International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 89-96 www.ijaem.net ISSN: 2395-5252

An Advanced Level Security Design for Key Access on Cloud Computing

Dr.D.J.Samathanaidu[#1], D.Sudhakar[*2], R.Akhila[#3]

[1]Professor&Principal,APGCCS,Rajampet,YSRKadapa,India
[2]Assistant Professor, MCA Department, APGCCS, Rajampet, YSR Kadapa, India[3]MCA Department, APGCCS, Rajampet, YSR Kadapa, India

----
Date of Submission: 25-08-2022 Date of Acceptance: 05-09-2022

ABSTRACT— Digitizing several services increase demands on storage systems, large-scale computations, and hosting. The proposed scheme allows any public cloud system to be used as a private cloud. I consider the data owner an entity consisting of several organization units. I provide a secure method for each user of this entity to access the public cloud from both inside and outside the company's network. The idea of my key access control scheme, which is based on Shamir's secret sharing algorithm and polynomial interpolation method, is suitable especially for hierarchical organizational structures. It offers a secure, flexible, and hierarchical key access mechanism for organizations utilizing mission-critical data. It also minimizes concerns about moving mission-critical data to the public cloud and ensures that only users with sufficient approvals from the same or higher privileged users can access the key by making use of the topological ordering of a directed graph, including self-loop from a security perspective, my scheme is both resistant to collaboration attacks and provides key in distinguishability security. Since the key does not need to be held anywhere, the problem of a data breach based on key disclosure risk is also eliminated.

Keywords—
Bandwidth,Encryption,ComputationalIntelligence, Hash-Solomon,DistributionProportion.

I. INTRODUCTION

Since the 21st century, computer technology has developed rapidly. Cloud computing, an emerging technology, was first proposed in SES 2006 (Search Engine Strategies 2006) by San José and defined by the NIST (National Institute of Standards and Technology). Since its first proposal, cloud computing has attracted great attention from different sectors of society. Cloud computing has gradually matured thanks to

the efforts of so many people. So there are some cloud-based technologies derived from cloud computing. Cloud storage is an important part of them. With the rapid development of network bandwidth, the volume of user data increases geometrically. The capacity of the local machine can no longer meet user requirements. Therefore, people try to find new ways to store their data. In search of more powerful storage capacity, an increasing number of users are selecting cloud storage. Archiving data on a public cloud server is a future trend and cloud storage technology will spread in a few years. Cloud storage is a cloud computing system that provides data storage and management services. With a group of applications, network technology and distributed file system technology, cloud storage allows a large number of different storage devices to work together in a coordinated way. Today there are many companies that offer a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc. These companies offer a large storage capacity and various services related to other popular applications, which in turn lead to their success in attracting humorous subscribers. However, the cloud storage service still has many security concerns. The privacy issue is particularly significant among these security concerns. In history, there have been some famous events of privacy leaks in cloud storage. For example, the Apple iCloud loss event in 2014, numerous private photos of Hollywood actresses stored in the clouds were stolen.

Purpose

Perhaps the most important aspect of your cloud security strategy is how you respond to security incidents. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Scope

The scope of application is Hash-Solomon code algorithm is designed to divide data into different parts. Then, I can put a small part of data in local machine and fog server in order to protect the privacy.

II. RELATED WORK

ExistingSystem

Secure key access control scheme in the hierarchical structure to demonstrate how we can securely consume the DSaaS service. The DSaaS permits users and organizations to store an enormous amount of data on demand in a cost-effective manner. They do not consider the fact that the user may have access to the private key of a class for a certain period of time. The first time-bound access control scheme is based on tamper-proofed devices. The first one is collusion resistant but costly and unsuitable for the cloud, limiting user convenience. But, the 3 second one can be used efficiently in the cloud due to the characteristic of broad network access.

Disadvantages

Increased cost
Low Performance
Less Secure
III.PROPOSEDWORK

ProposedSystem

The proposed scheme allows any public cloud system to be used as a private cloud. We consider the data owner an entity consisting of several organization units. We provide a secure method for each user of this entity to access the public cloud from both inside and outside the company’s network. The idea of my key access control scheme, which is based on Shamir’s secret sharing algorithm and polynomial interpolation method.

