ISSN: 2366-1313

# DUAL ACCESS CONTROL FOR CLOUD BASED DATA STORAGE AND SHARING

**[1]G Swetha, [2]Andru Rakshitha, [3]Gurram Anil, [4]J M Shilpa**

[1]Assistant Professor, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

swethareddy630@gmail.com

[2]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

rakshithaandru@gmail.com

[3]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

gurramanil7330@gmail.com

[4]BTech student, Dept.of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

shilpasindhuri345@gmail.com

***Abstract***: *Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low-cost management. Since it provides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.*

***Keywords***: *Cloud computing, dual data accessing, data sharing, AES, Denial of Sustainability*.

## I. INTRODUCTION

Due to its extensive list of advantages, which includes access freedom and the lack of local data management, in many Internet-based commercial products (such as Apple iCloud). Nowadays, a growing

ISSN: 2366-1313

number of people and businesses prefer to outsource their data to faraway clouds in order to avoid having to upgrade their local data management facilities or devices. However, one of the biggest barriers preventing Internet users from embracing cloud-based storage services generally may be their concern about security breaches involving outsourced data. Outsourced data may need to be subsequently shared with others in many practical scenarios. Alice, a Dropbox user, might send her friends pictures [1].

Without employing data encryption, Alice must first create a sharing link and then distribute it to others in order to share the images. The sharing link may be exposed at the Dropbox administration level, even though it guarantees some level of access restriction over unauthorized users (for example, those who are not Alice's friends) (e.g., administrator could reach the link).

A simple solution to prevent shared photos from being accessed by system "insiders" is to specify the group of authorized data users before encrypting the data. However, Alice might not always be aware of who will be receiving or using the photos. Alice might only be aware of attributes related to photo receivers.

One of the emerging developments is distributed computing. It addresses a fundamental shift in perspective in the way frameworks are communicated [2]. "Computing on a larger scale is a model for enabling ubiquitous, high-performance computing, advantageous, on-demand network access to a shared pool of figurable assets that can be customised It may be provisioned and delivered fast with minimum administrative effort or reliance on a specialised organisation." This distributed computing provides a number of benefits, particularly in ubiquitous administrations where anyone can use PC administrations via the internet. You may create a device with a small display, processor, and RAM using distributed computing. Different types of equipment, such as extra memory, are not required. It will make our new invention gadgets smaller. In addition, it lowers our framework's costs Virtualization, on-demand configuration, Internet administration distribution, and open-source programming is examples of distributed computing [3]. The distributed computing model is depicted in the diagram below.

ISSN: 2366-1313

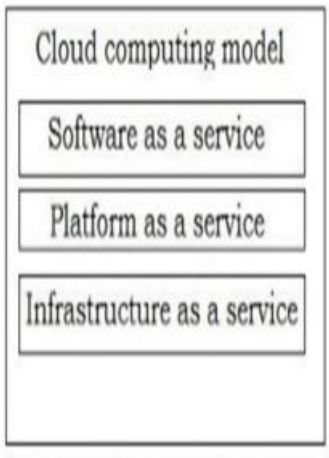



Fig.1 Model of cloud computing

**SaaS** - To make use of the vendor's cloud-based apps, which are available via a simple client interface, as in a Web application, from a range of client devices.

**PaaS**-To upload customer-made apps to the cloud using the provider's supported programming languages and tools ( java, python, .Net) c.

**IaaS**-To set up handling, capacity, organisations, and other basic figuring assets where the customer can deliver and run irregular programming, such as functional frameworks and applications.

We currently have a selection of access control methods in distributed computing. These, on the other hand, are difficult to recover upon use and useless. Because of this issue, we are trying to recommend a new and more efficient approach to managing access to distributed computing.

## II. LITERATURE SURVEY

Literature survey is the most important step in software and project development process. Before developing, it is necessary to determine the use, efficiency, and application of the to-be developed project. Once these things are identified, then next steps are, to determine which operating system and language can be used for developing the project. After the start of building the project, lot of external support is required. This support can be obtained from senior programmers, from book or from websites and from the existing systems. Before building the system, the considerations from existing system are considered for developing the proposed system.

