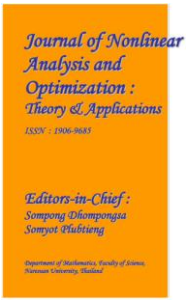
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



DUAL ACCESS CONTROL FOR CLOUD BASED DATA SHARING AND STORAGE

K. RAMBABU [1], B. LOKESH [2],

[1]**Assistant professor(HOD) , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-kattarambabudnr@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-lokeshboppe1215@gmail.com

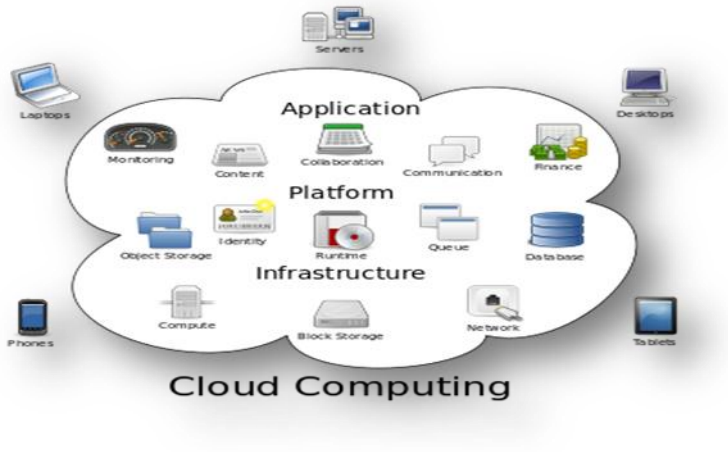
ABSTRACT

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.

1 INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

2 RELEATED WORK

Charm: a framework for rapidly prototyping cryptosystems

AUTHORS: Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin

We describe Charm, an extensible framework for rapidly prototyping cryptographic systems. Charm provides a number of features that explicitly support the development of new protocols, including support for modular composition of cryptographic building blocks, infrastructure for developing interactive protocols, and an extensive library of re-usable code. Our framework also provides a series of specialized tools that enable different cryptosystems to interoperate. We implemented over 40 cryptographic schemes using Charm, including some new ones that, to our knowledge, have never been built in practice. This paper describes our modular architecture, which includes a built-in benchmarking module to compare the performance of Charm primitives to existing C implementations. We show that in many cases our techniques result in an order of magnitude decrease in code size, while inducing an acceptable performance impact. Lastly, the Charm framework is freely available to the research community and to date, we have developed a large, active user base.

3 implementation study

Existing System:

- Antonis Michalas proposed a data sharing protocol that combines symmetric searchable encryption and ABE, which allows users to directly search over encrypted data. To implement the functionality of key revocation in ABE, the protocol utilizes SGX to host a revocation authority.

Disadvantages:

- The worry of security breach over outsourced data may be one of the main obstacles hindering Internet users from widely using cloud-based storage service.
- Apart from economic loss, unlimited download itself could open a window for network attackers to observe the encrypted download data that may lead to some potential information leakage (e.g., file size).

Proposed System & alogirtham

- In this project, we propose a new mechanism, dubbed dual access control, to tackle the existing system problem. To guarantee the confidentiality of outsourced data without loss of policy based access control, we start with a CP-ABE system, which is seen as one of the building blocks. We further employ an effective control over data users' download request on the top of the CP-ABE system. We design a new approach to avoid using the technique of "testing" ciphertext. Specifically, we allow data user to generate a download request. Upon receiving the download request, with help of the authority or the enclave of Intel SGX, a cloud server is able to check if the data user is authorized to gain access to the data. No other information is revealed to the cloud server except the knowledge of whether the user is authorized. Based on the above mechanism, the cloud maintains the control of the download request.

4.1 Advantages:

- Confidentiality of outsourced data
- Anonymity of data sharing
- Fine-grained access control over outsourced (encrypted) data
- Control over anonymous download request and EDoS attacks resistance
- High efficiency

