A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS MANAGEMENT ON CLOUD COMPUTING

Dr.R. Prema
AP/CSE
SCSVMV University
Kanchipuram

Byrapuneni Sai Amulya
B.E(CSE)
SCSVMV University
Kanchipuram

Amuri Homya
B.E(CSE)
SCSVMV University
Kanchipuram

ABSTRACT

In this work, we make a crucial access operation scheme that translates any access policy with a hierarchical structure to the digital media. According to the proposed plan, any google cloud system can be used as a corporate cloud. We view the data proprietor as a reality comprising numerous organizational rudiments. Each stoner of this reality has access to a secure medium from both inside and outside the company's network to pierce the Google Cloud. Our crucial access control strategy, which is grounded on the polynomial interpolation system and Shamir's secret sharing algorithm, is particularly well suited for hierarchical organizational systems. It provides a hierarchical, secure, and customizable crucial access system for businesses using charge-critical data. also, it lessens worries about releasing charge-critical data to the general public.

KEYWORDS: Interpolation, Organization, Access policy, Secret sharing, Hierarchical, Secure.

INTRODUCTION

The demand for hosting, large-scale computing, and warehousing systems will rise as more services go digital. Additionally, corporations are outsourcing these services due to advancements in networking technology and executive challenges. Drug users can access services from anywhere, at any time, thanks to a relatively new technology called cloud computing. In this project, we'll develop a fresh strategy for breaching a cloud storage system that relies on a third-party cloud architecture. With the suggested solution, Google Cloud structure can be used by associations with a high level of security. Google Cloud is a cloud computing environment that is characterized as a multi-rental environment with many other drug users. A single rental area known as Corporate Cloud is dedicated to a single tackle dealer, warehouse, and network. The communal pall is given to a particular stoner community for personal use and is owned, run, and maintained by associations within the community. Additionally, a cold-blooded pall is the result of combining two or more distinct cloud expansion models. Because the cloud storehouse in the Primis structure is controlled and owned by the provider, compliance, security, and sequestration circumstances can generally cause issues in the Google Cloud. Any stoner who pays the fee can get through the security. However, in a corporate cloud, where the client owns and operates the building, these circumstances typically don't present a problem. Although the Google Cloud Platform offers several advantages, many businesses are slowing down their total Google Cloud Reliance schemes, particularly in terms of total cost. The Google Cloud offers businesses trustworthiness, voidness, data integrity, and non-supervision compliance. As a result, Google Cloud relinquishment walls comprise audibility, business durability, data cinch-in data sequester, and vacuity. The suggested plan offers new security measures to assuage or console these businesses regarding the transfer of revenue-critical data to the Google Cloud. The key components of our plan, which is intended for data owners who want to use Google Cloud's DSaaS, are exemplified by the excellent Newton Interpolation tool. The organizational unit (OU) within an association, which is primarily one of several systematized groupings targeted at accomplishing a given performance within an association, is defined for the proposed Key Access Control Scheme. Therefore, if they receive enough favors by choosing one of the following options, drug users can access data.

1) Benefits from drug users in its group;

2) Benefits from both drug users in their group and advanced security concurring groups;

3) Only druggies of advanced security concurrence groups' security policy should be used to obtain blessings.

LITERATURE SURVEY

Cloud Computing: Concepts, Technology & Architecture

Clouds are decentralized technology platforms that make use of slice-edge technological advancements to offer extremely scalable and robust surroundings that can be used ever by businesses in a wide range of effective ways. It takes knowledge of the common inner workings, architectural layers, and models — as well as knowledge of the business and profitable counteraccusations to successfully make upon, integrate with, or indeed produce a pall terrain. Thomas Erl, one of the top-selling IT authors in the world, collaborates with pall computing experts and experimenters to break down established and mature pall calculating technologies and practices into several easily defined generalities, models, technology mechanisms, and technology infrastructures, effects from a request- and seller-independent perspective. With a focus on structure, clarity, and easily defined structure blocks for popular pall calculating platforms and operations, the book establishes practical, scholarly content in this way. The book also establishes business-centric models and criteria that enable the fiscal evaluation of pall-grounded IT coffers and their comparison to those hosted on traditional IT enterprise demesne after furnishing technology-centric content. also offered are several examinations of the SaaS, PaaS, and IaaS delivery models as well as templates and formulas for generating SLA-related quality- of- service values.