In this section, we'll look at some of the existing access control mechanisms that have been presented. We will go over our solution to distributed computing access control. FADE, which was given by Y.Tang and colleagues , is another key approach for access control. For re-appropriated information on the cloud, the technique in [4] provides fine-grained admission control and guaranteed erasure. However, this strategy isn't actually necessary. If the information owners and specialised cooperatives are in the same area, it is a good idea Another access control plan is HASBE

ISSN: 2366-1313

Alexandros Baka's et al. [5] Secure cloud storage is considered as one of the most important issues that both businesses and end-users consider before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of AttributeBased Encryption (ABE). In this paper, we propose a hybrid encryption scheme that combines both SSE and ABE by utilizing the advantages of both these techniques. In contrast to many approaches, we design a revocation mechanism that is completely separated from the ABE scheme and solely based on the functionality offered by SGX.

Antonis Michalas et al. [6] Secure cloud storage is considered one of the most important issues that both businesses and end-users are considering before moving their private data to the cloud. Lately, we have seen some interesting approaches that are based either on the promising concept of Symmetric Searchable Encryption (SSE) or on the well-studied field of Attribute-Based Encryption (ABE). In the first case, researchers are trying to design protocols where users' data will be protected from both internal and external attacks without paying the necessary attention to the problem of user revocation. On the other hand, in the second case existing approaches address the problem of revocation. However, the overall efficiency of these systems is compromised since the proposed protocols are solely based on ABE schemes and the size of the produced ciphertexts and the time required to decrypt grows with the complexity of the access formula. In this paper, we propose a protocol that combines both SSE and ABE in a way that the main advantages of each scheme are used. The proposed protocol allows users to directly search over encrypted data by using an SSE scheme while the corresponding symmetric key that is needed for the decryption is protected via a Ciphertext- Policy Attribute-Based Encryption scheme.

G. Wang et al. [7] Searchable Encryption (SE) has been extensively examined by both academic and industry researchers. While many academic SE schemes show provable security, they usually expose some query information (e.g., search and access patterns) to achieve high efficiency. However, several inference attacks have exploited such leakage, e.g., a query recovery attack can convert opaque query trapdoors to their corresponding keywords based on some prior knowledge. On the other hand, many proposed SE schemes require significant modification of existing

ISSN: 2366-1313

applications, which makes them less practical, weak in usability, and difficult to deploy. In this paper, we introduce a secure and practical searchable symmetric encryption scheme with provable security strength for cloud applications, called IDCrypt, which improves the search efficiency, and enhances the security strength of SE using symmetric cryptography. To address the above issues, we propose a token adjustment search scheme to preserve the search functionality among multi-indexes, and a key sharing scheme which combines identity-based encryption and public-key encryption. Our experimental results show that the overhead of the key sharing scheme is fairly low.

## III. PROPOSED METHODOLOGY

The development of our proposed model. As seen in Figure 2, our proposed model has a progressive construction