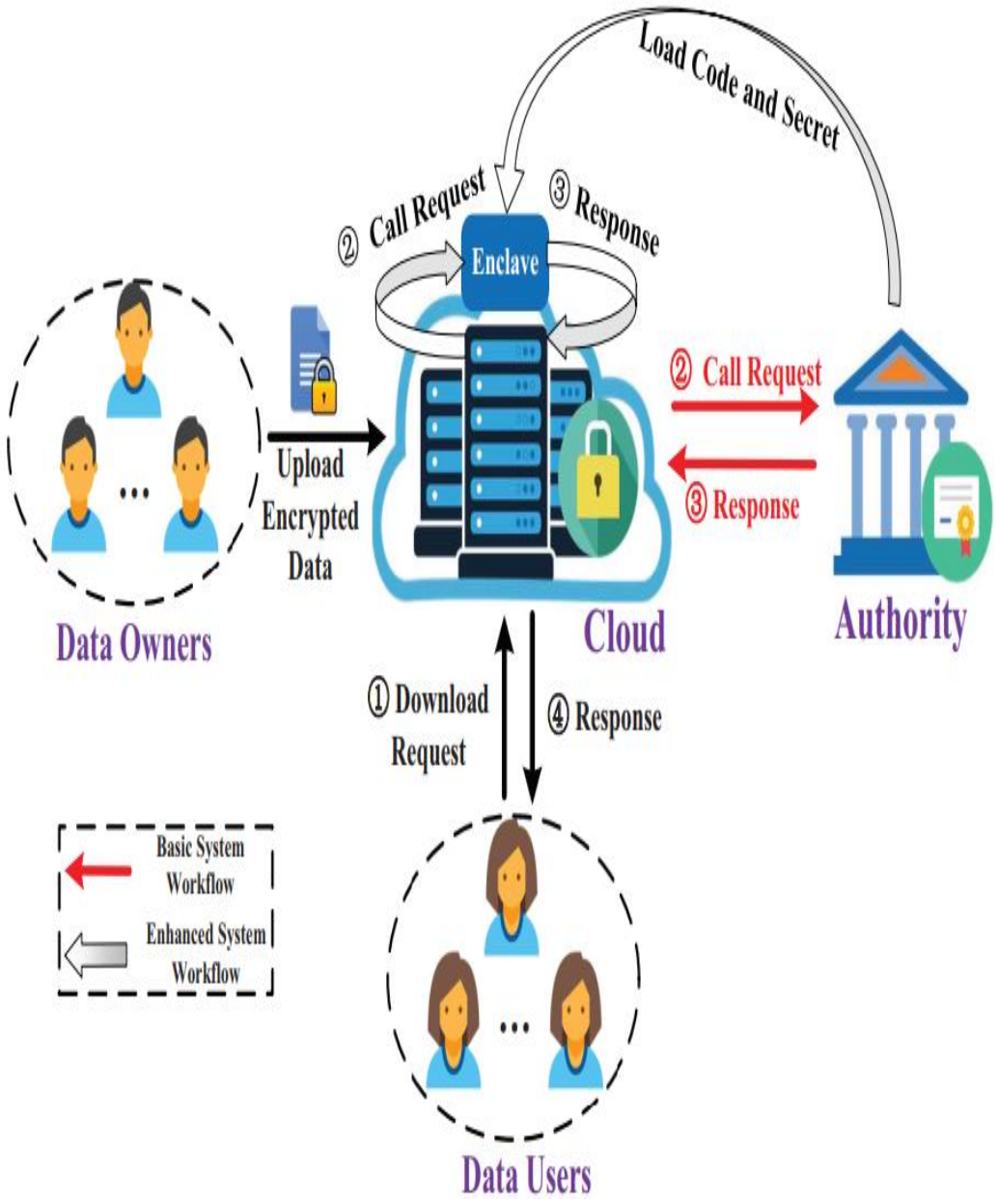


Fig1: SYSTEM ARCHITECTURE

4. IMPLEMENTATION

MODULES:

MODULES DESCRIPTION:

Data owner:

Data owner holds the data and wants to outsource his data to the cloud. In particular, data owners only want to share their data with those who satisfy certain conditions (e.g., student, professors or principal). They will be offline once their data have been uploaded to the cloud.

The Data Owner Module is a critical component in a dual access control system for cloud-based data sharing and storage. It empowers data owners with the ability to manage and control access to their data, ensuring that only authorized users can access sensitive information. This module typically includes the following functionalities:

1. Role Definition and Assignment

Role Creation: Allows data owners to create specific roles that correspond to different levels of access and responsibility within the organization.

Role Assignment: Enables the assignment of these roles to users, defining who has access to what data and what actions they can perform.

2. Access Control Management

Permission Settings: Provides data owners with the tools to set permissions for accessing, modifying, sharing, and deleting data.

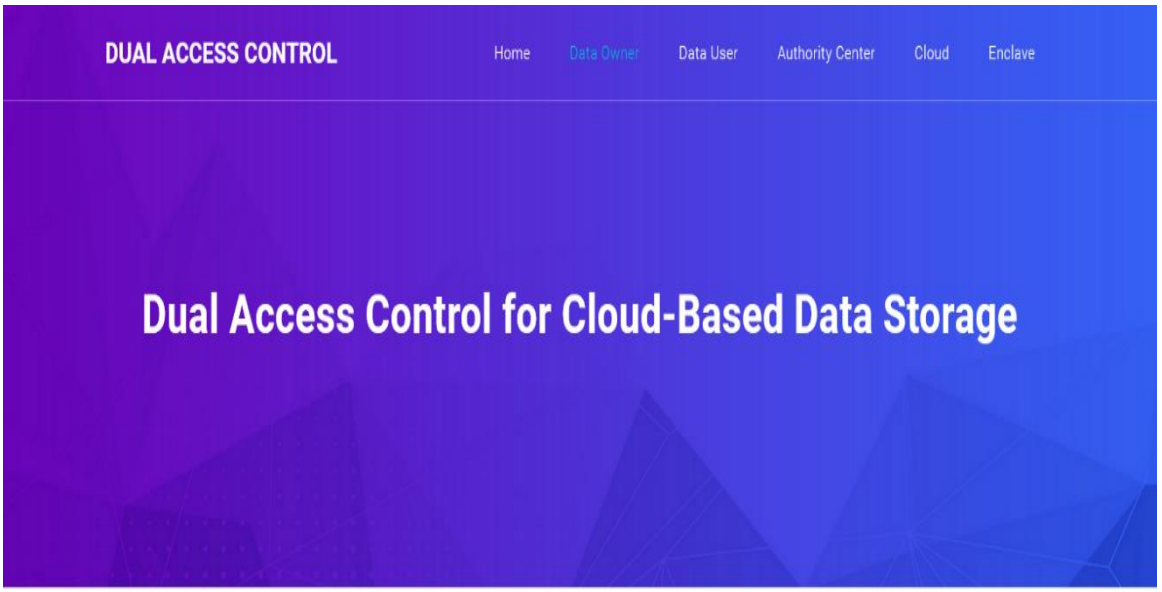
Access Policies: Enables the creation and enforcement of access policies based on roles, attributes, and conditions (e.g., time of access, location).