Advantages
Resistant to collaboration attacks
Computationally efficient.
Cost-effectiv

COMPARATIVE RESULTS

Implementation is the process of ensuring that the information system is operational and therefore allowing the user to perform his operations for his use and evaluation operations. The implementation includes the following activities.

a. Obtain and install system hardware.
b. Install the system and run it on the intended hardware.
c. Provide users with access to the system.
d. Database creation and updating.
e. Train users on the new system.
f. Document the system for its users and for those who will be responsible for its maintenance in the future.
g. Make arrangements to support the user while using the system.
h. Transfer of responsibilities underway for the developer&#39;s system in operation or maintenance.

Sample Screens & reports

Advanced Level Security
An Advance Level Security Design For Key Access On Cloud Computing
You Have A Vision. We Have A Team To Get You There
Get Started

Screen 5.1.1: Home Page

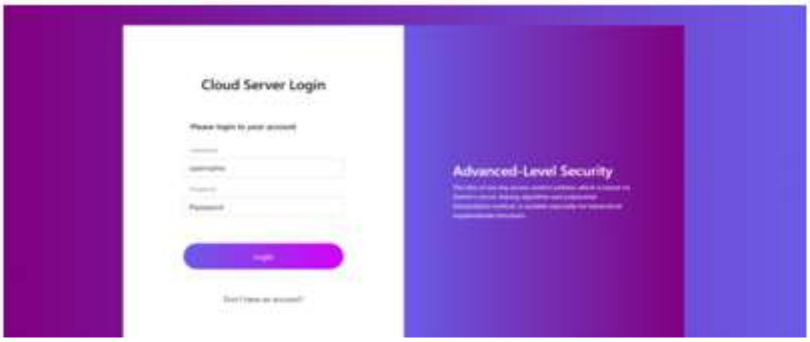
Description: The above screen displays home page of the An advanced level design for key access on cloud computing

Data Owner Register

Advanced-Level Security

Screen2:RegistrationModule

Description: This screen displays Data User Registration which contains the fields like name, password, mail address, mobile and other fields.


Cloud Server Login

Please login to your account

Advanced-Level Security

Screen 5.1.3: Data User login

Description: The above screen displays to login page of data owner.

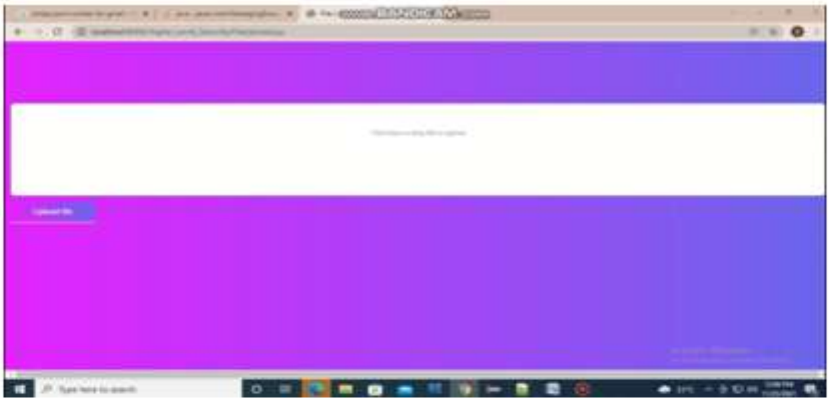
Welcome Possessor...!