## SYSTEM ARCHITECTURE

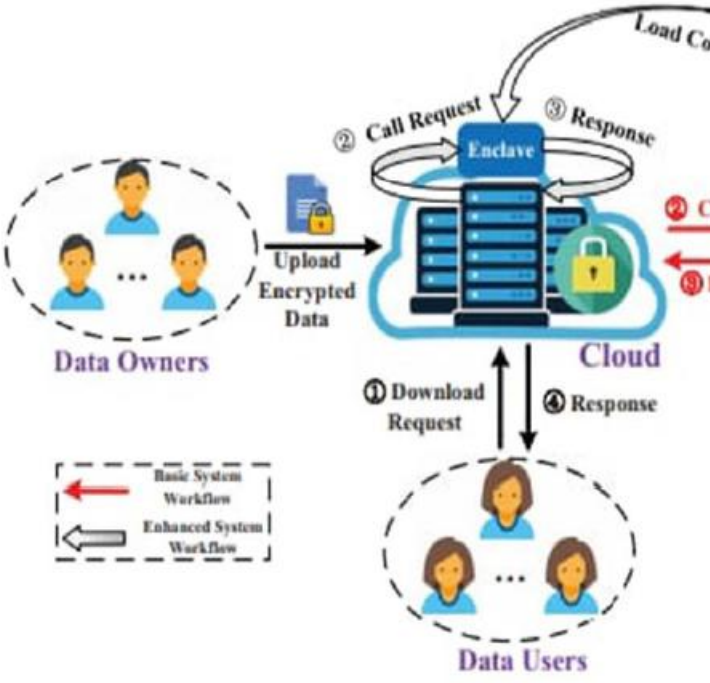



Fig.2 System architecture

The believed power serves as the foundation of confidence in this progressive structure, approving high-level space professionals. Furthermore, the cloud clients are approved by this high-level area specialist. As a cloud client, we consider both the proprietors and the clients. Our system retains a trait set for each cloud client, which contains a number of traits specific to that client. It is possible that it will change depending on the client. A space consists of a single area authority and a large number of cloud clients. We also use a clock to time the creation of the key.

### Framework Model

ISSN: 2366-1313

Figure 3 depicts the real-world model of our approach. There are four sections in total in this model. Owner of the cloud, untrustworthy cloud, clock, and cloud client

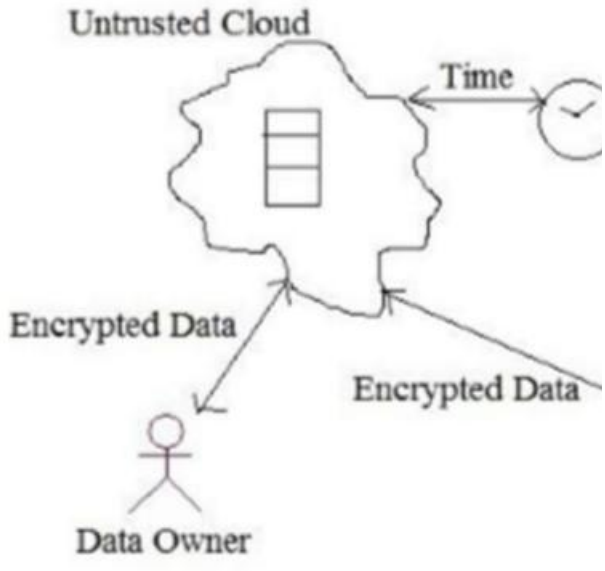



Fig.3 System Model

The owner of the data can upload it to the cloud from here. To make his record as untrustworthy as possible, he will scramble the document straight away and then move it to the untrusted cloud. Only the owner of the information is aware of how to decrypt the records. As a result, the transferred data is safe in the untrustworthy cloud. When an information client needs to access a record from the cloud, it sends a request to the cloud. Following that, the cloud will forward the request to the proprietor. The owner will then check the client's distinctive arrangement. If the client has a large number of traits, the owner will transmit a key to the client. The clock will start counting when the proprietor sends the client a key. That key becomes invalid when a certain amount of time has passed. As a result, the client must complete the requested paper within the specified timeframe.

**Fundamental tasks of the proposed model**

**1. Registration:**

The client and the owner must both enrol in order to perform any action in the cloud. The client and the proprietor will send an enlistment request to the comparing space authority for enrolment. The space authority then confirms that the new part is complying with the agreements. If they are willing to accept the terms, the area authority will forward the request to the confided in space. The thought power will then provide every one of the proprietors and clients with an exceptionally long-lasting id. Then they'll be able to create a secret key for them.

**2. Document Upload:**

To convey a document to a higher level, the information owner must first encrypt it with his confidential key and then send itto the next higher level. That is the jurisdictional authority. The space authorities will then verify whether or not

ISSN: 2366-1313

the proprietor is registered. If he is a registered proprietor, the space authority will send that encoded record to the confided in authority.