5 RESULTS AND DISCUSSION

SCREENSHORTS

5.3.1 HOME PAGE

Fig 5.1 HOME PAGE



5.3.2 DATA OWNER LOGIN

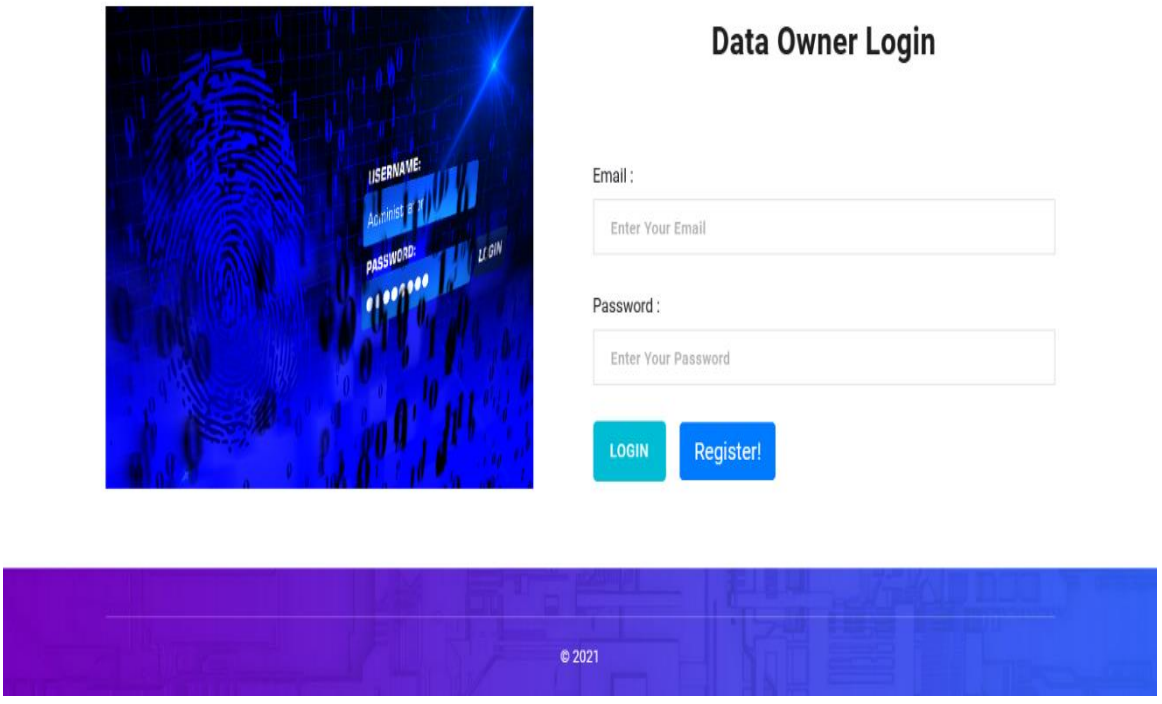
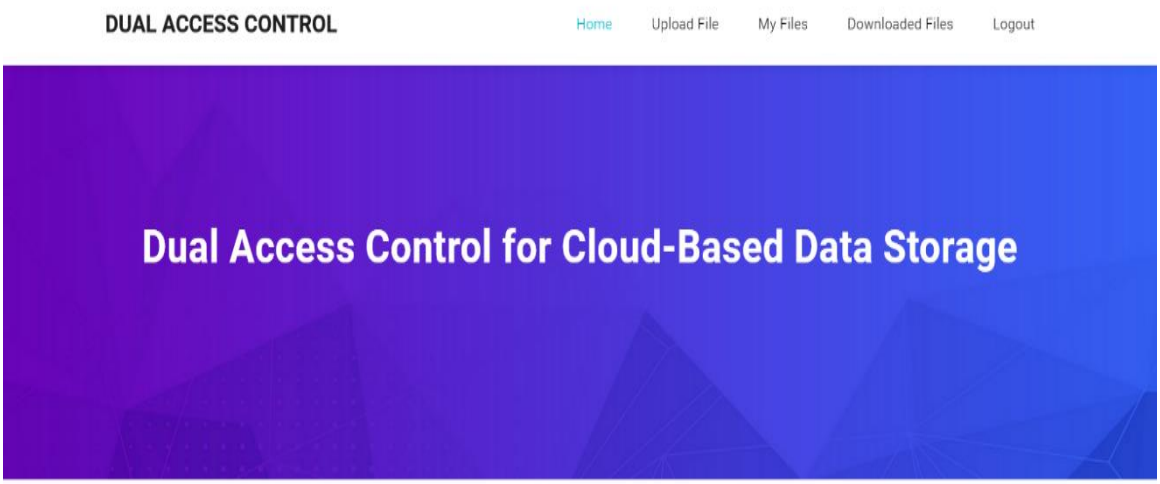
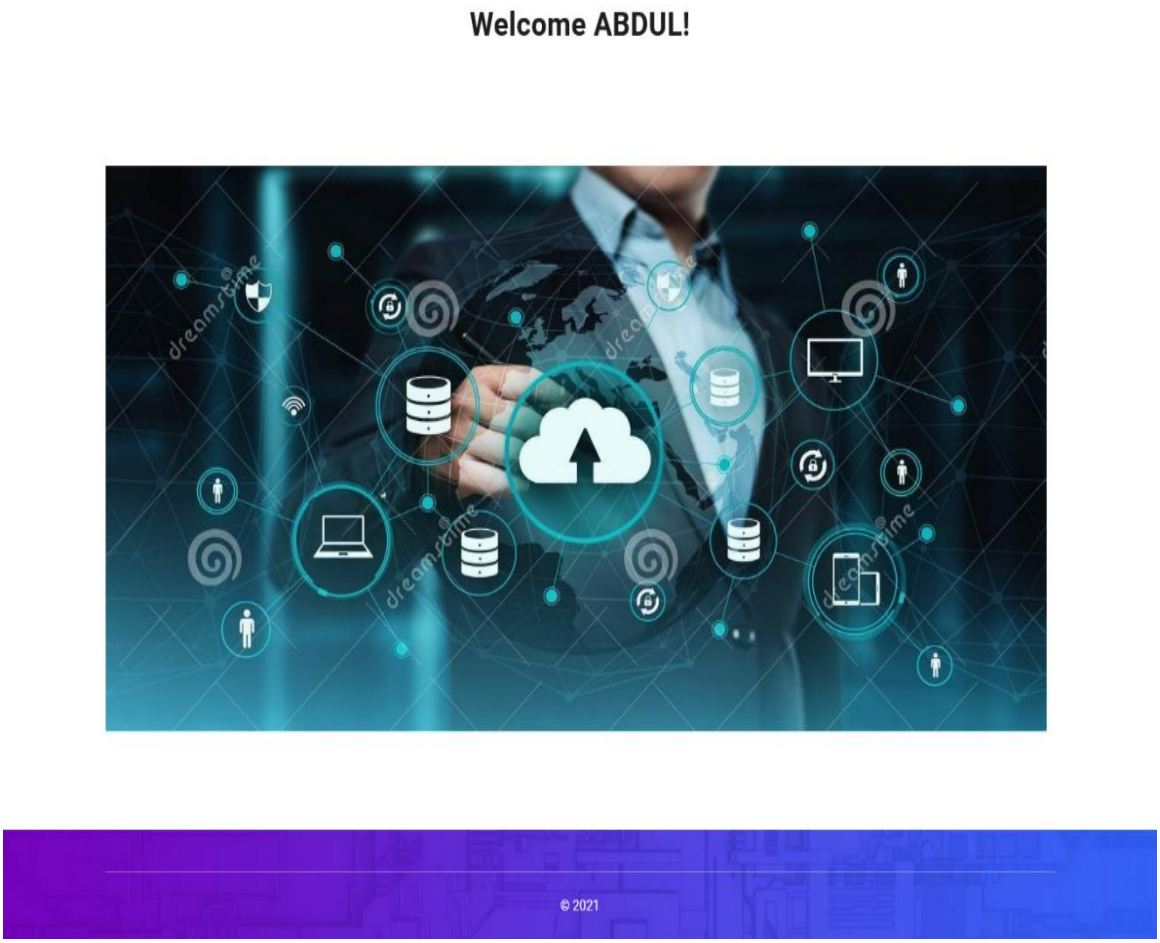