The NIST Definition of Cloud Computing

cloud computing is a model for enabling ubiquitous, accessible, on-demand network access to a shared pool of configurable computing sources(e.g., networks, storehouses, operations, and services) that can be swiftly provisioned and released with minimal operation trouble or service provider commerce. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

ISO/IEC 17789:2014 Information technology — Cloud computing — Reference architecture

ISO/IEC 17789:2014 specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities, and the cloud computing functional components and their relationships.

TTS/ISO/IEC 17788:2020, Information Technology – Cloud Computing – Overview and Vocabulary

This National Standard provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards. This National Standard applies to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage

With the rapid developments occurring in cloud computing and services, there has been a growing trend to use the cloud for large-scale data storage. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. One well-known access control model is the role-based access control (RBAC), which provides flexible controls and management by having two mappings, users to roles and roles to privileges on data objects. In this paper, we propose a role-based encryption (RBE) scheme that integrates cryptographic techniques with RBAC. Our RBE scheme allows RBAC policies to be enforced for the encrypted data stored in public clouds. Based on the proposed scheme, we present a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud while maintaining the sensitive information related to the organization's structure in a private cloud. We describe a practical implementation of the proposed RBE-based architecture and discuss the performance results. We demonstrate that users only need to keep a single key for decryption, and system operations are efficient regardless of the complexity of the role hierarchy and user membership in the system.

Achieving secure and efficient data collaboration in cloud computing

Cloud storage services enable users to remotely store their data and eliminate the excessive local installation of software and hardware. One critical issue is how to enable a secure data collaboration service including data access and update in cloud computing. A data collaboration service is to support the availability and consistency of shared data among multi-users. In this paper, we propose a secure and efficient data collaboration scheme SECO. In SECO, we employ a two-level hierarchical identity-based encryption (HIBE) to guarantee data confidentiality against an untrusted cloud. This paper is the first attempt to explore a secure cloud data collaboration service that precludes information leakage and enables a one-to-many encryption paradigm, data writing operation, and fine-grained access control simultaneously. Security analysis indicates that the SECO enforces fine-grained access control and collision resistance. Extensive performance analysis and experiment results demonstrate that SECO is highly efficient and has a low overhead on computation and communication.

EXISTING SYSTEM

In being a system, we're using google cloud. In a Google cloud, generally, compliance, security, and sequestration conditions can produce an issue since the structure is managed and possessed by a Pall storehouse provider that's located out-premise. the system can be penetrated by any stoner who pays for the service. On the other hand, in the corporate cloud, these conditions don't generally produce an issue since the structure which is managed and possessed by the client is located on-premise.

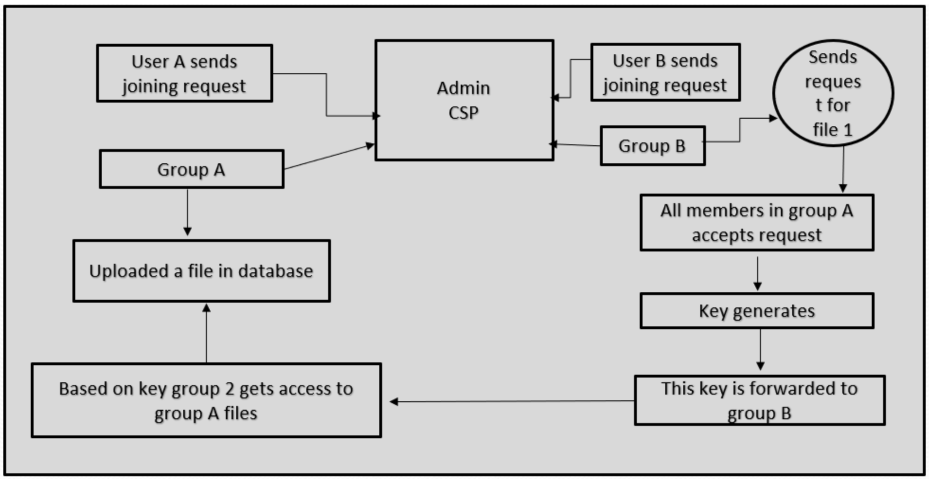
PROBLEM STATEMENT

The security enterprises listed then include Data protection, Control of identity, and access to crucial administration security for virtual machines. Data security and integrity are allowed to be the most grueling issue among five major pall security enterprises, and it may circumscribe the use of all computing. In actuality, data security enterprises include access control and crucial operation. Data confidentiality, integrity, vacuity, and traceability are all terms used to describe data security in the pall, and these conditions give significant challenges for all computing.