3**. Document Download**:

To download any record from the cloud, the information client must first send a request to his corresponding space authority. The client will then be checked by the local authority. If the client is legitimate, the request will be forwarded to the trusted in power. The believed power will then forward this request to the owner of the relevant data. The proprietor will then examine the client's trait set. If the client has a large number of traits, the owner will transmit a key to the client. The clock will start counting whenever the proprietor sends a key to a client. That key becomes invalid when a certain amount of time has passed. As a result, the client must complete the requested paper within the specified time frame

.

## IV. RESULTS

**4. Document Deletion**

Only the owner of the data has the ability to delete it from the cloud. During the information proprietor's enlisting season, the believed power will assign each information proprietor an id number. Forthem, these id numbers are exceptionally long-lasting. Similarly, each of them has a secret key that isn't particularly longlasting. To delete a document, the information owner must first file a request to his corresponding space authority. The proprietor id and document name are included in this solicitation. The area administration will then inquire about the proprietor's secret word. The area authority will forward the deletion request to the confided in power if the proprietor offers the correct secret word. The believed power will then delete the document from the cloud

ISSN: 2366-1313


Fig.4 Home page

The home page showing various details to go through it. It consists of menu like User, Server1, Server2 and Registrations for new users. Users can be able to access all the modules which have implemented in the menu of home page.