An Advance Level Security Design For Key Access On Cloud Computing

You Have A Vision. We Have A Team To Get You There

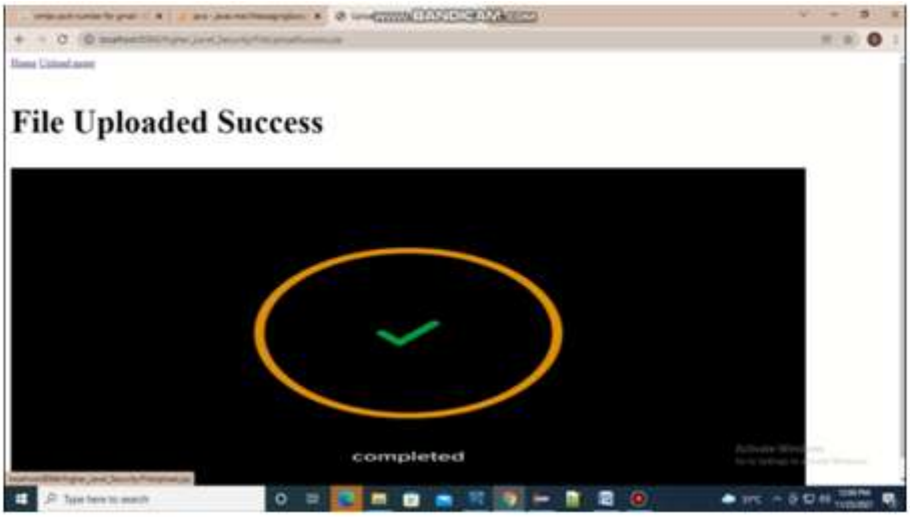
Screen 5.1.4: Data owner home page

Description: The above screen display Data owner home page.



Screen 5.1.5: Data Owner Upload file

Description: The above screen displays the data owner Upload file.

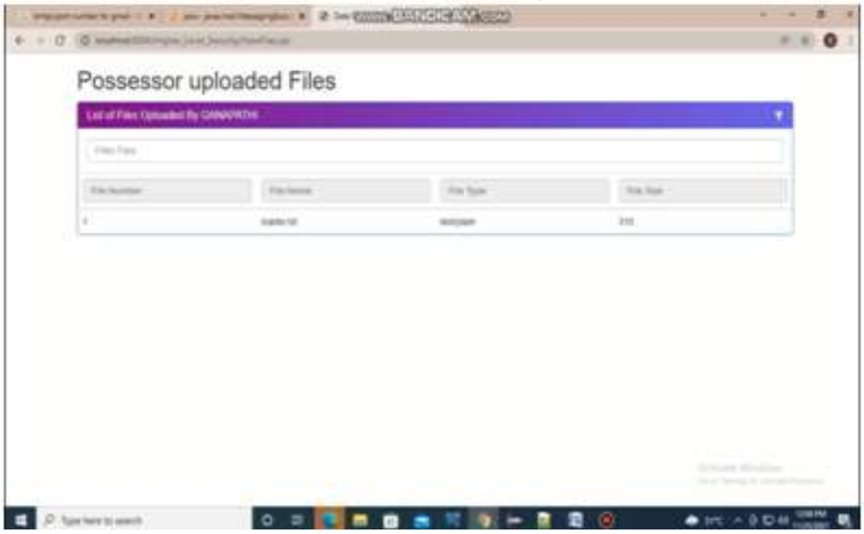


File Uploaded Success

completed

Screen 5.1.6: File upload successfully

Description: The above screen display thedata owner is uploading a file in to cloud server in successfully.

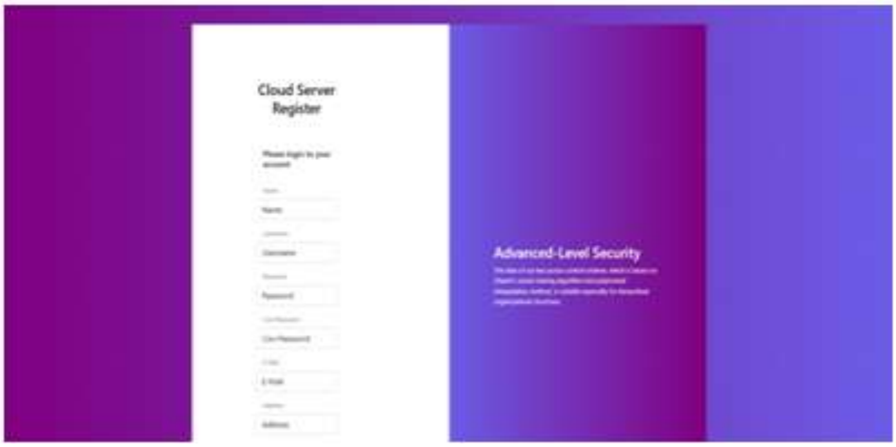


Possessor uploaded Files

File Number	File Name	File Type	File Size
1	[illegible]	[illegible]	[illegible]

Screen 5.1.7: Data Owner view files

Description: The above screen displays Data Owner view files.