Fig 5.2 DATA OWNER LOGIN



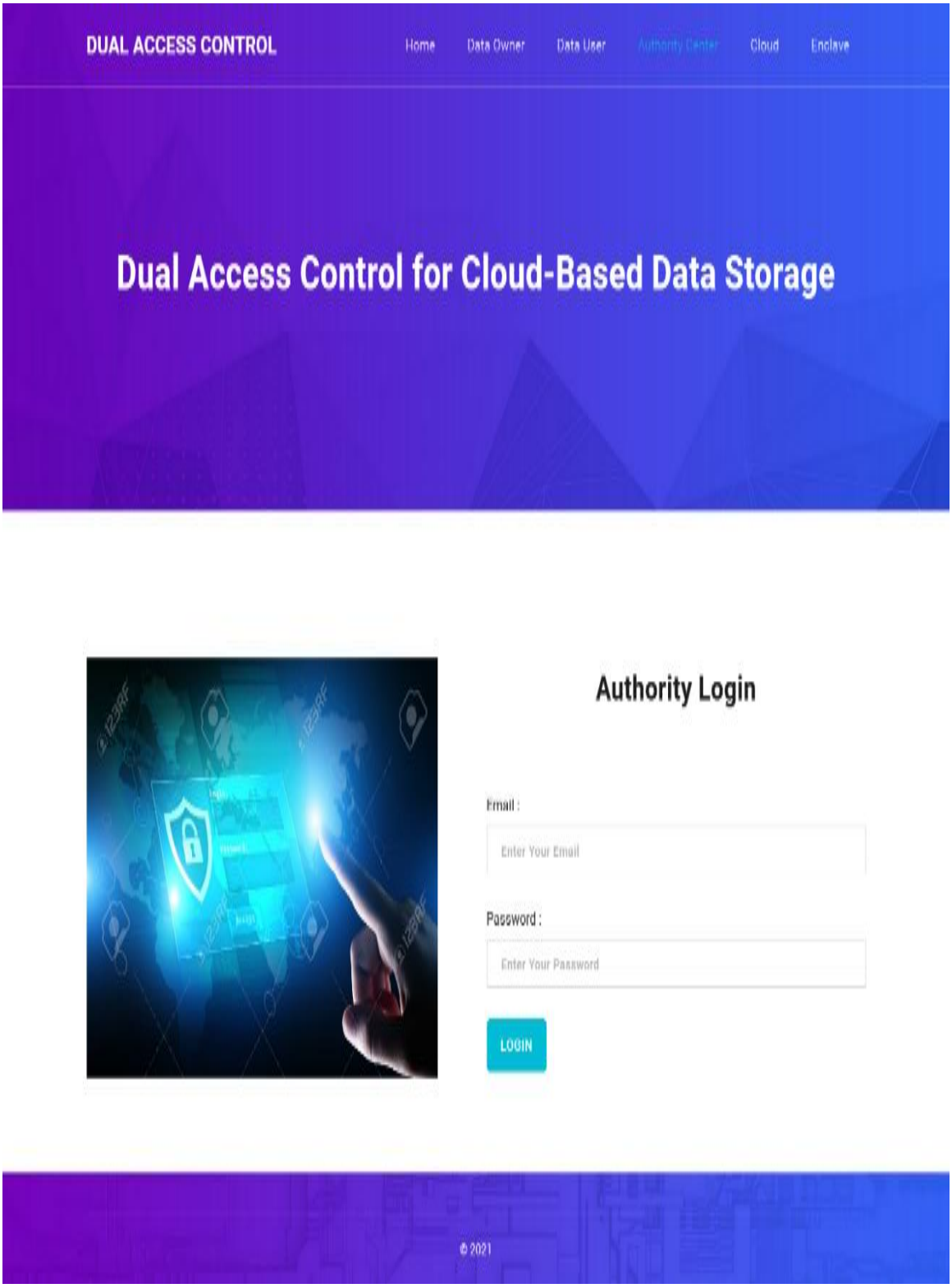
5.2.3



LOGIN

Fig 5.3 LOGIN COMPLETE

5.2.4