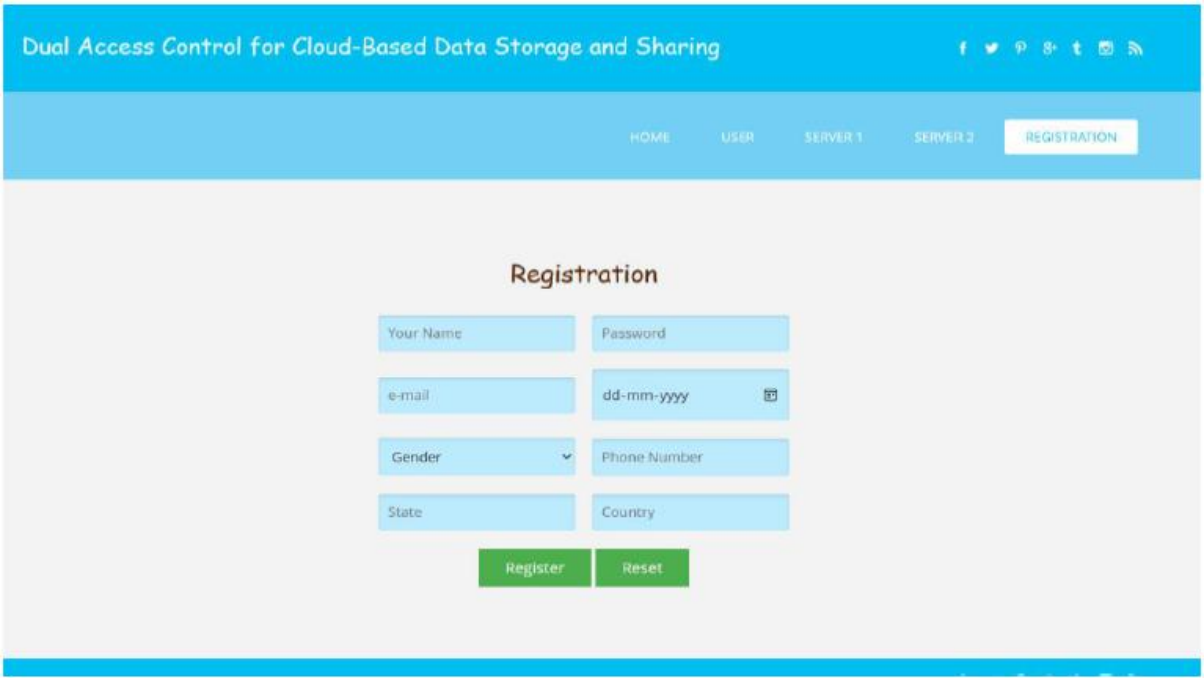


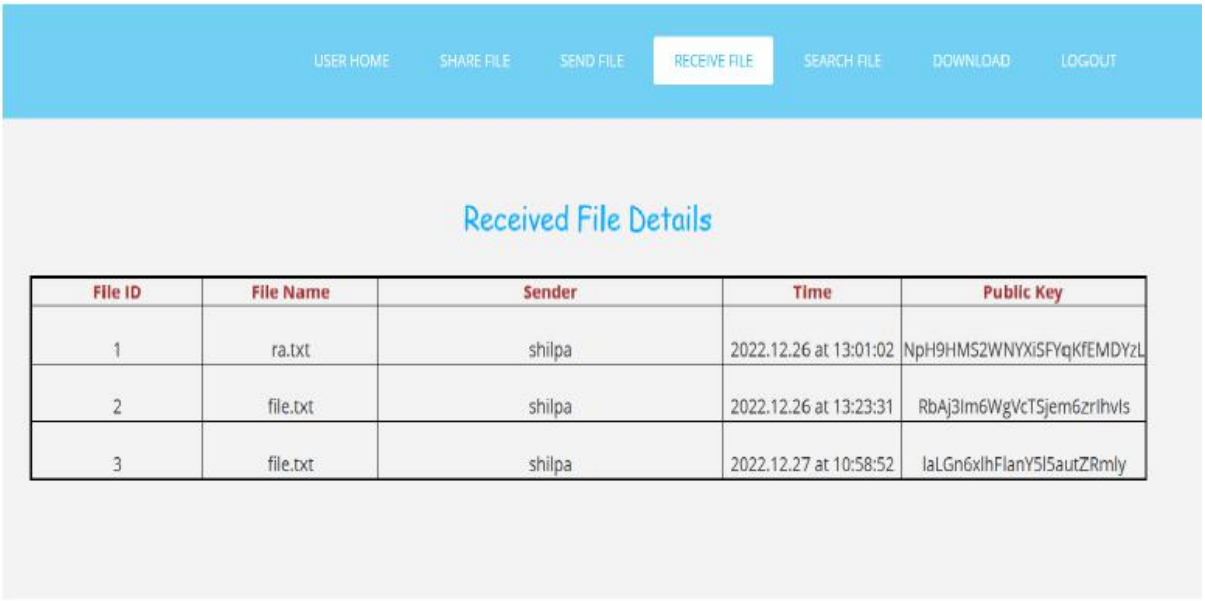

Fig.5 Registration

Users can register with their email id's and with some other details. It accepts multiple users to register in order to access the files uploaded by other users or data owners. After registering a pop up shows the acknowledgement either success or failed

ISSN: 2366-1313


Fig.6 Login page

After registering users can login through their hypertexts. Server's login should be done to get file details and downloads list