Cloud Server Register

Name

Username

Password

Con Password

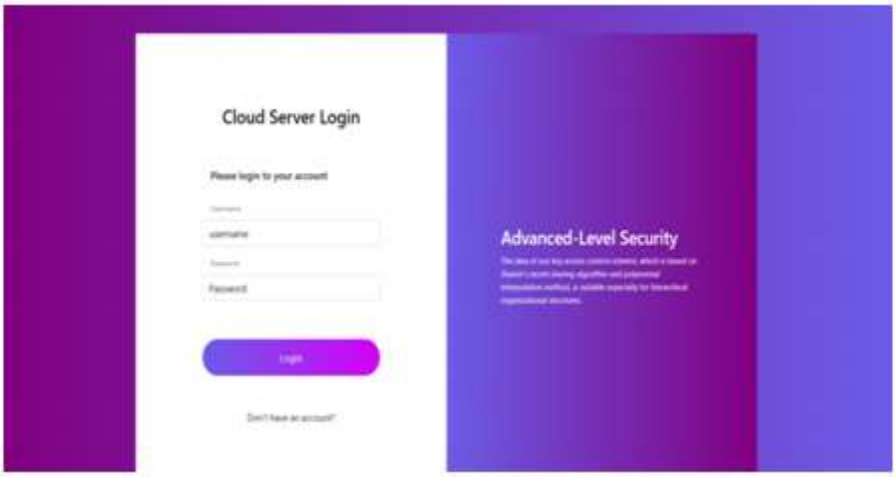
E-mail

Address

Advanced-Level Security

Screen 5.1.8: Data user Register

Description: The above screen display the data user registration

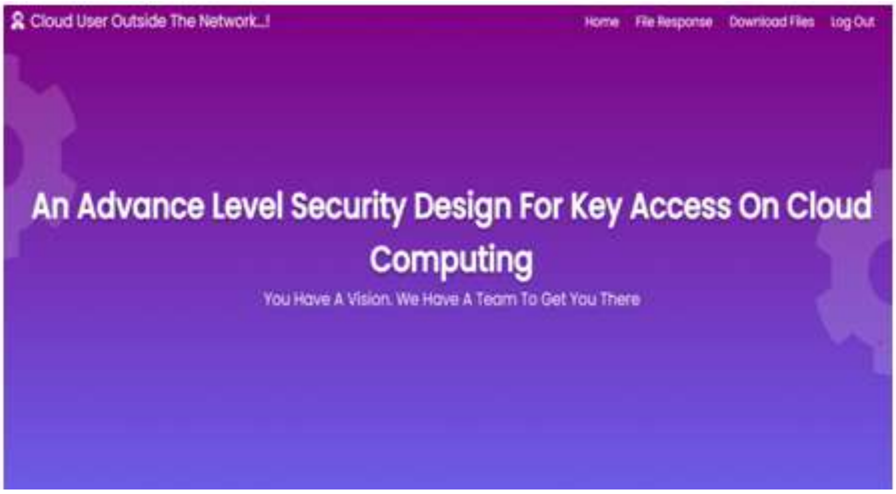


Advanced-Level Security

The idea of our key access control scheme, which is based on Shamir's secret sharing algorithm and polynomial interpolation method, is suitable especially for hierarchical organizational structures.