PROPOSED SYSTEM

Perpetration of Shamir’s secret sharing algorithm to exclude the security and effectiveness issues being in a public pall system. The Credential Generator is responsible for the construction of the secret key by using the crucial factors entered and sending the secret key to Cloud ManagementClient.This operation would give secure communication with a standalone workstation inside the network and performs encryption of data before uploading and decryption of data after downloading data.

ARCHITECTURE


User A sends joining request
Admin CSP
User B sends joining request
Sends reques t for file 1
Group B
Group A
All members in group A accepts request
Uploaded a file in database
Key generates
Based on key group 2 gets access to group A files
This key is forwarded to group B

ALGORITHM

SHAMIRS SECRET ALGORITHM

An algorithm for distributing keys is called Shamir's Secret Sharing (SSS). The Rivest-Shamir-Adleman (RSA) algorithm was co-invented by the well-known Israeli cryptographer Adi Shamir, after whom it is called.SSS divides a secret into pieces called shares, like a cryptographic key. A group of participants in the conversation receive shares in the company. Shamir's Secret Sharing has the key property that the complete number of shares is not required to rebuild the secret; rather, the pieces of the secret are combined to reconstruct the secret. The threshold is the amount that must be smaller than the total amount. If just one or a few parties are absent, this helps prevent failures in the decryption of sensitive information. Since SSS offers a workable solution to the key-sharing issues that many arrangements encounter, it is frequently used to protect the keys to data that has been encrypted or made safe using other tools or algorithms. A vault that only a company board can access serves as a straightforward example of SSS. A quorum (threshold) of board members is required to approve the display or release of the vault passcode because the passcode is encrypted by SSS. SSS still permits a reasonable assurance that the vault is secure even if a board member is out of town and the requirement is still met.

EXPERIMENTAL ANALYSIS

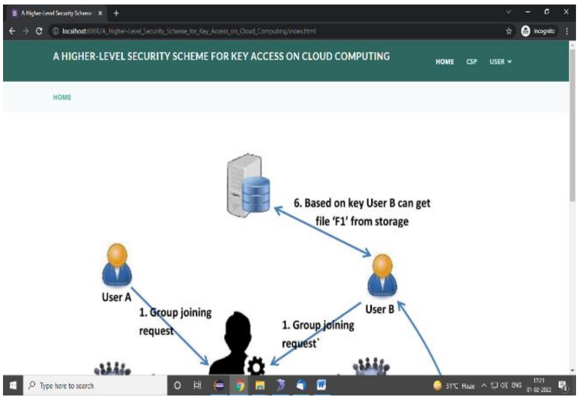

A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME
CSP
USER
HOME
6. Based on key User B can get file 'F1' from storage
User A
1. Group joining request
User B
1. Group joining request

Fig.1 Home

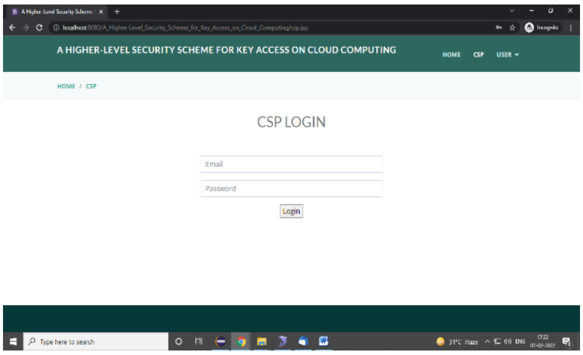

A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME
CSP
USER
HOME / CSP
CSP LOGIN
Email
Password
Login