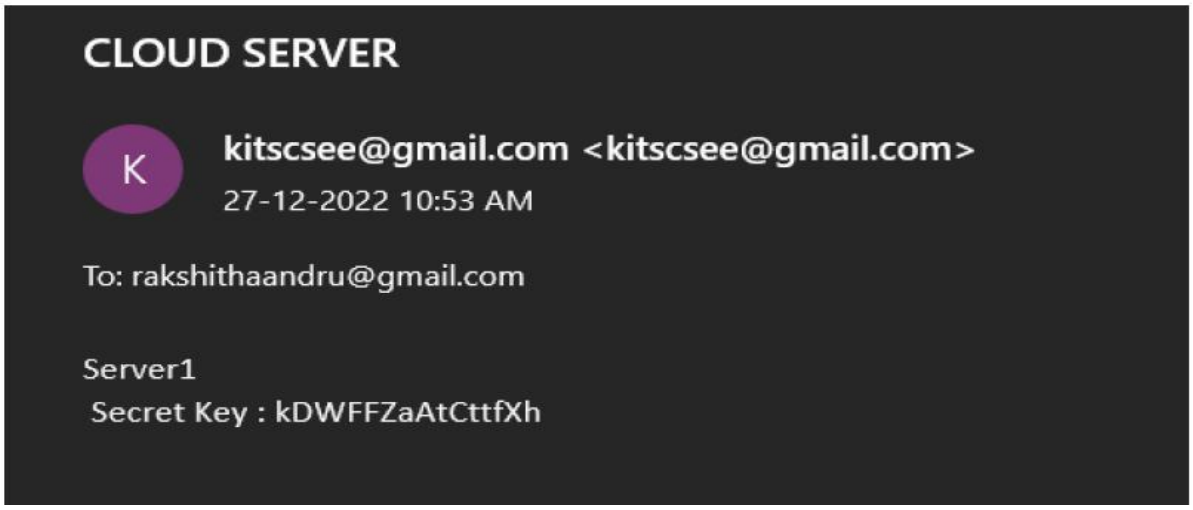



| File ID | File Name | Sender | Time | Public Key |
|---|---|---|---|---|
| 1 | ra.txt | shilpa | 2022.12.26 at 13:01:02 | NpH9HMS2WNYXiSFYqKfEMDYzL |
| 2 | file.txt | shilpa | 2022.12.26 at 13:23:31 | RbAj3Im6WgVcTSjem6zrIhvIs |
| 3 | file.txt | shilpa | 2022.12.27 at 10:58:52 | IaLGn6xIhFIanY5I5autZRmIy |

**Fig.7** File details page

Data owner can upload files and the received files can be shown in all the modules. Keys are shown in users pages where details are given along with time of upload and receiving.

ISSN: 2366-1313




File.8 server page

After data owner upload their files then the client who wants to access the files which are stored in cloud need to get the key to download. In that case, after server1 login the client sends request to cloud thus a mail is sent to client by the server giving key.