Screen 5.1.9: Data user login

Description: The above screen displays the data login page

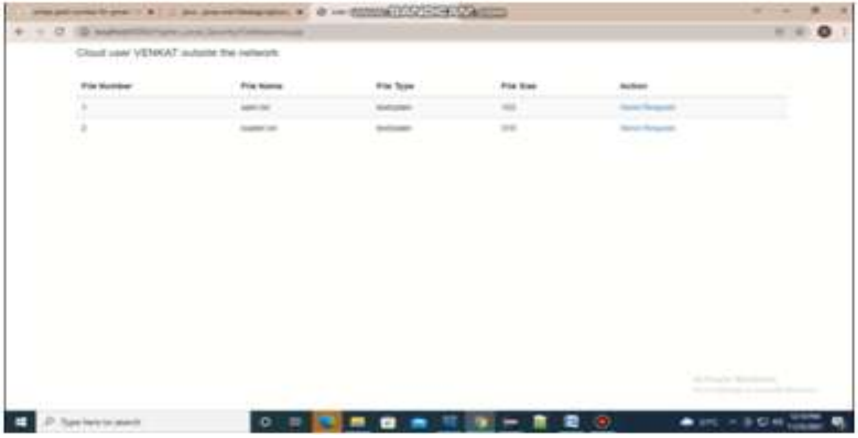


An Advance Level Security Design For Key Access On Cloud Computing

You Have A Vision. We Have A Team To Get You There

Screen 5.1.10: Dta User Home page

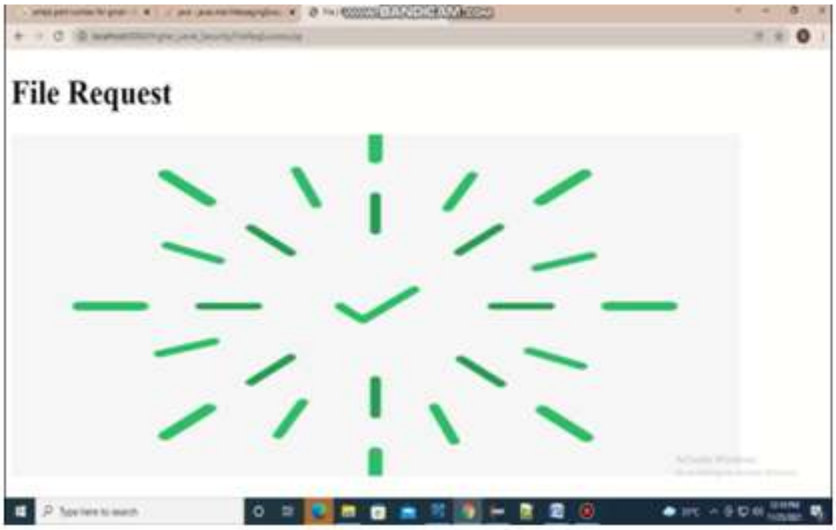
Description: The above screen display the data user home page


Cloud user VENKAT outside the network

File Number	File Name	File Type	File Size	Action
1	[illegible]	text/plain	[illegible]	Send Request
2	[illegible]	text/plain	[illegible]	Send Request

Screen 5.1.11 Data user view files and request file

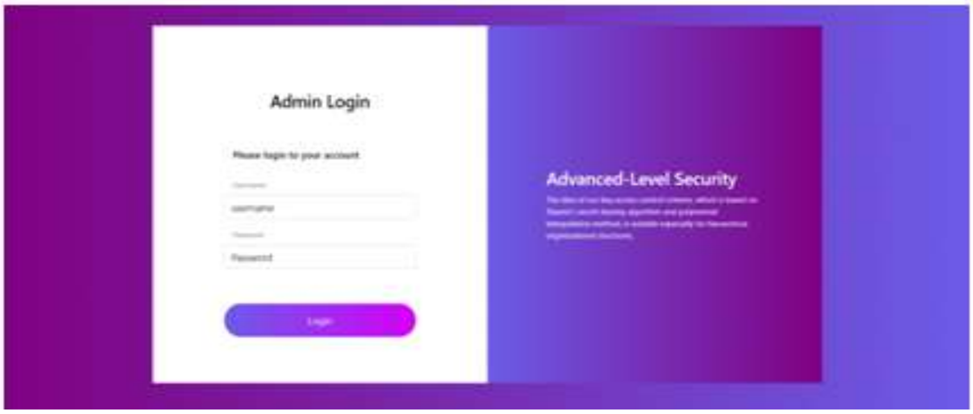
Description: The above screen display to data user view file and also request files



File Request

Screen 5.1.12: File Request

Description: The above screen contains to display the data receiver file details. The data receiver has to download a file to send request to data owner.