Fig.2 CSP Login

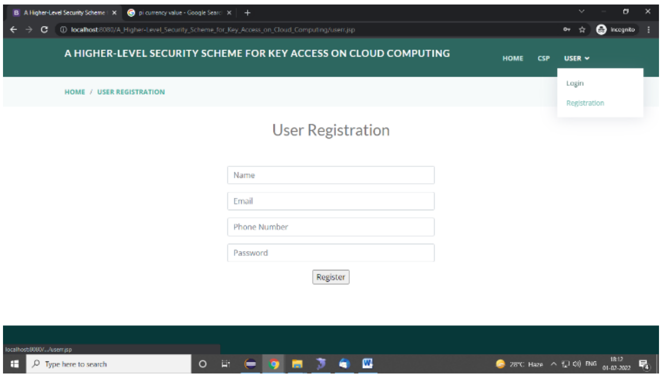


Fig.3 User Registration

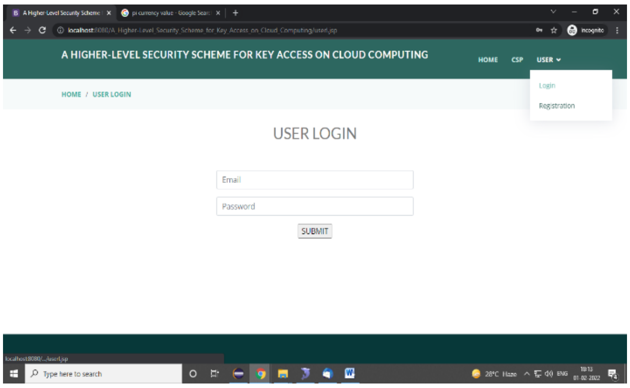
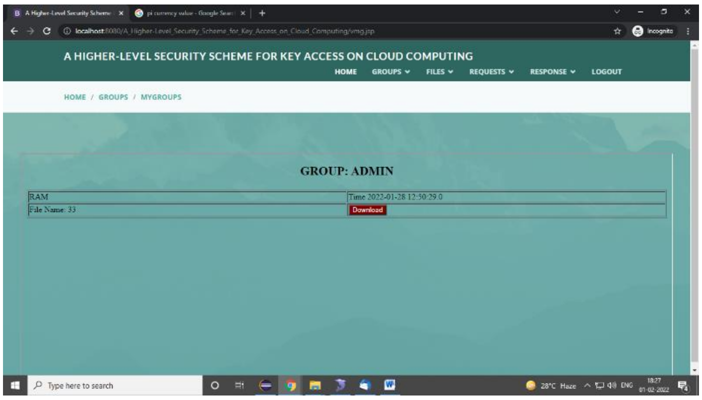