AUTHORITY LOGIN

Fig 5.4 AUTHORITY LOGIN

5.2.5 FILE UPLOAD

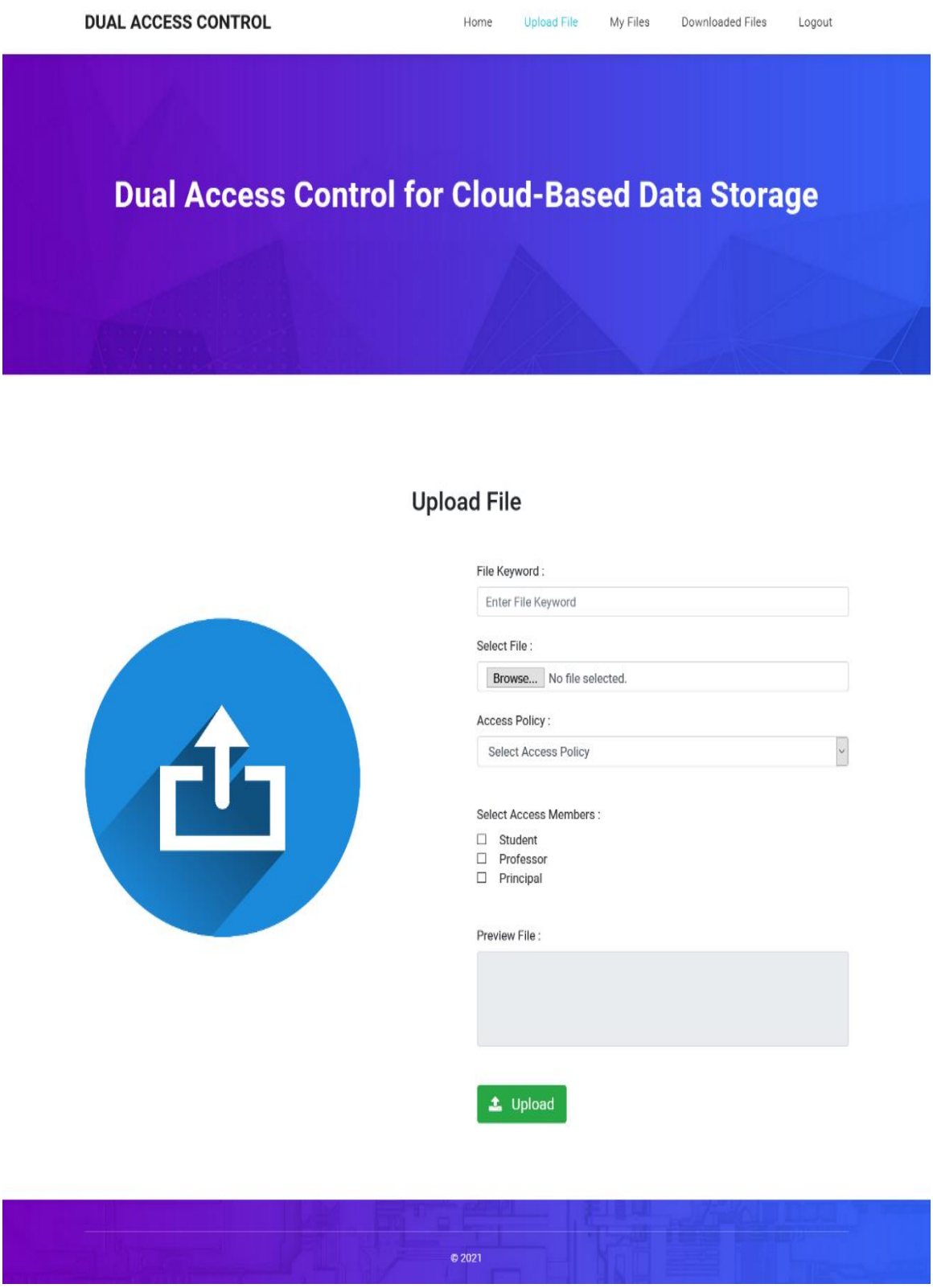