Admin Login

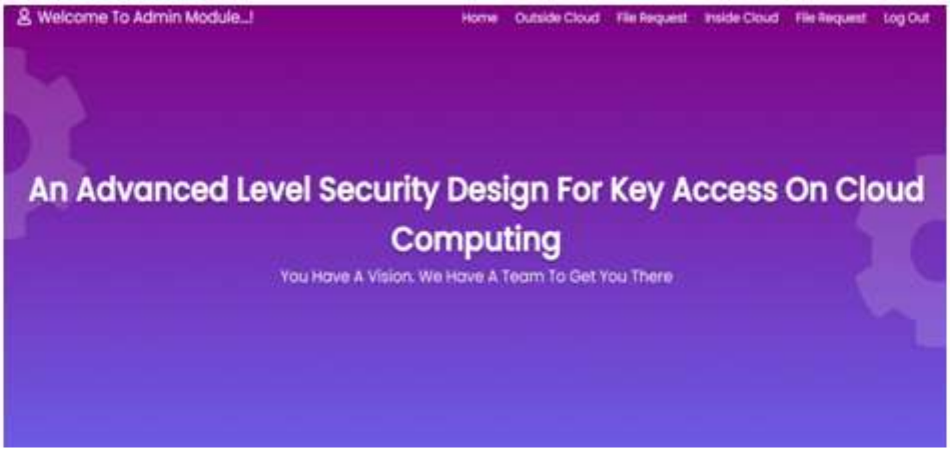
Please login to your account

username

Password

Screen 5.1.13: Admin login page

Description: The above screen display the admin login page



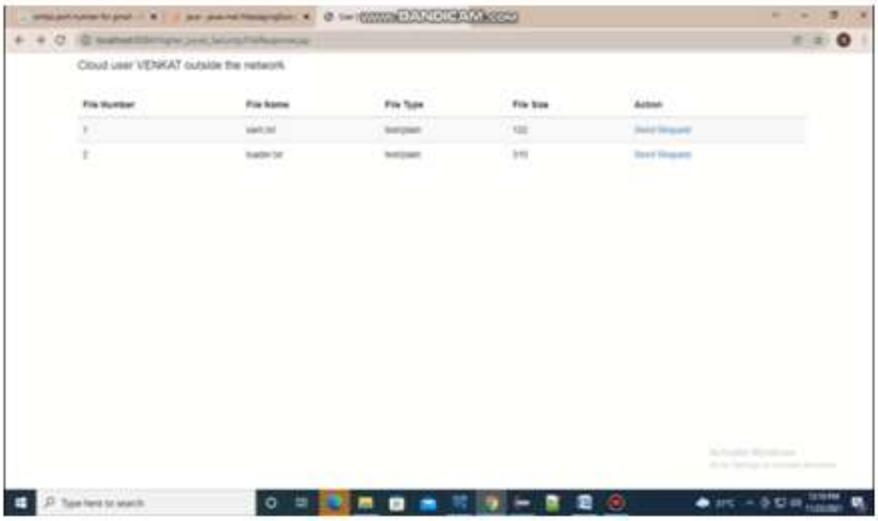
Welcome To Admin Module..!

An Advanced Level Security Design For Key Access On Cloud Computing

You Have A Vision. We Have A Team To Get You There

Screen 5.1.14: Admin home page

Description: The above screen is display the admin home page



Cloud user VENKAT outside the network

File Number	File Name	File Type	File Size	Action
1	sam.txt	text/plain	122	Send Request
2	loader.txt	text/plain	370	Send Request

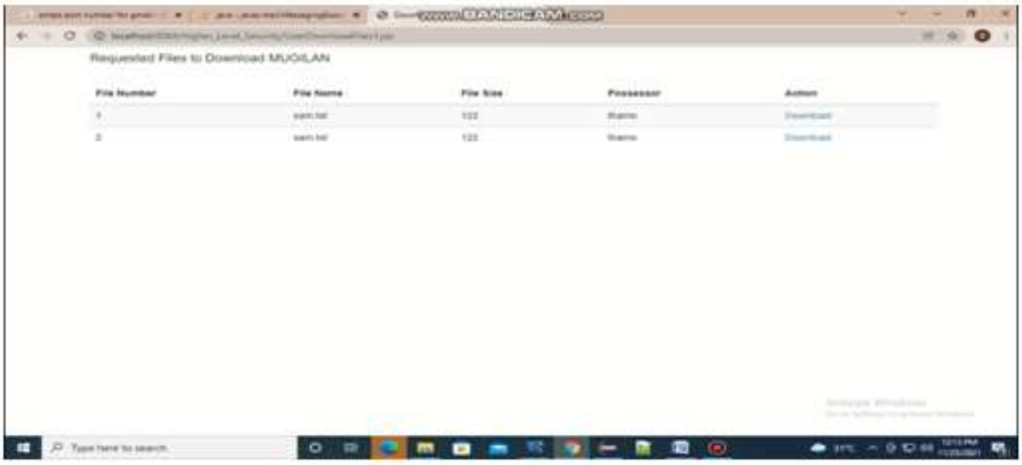
Screen 5.1.15: Admin view and send request

Description: The above screen is display the admin view file and send request file