Fig.4 User Login


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME
GROUPS
FILES
REQUESTS
RESPONSE
LOGOUT
HOME / GROUPS / MYGROUPS

GROUP: ADMIN

RAM	Time 2022-01-28 12:50:29.0
File Name: 33	Download

Fig.5 View file shares

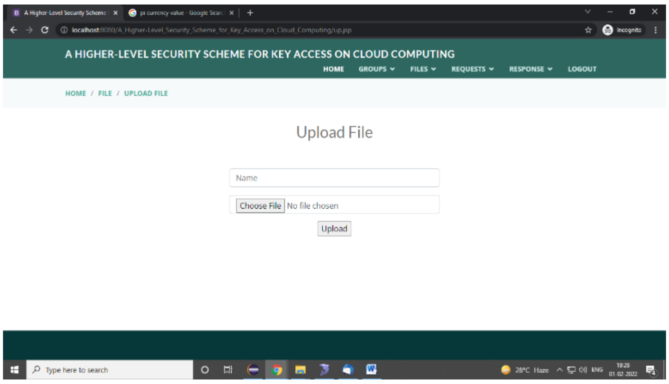
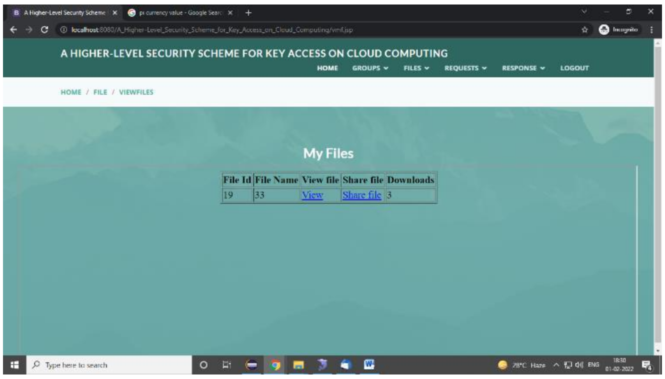
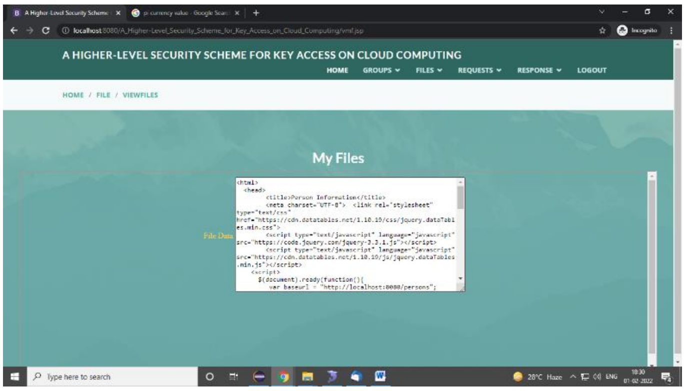

A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME
GROUPS
FILES
REQUESTS
RESPONSE
LOGOUT
HOME / FILE / UPLOAD FILE
Upload File
Name
Choose File No file chosen
Upload

Fig.6 Upload Files


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / FILE / VIEWFILES
My Files

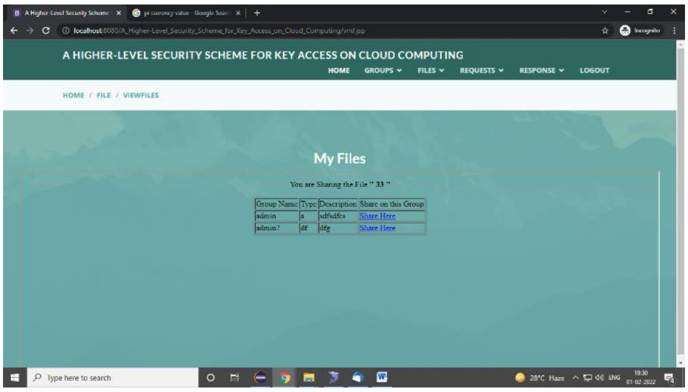
File Id	File Name	View file	Share file	Downloads
19	33	View	Share file	3

Fig.7 View Files


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / FILE / VIEWFILES
My Files
File Data

```
<html>
  <head>
        <title>Person Information</title>
        <meta charset="UTF-8">  <link rel="stylesheet"
type="text/css"
href="https://cdn.datatables.net/1.10.19/css/jquery.dataTabl
es.min.css">
        <script type="text/javascript" language="javascript"
src="https://code.jquery.com/jquery-3.3.1.js"></script>
        <script type="text/javascript" language="javascript"
src="https://cdn.datatables.net/1.10.19/js/jquery.dataTables
.min.js"></script>
    <script>
      $(document).ready(function(){
        var baseurl = "http://localhost:8080/persons";
```

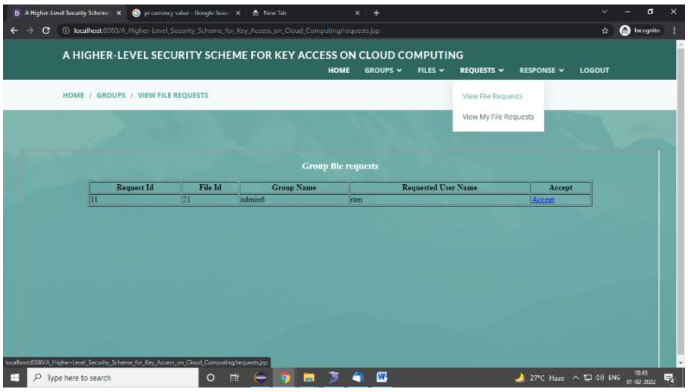
Fig.8 View File Data


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / FILE / VIEWFILES
My Files

You are Sharing the File " 33 "