Fig 5.5 FILE UPLOAD

5.2.6 MY FILES

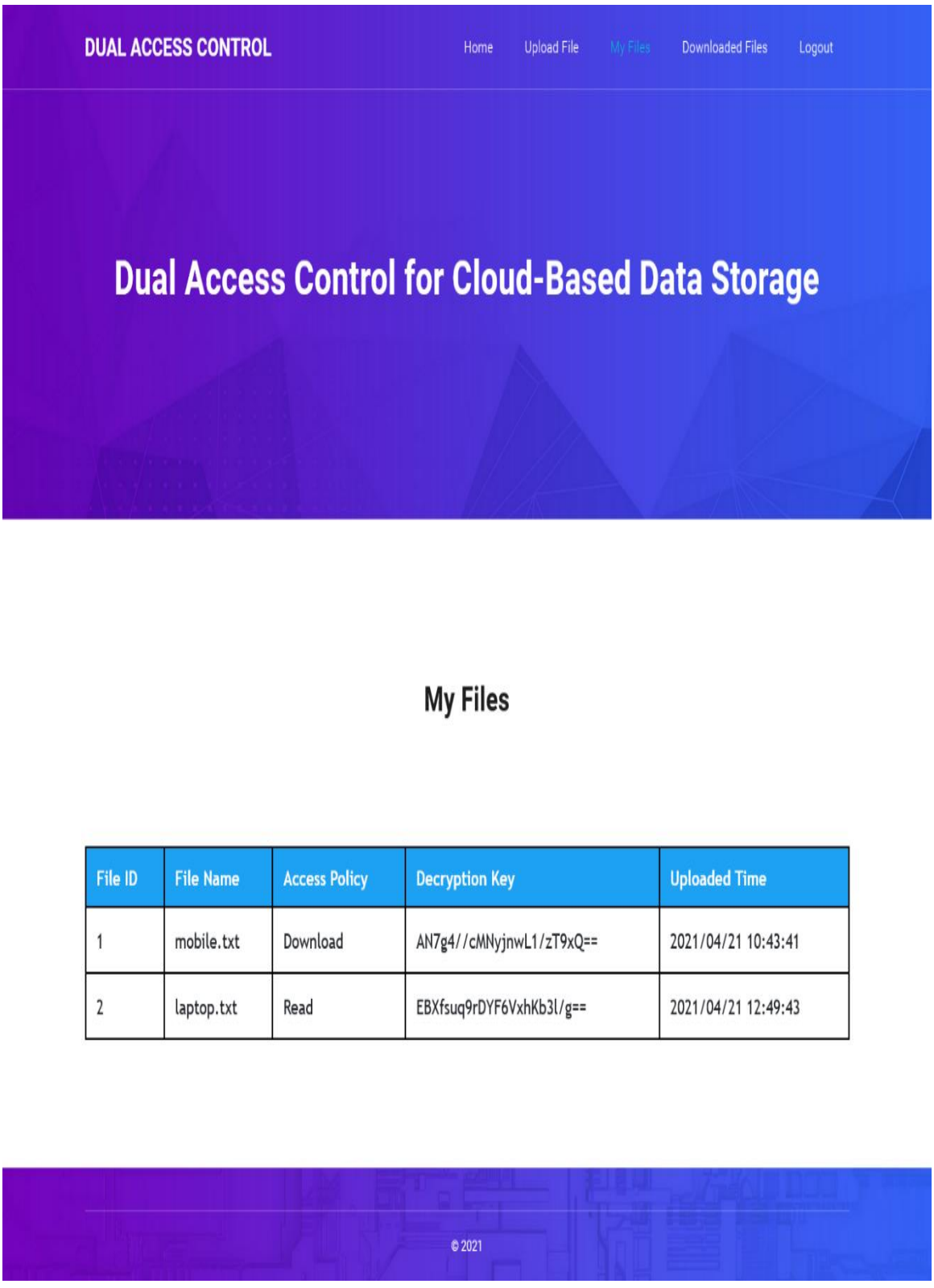
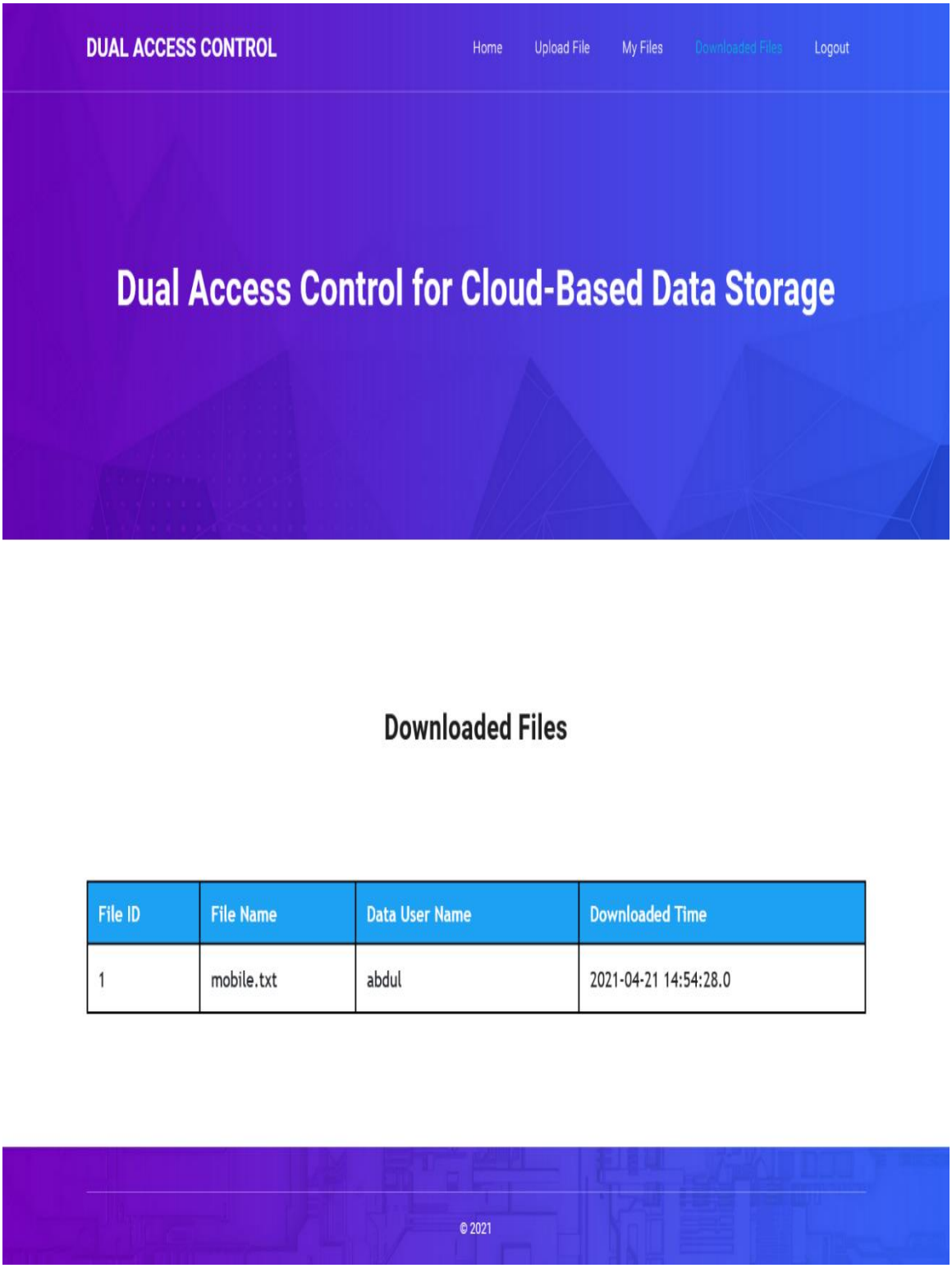