File Accepted

Screen 5.1.16: File Accepted

Description: The above screen is display file Accepted successfully

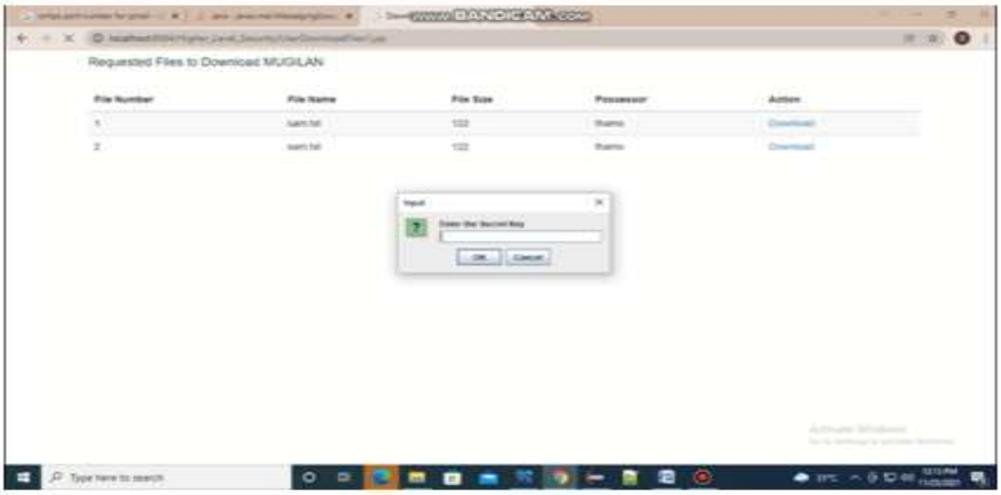


Requested Files to Download MUOILAN

File Number	File Name	File Size	Possessor	Action
1	sam.txt	122	Rama	Download
2	sam.txt	122	Rama	Download

Screen 5.1.17: Download File

Description: The above screen is display the data user download a file



Requested Files to Download MUGILAN

File Number	File Name	File Size	Possessor	Action
1	sam.txt	122	thamo	Download
2	sam.txt	122	thamo	Download

Input

Enter the Secret Key

Screen 5.1.18: Data user download file using key

Description: The above screen is display the data user downloading files

III. CONCLUSION

Finally, I conclude that, this work, Shamir's secret sharing scheme and Newton's interpolation method have been exploited to construct a flexible hierarchical key access control mechanism that can be employed in various real-time scenes, especially for any cloud infrastructures. Public and private storage needs are one of the main overheads for the data owners. Our scheme has reduced the concern on the security of data access policy based on a hierarchical structure. The proposed key access control scheme provides a computationally efficient method for key derivation. The scheme is collusion resistant, and this means KRs and KIs. The proposed scheme provides both the private cloud security and the functionality, accessibility, and cost savings of the public cloud. With the use of the public cloud by companies, other advantages such as the reliability of the public cloud and the minimum maintenance and management requirements.

ACKNOWLEDGMENT
We thank all the authors and their value Contribution Work helped me to complete my final year project.

REFERENCES

[1]. 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.

[2]. 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.

[3]. W.-G. Tzeng, ''A time-bound cryptographic key assignment scheme for access control in a hierarchy,'' IEEE Trans. Knowl. Data Eng., vol. 14, no. 1, pp. 182–188, Aug. 2002.

[4]. H. M. Sun, K. H. Wang, and C. M. Chen, ''On the security of an efficient time-bound hierarchical key management scheme,'' IEEE Trans. Dependable Secure Comput., vol. 6, no. 2, pp. 159–160, Apr. 2009.

[5]. S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, ''Achieving simple, secure and efficient hierarchical access control in cloud computing,'' IEEE Trans. Comput., vol. 65, no. 7, pp. 2325–2331, Jul. 2016.

[6]. A. K. Das, N. R. Paul, and L. Tripathy, ''Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem,'' Inf. Sci., vol. 209, pp. 80–92, Nov. 2012.

[7]. Y.-L. Lin and C.-L. Hsu, ''Secure key management scheme for dynamic hierarchical access control based on ECC,'' J. Syst. Softw., vol. 84, no. 4, pp. 679–685, 2011.

[8]. A. De Santis, A. L. Ferrara, and B. Masucci, ''Efficient provably-secure hierarchical key assignment schemes,'' Theor. Comput.Sci., vol. 412, no. 41, pp. 5684–5699, 2011.