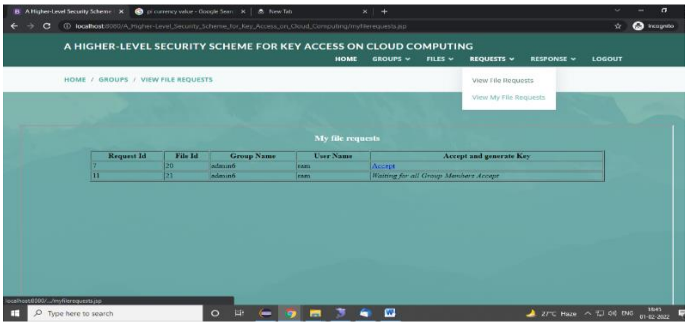
Group Name	Type	Description	Share on this Group
admin	a	sdfsdfcs	Share Here
admin7	df	dfg	Share Here

Fig.9 Share File


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / GROUPS / VIEW FILE REQUESTS
View File Requests
View My File Requests
Group file requests

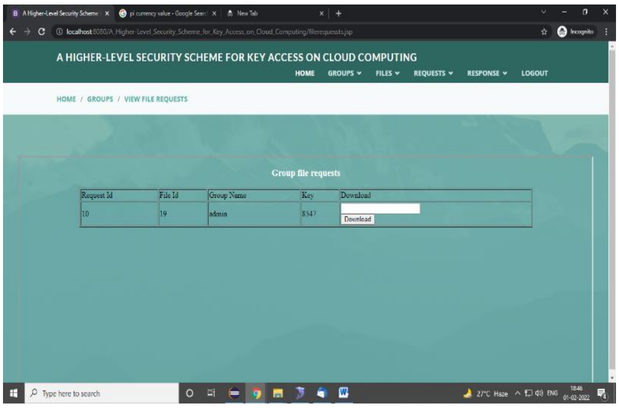
Request Id	File Id	Group Name	Requested User Name	Accept
11	21	admin6	ram	Accept

Fig.10 Group File Requests


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / GROUPS / VIEW FILE REQUESTS
View File Requests
View My File Requests
My file requests

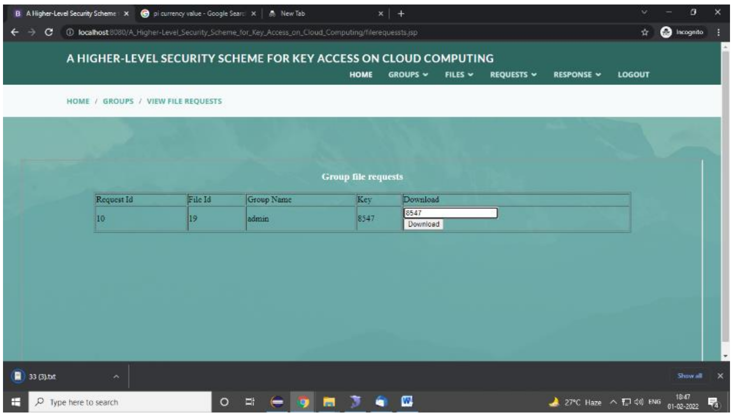
Request Id	File Id	Group Name	User Name	Accept and generate Key
7	20	admin6	ram	Accept
11	21	admin6	ram	*Waiting for all Group Members Accept*

Fig.11 View My File Requests


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / GROUPS / VIEW FILE REQUESTS
Group file requests

Request Id	File Id	Group Name	Key	Download
10	19	admin	8547	Download

Fig.12 Response


A HIGHER-LEVEL SECURITY SCHEME FOR KEY ACCESS ON CLOUD COMPUTING
HOME GROUPS FILES REQUESTS RESPONSE LOGOUT
HOME / GROUPS / VIEW FILE REQUESTS
Group file requests