Fig 5.6 MY FILES

5.2.7



DOWNLOADED FILES

Fig 5.7 DOWNLOADED FILES

5.2.8 ALL FILES

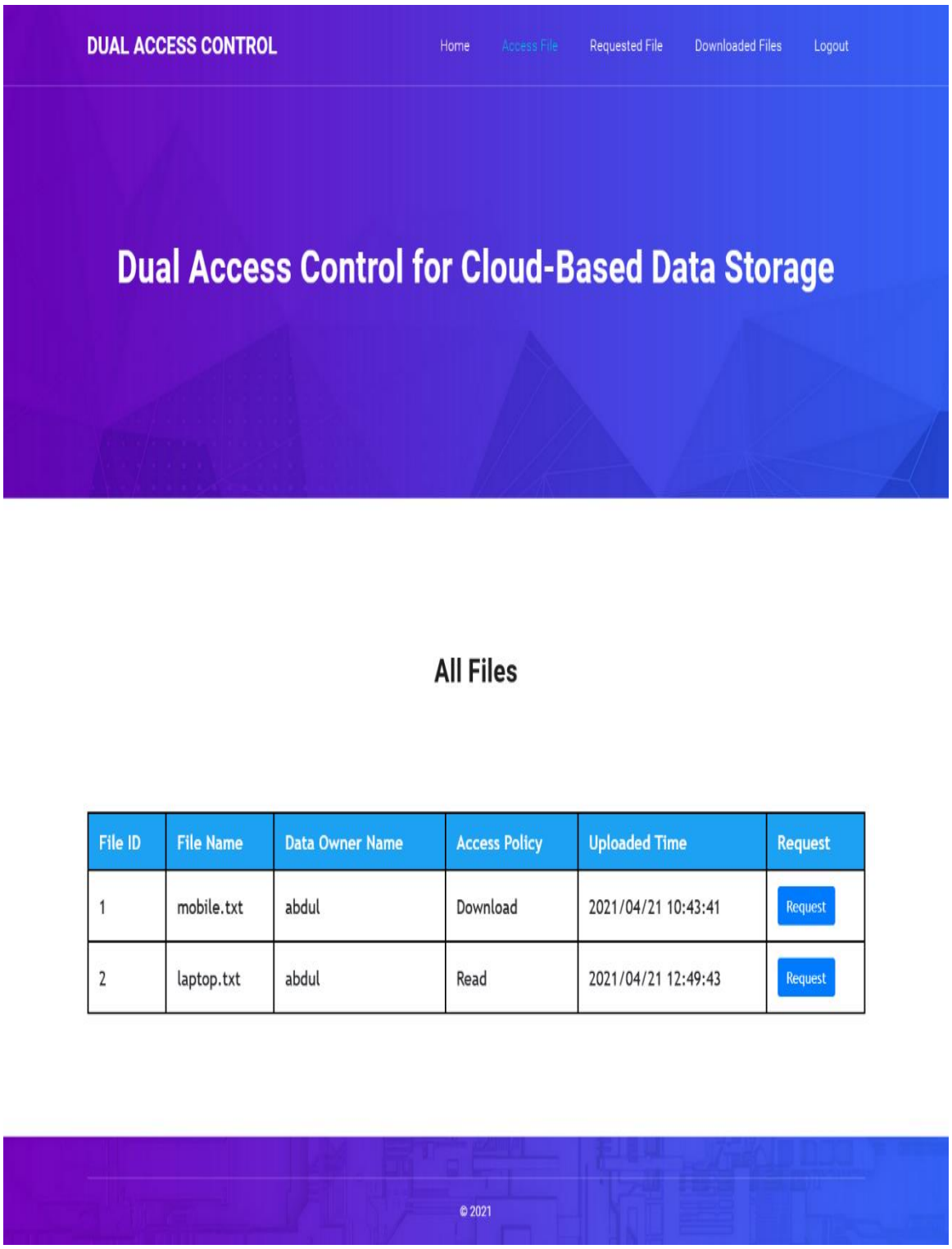
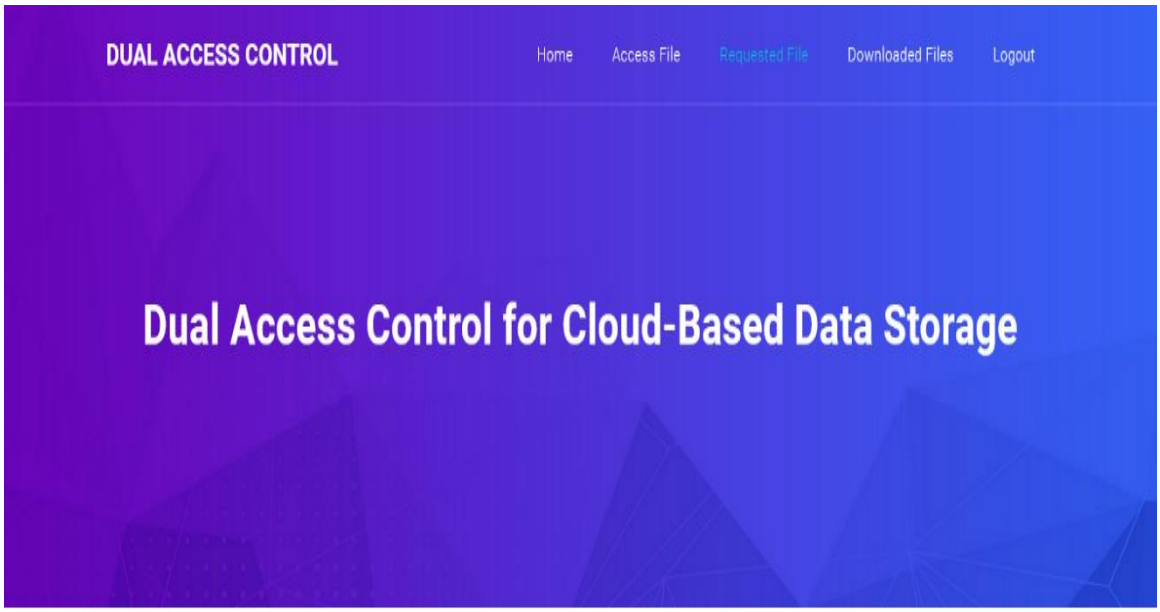