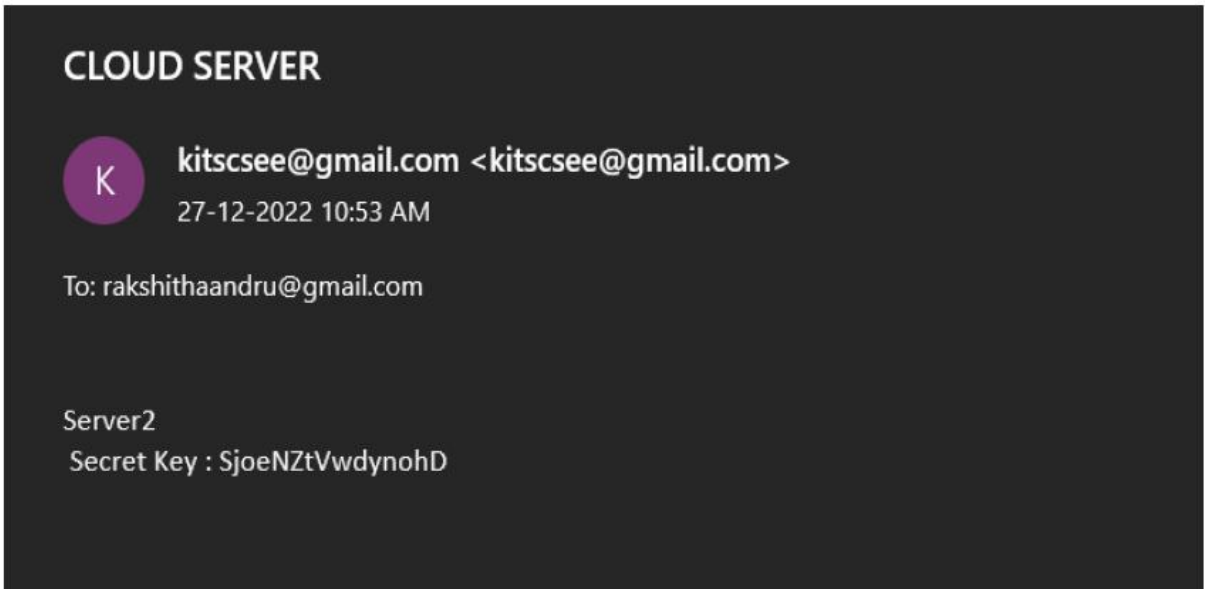



Fig.9 server 2 mail

ISSN: 2366-1313

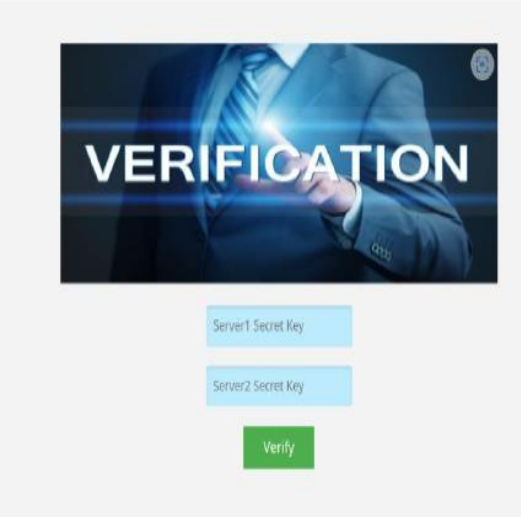



Fig.10 Verification Page

After verifying the keys file will be accessible for client to download

## V. CONCLUSION

In this Project, we addressed an interesting and long-lasting problem in cloud-based data sharing, and presented two dual access control systems. The proposed systems are resistant to DDoS/EDoS attacks. We state that the technique used to achieve the feature of control on download request is "transplantable" to other CP-ABE constructions. Our experimental results show that the proposed systems do not impose any significant computational and communication overhead (compared to its underlying CP-ABE building block). In our enhanced system, we employ the fact that the secret information loaded into the enclave cannot be extracted. However, recent work shows that enclave may leak some amount so fits secret(s) to a malicious host through the memory access patterns or other related side-channel attacks. The model of transparent enclave execution is hence introduced in. Constructing a dual access control system for cloud data sharing from transparent enclave is an interesting problem. In our future work, we will consider the corresponding solution to the problem.

## REFERENCES

[1] Dr. C.N. Sakhale, D.M. Mate, Subhasis Saha, Tomar Dharmpal, Pranjit Kar, Arindam Sarkar, Rupam Choudhury, Shahil Kumar , ―An Approach to Design of Child Saver Machine for Child Trapped in Borehole ― , International Journal of Research in Mechanical Engineering, October-December, 2013, pp. 26-38.

ISSN: 2366-1313

[2] K. Saran, S. Vignesh, Marlon Jones Louis have discussed about the project is to design and construct a ― Bore-well rescue robot‖ (i.e. to rescue a trapped baby from bore well), International Journal of Research in Aeronautical and Mechanical Engineering, Boar well rescue robot , pp. 20-30 April 2014

[3] G. Nithin, G. Gowtham, G. Venkatachalam and S. Narayanan, School of Mechanical Building Sciences, VIT University, India, Design and Simulation of Bore well rescue robot – Advanced, ARPN Journal of Engineering and Applied Sciences, pp. MAY 2014.

[4] Camera - Direct web search on google.com

[5] J. Burke and R.R.Murphy, ― Human-robot interaction in USAR technical search: Two heads are better than one, ‖ inProc.IEEE Int. Workshop ROMAN, Kurashiki, Japan, 2004, pp. 307-312.

[6] J. Casper and R. R. Murphy, ―Human-robot interactions during the robot assisted urban search and rescue response at the world trade center, ‖ IEEE Trans. Syst., Man, Cybern. B, Cybern., Vol. 33, no. 3, pp. 367–385, Jun. 2013.

[7] R. R. Murphy, ― Activities of the rescue robots at the World Trade Center from 11 – 21 September 2001, ‖ in Proc. IEEE Robot. Autom. Mag., 2004, pp. 50–61.

[8]Alexandros Baka's and Antonis Machala's. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In Secure COMM 2019, pages 472–486, 2019.

[9] Antonis Michalas. The lord of the shares: combining attribute-based encryption and searchable encryption for flexible data sharing. In SAC 2019, pages 146–155, 2019

[10] G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "Idcrypt: A multi-user searchable symmetric encryption scheme for cloud applications," IEEE Access, vol. 6, pp. 2908–2921, 2018.