Request Id	File Id	Group Name	Key	Download
10	19	admin	8547	8547 Download

Fig.13 Response

CONCLUSION

This study makes use of Shamir's secret sharing system to provide a versatile hierarchical key access control mechanism that may be used in a variety of real-time scenarios, particularly for any cloud infrastructure. One of the biggest expenses for data owners is the necessity for public and private storage. Our plan has lessened worries about the security of a hierarchically structured data access policy. The suggested key access control scheme offers a way for a key generation that is computationally effective. The scheme is resistant to collusion, which includes KRs and KIs.The suggested plan offers the functionality, accessibility, and cost savings of the public cloud along with the private cloud's security. Other benefits that come with using the public cloud by businesses are its dependability and low maintenance and management requirements. The following are some additional benefits:

1) The data owner has complete control over the data;

2) It offers hierarchical and organization unit-based management of the data to be processed on the public cloud;

3) Organization unit and user group-based security level policies, namely the multi-hierarchical security mechanism, are provided;

4) The data owner can dynamically adjust the company's security level policies;

5) It provides multi-hierarchical security mechanisms.

5) The data owner can add the user to any user group for any organizational unit. Consequently, the user has control over the data of a different organizational unit.

REFERENCES

1. E. Thomas, P. Ricardo, and M. Zaigham, Cloud Computing: Concepts, Technology, and Architecture, 1st ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2013.
2. M. Peter and G. Timothy, ‘‘The NIST definition of cloud computing, recommendations of the national institute of standards and technology,’’ NIST, Gaithersburg, MD, USA, Tech. Rep. 800-145, 2013.
3. Information Technology-Cloud Computing-Reference Architecture, Standard ISO/IEC 17789:2014, 2014.
4. Information Technology-Cloud Computing-Overview and Vocabulary, Standard ISO/IEC 17788:2014, 2014.
5. L. Zhou, V. Varadharajan, and M. Hitchens, ‘‘Achieving secure role-based access control on encrypted data in cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.
6. S. Kamara and K. Lauter, ‘‘Cryptographic cloud storage,’’ in Proc. Int. Conf. Financial Cryptogr. Data Security., Tenerife, Spain, 2010, pp. 136–149, doi: 10.1007/978-3-642-14992-4_13.
7. X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, ‘‘Achieving secure and efficient data collaboration in cloud computing,’’ in Proc. IEEE/ACM 21st Int. Symp. Qual. Service (IWQoS), Jun. 2013, pp. 1–6, doi: 10.1109/IWQoS.2013.6550281.
8. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, ‘‘A view of cloud computing,’’ Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.
9. L. Zhou, V. Varadharajan, and M. Hitchens, ‘‘Trust enhanced cryptographic role-based access control for secure cloud data storage,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2381–2395, Nov. 2015.
10. S. G. Akl and P. D. Taylor, ‘‘Cryptographic solution to a problem of access control in a hierarchy,’’ ACM Trans. Comput. Syst., vol. 1, no. 3, pp. 239–248, 1983.
11. S. J. Mackinnon, P. D. Taylor, H. Meijer, and S. G. Akl, ‘‘An optimal algorithm for assigning cryptographic keys to control access in a hierarchy,’’ IEEE Trans. Comput., vol. C-34, no. 9, pp. 797–802, Sep. 1985.
12. R. S. Sandhu, ‘‘Cryptographic implementation of a tree hierarchy for access control,’’ Inf. Process. Lett., vol. 27, no. 2, pp. 95–98, 1988.
13. L. Harn and H.-Y. Lin, ‘‘A cryptographic key generation scheme for multilevel data security,’’ Comput. Secure., vol. 9, no. 6, pp. 539–546, Oct. 1990
14. C.-C. Chang, R.-J. Hwang, and T.-C. Wu, ‘‘Cryptographic key assignment scheme for access control in a hierarchy,’’ Inf. Syst., vol. 17, no. 3, pp. 243–247, May 1992.
15. H. T. Liaw, S. J. Wang, and C. L. Lei, ‘‘A dynamic cryptographic key assignment scheme in a tree structure,’’ Comput. Math. Appl., vol. 25, no. 6, pp. 109–114, Mar. 1993.

16. M. S. Hwang, C. C. Chang, and W. P. Yang, ‘‘Modified Chang-Hwang-Wu access control scheme,’’ Electron. Lett., vol. 29, no. 24, pp. 2095–2096, 1993.
17. Web application development with component frameworks
18. A Java-based approach for developing web application system