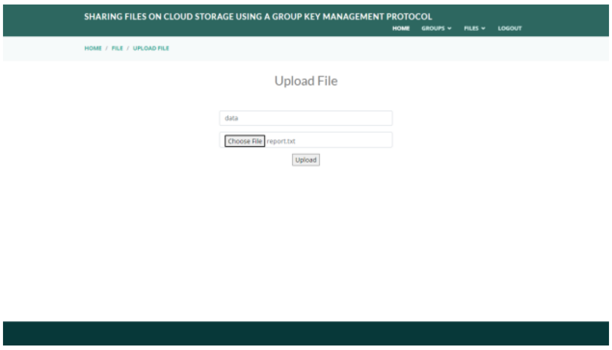
View users group page: User can view groups and join in specific groups, view all his groups and view the time line.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
FILES
LOGOUT
HOME / GROUPS / VIEWGROUPS

Groups

Name	Type	Description	No of Members	Join
admin	a	sdfsdfcs	4	Join
admin6	sdf	sdf	1	Join
aq	java	about java	0	Join
mani	flat	flat subject	0	Join
flat	test	desc	1	Join
teradata	education	sndsdnms	2	Join
sripath	education	xxxxxd	1	Join
Big Data	education	Big data files available	2	Join
hadoop	education Purpose	data sharing	0	Join

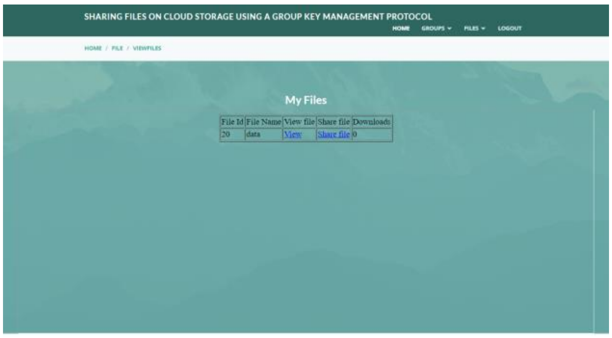
Upload files page: User can upload files.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
FILES
LOGOUT
HOME / FILE / UPLOAD FILE
Upload File
Choose File
Upload

data

report.txt

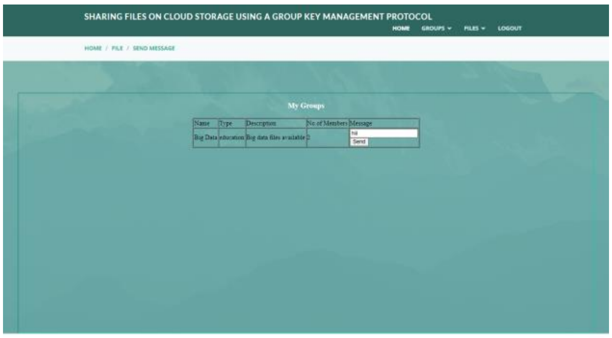
View files page: User can view those files and share files to specific groups and finally time line of groups.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
FILES
LOGOUT
HOME / FILE / VIEWFILES

My Files

File Id	File Name	View file	Share file	Downloads
20	data	View	Share file	0

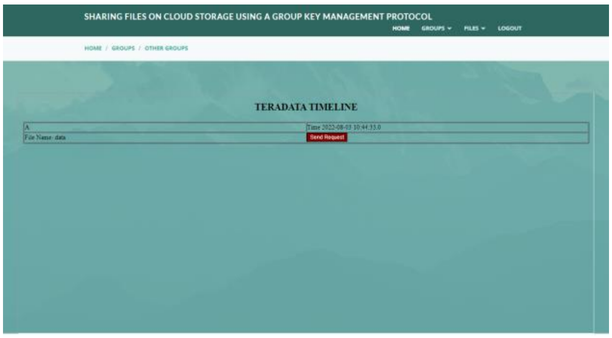
Send messages: Here the group members can send their messages.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
FILES
LOGOUT
HOME / FILE / SEND MESSAGE

My Groups

Name	Type	Description	No of Members	Message
Big Data	education	Big data files available	2	hii Send

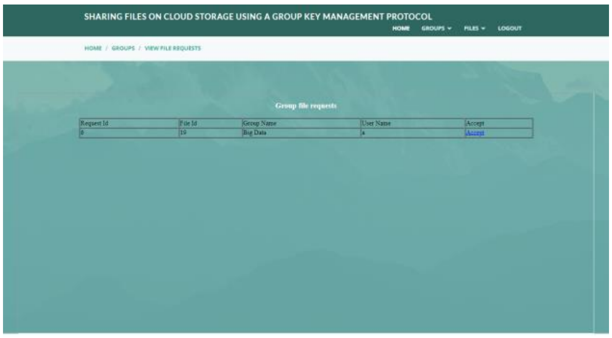
Request page: The User Sending the request for that file


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
FILES
LOGOUT
HOME / GROUPS / OTHER GROUPS

TERADATA TIMELINE

A	Time 2022-08-03 10:44:33.0
File Name: data	Send Request

User : in this page the User View the Request.


SHARING FILES ON CLOUD STORAGE USING A GROUP KEY MANAGEMENT PROTOCOL
HOME
GROUPS
FILES
LOGOUT
HOME / GROUPS / VIEW FILE REQUESTS

Group file requests

Request Id	File Id	Group Name	User Name	Accept
6	19	Big Data	a	Accept

Response : The User Downloading the file

VI. Conclusion

We developed a revolutionary group key management mechanism for cloud storage file sharing in this research. GKMP use publickey to ensure that group keys are distributed properly and that the cloud provider is immune to assault. We provide a detailed study of potential security threats and their related defences, demonstrating that GKMP is secure even under more lenient assumptions. We also show that the protocol is less complicated in terms of storage and computation.

VII. REFERENCES

[1]. CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing, IEEE Access, vol.7, pp.160482-160497, 2019. 1. J. Wu, Y. Li, T. Wang, et al.

[2]. C. Po-Wen and L. Chin, "Audit-Free Cloud Storage through Deniable AttributeBased Encryption," IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 414-427, 2018.

[3]. J. Zhou et al., "Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation", Comput. J., vol. 60, no. 8, pp. 1210-1222, Aug. 2017.

[4]. Hu, Jianfei, "Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud

Computing," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 4, pp. 461-462, August 2017.

[5]. Z. Fu X. Sun S. Ji G. Xie "Towards efficient content-aware search over encrypted outsourced data in cloud" Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM) pp. 1-9 Apr. 2016.

[6]. Y. S. Rao, "A safe and efficient ciphertext-policy attribute-based signcryption for personal health record sharing in cloud computing," Future Generation Computer Systems, vol. 67, no. 1, pp. 133-151, February 2017.

[7]. H. liu Y. huang J. K. Liu "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption" Future Gener. Comput. Syst. vol. 52 pp. 67-76 Nov. 2015.

Cite this article as :

Kandra Keerthi, Mr. A. Murali Mohan Kumar, "Sharing Files on Cloud Storage Using a Group Key Management Protocol", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 5, pp. 261-266, September-October 2022.
Journal URL : https://ijsrcseit.com/CSEIT228549