Fig 5.8 ALL FILES

5.2.9 REQUESTED FILES

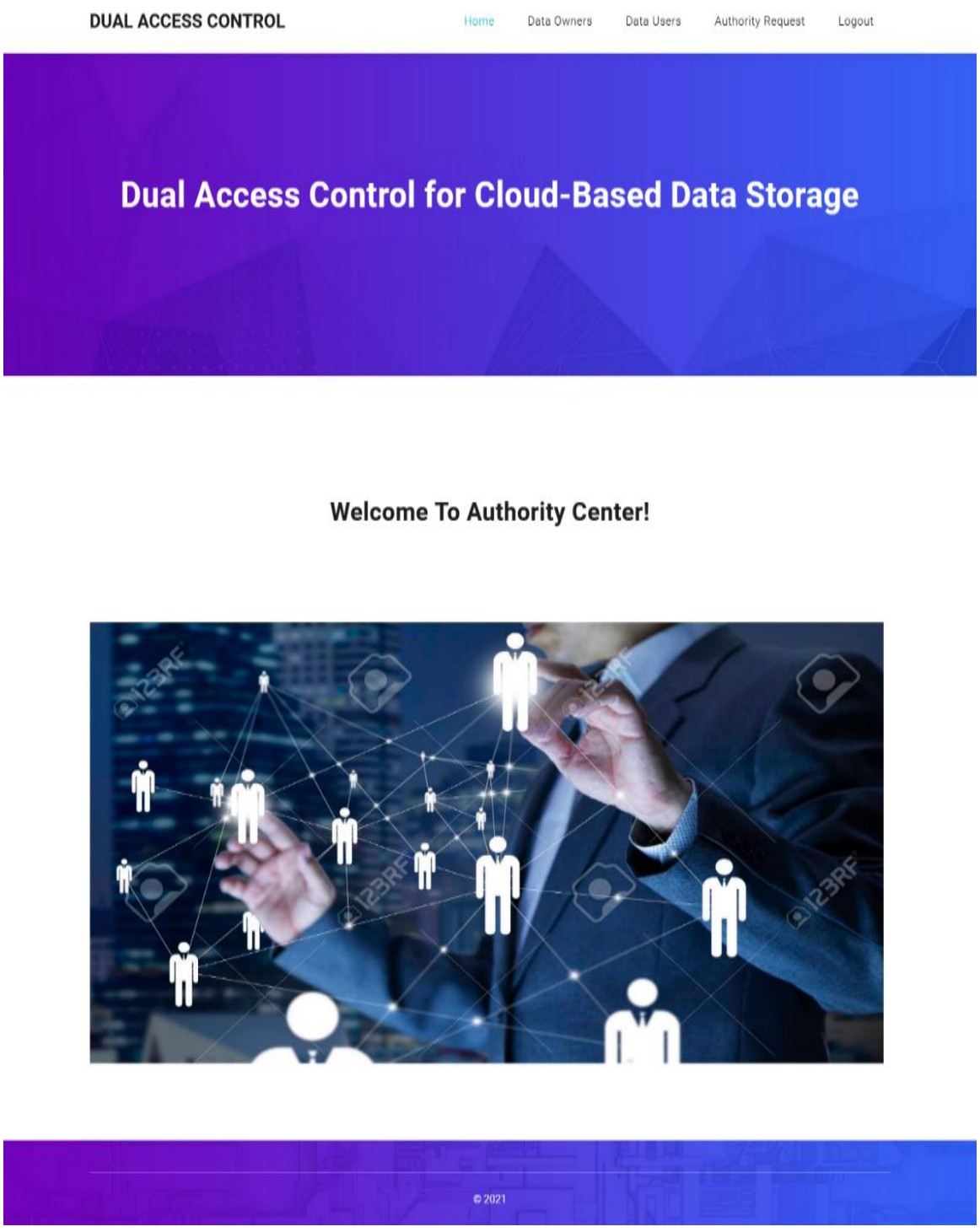
Fig 5.9



Requested Files

File ID	File Name	Authority Status	Enclave Status	Requested Time	Request
1	mobile.txt	Approved	Approved	2021/04/21 11:52:50	Download
2	laptop.txt	Approved	Approved	2021/04/21 14:55:34	Download

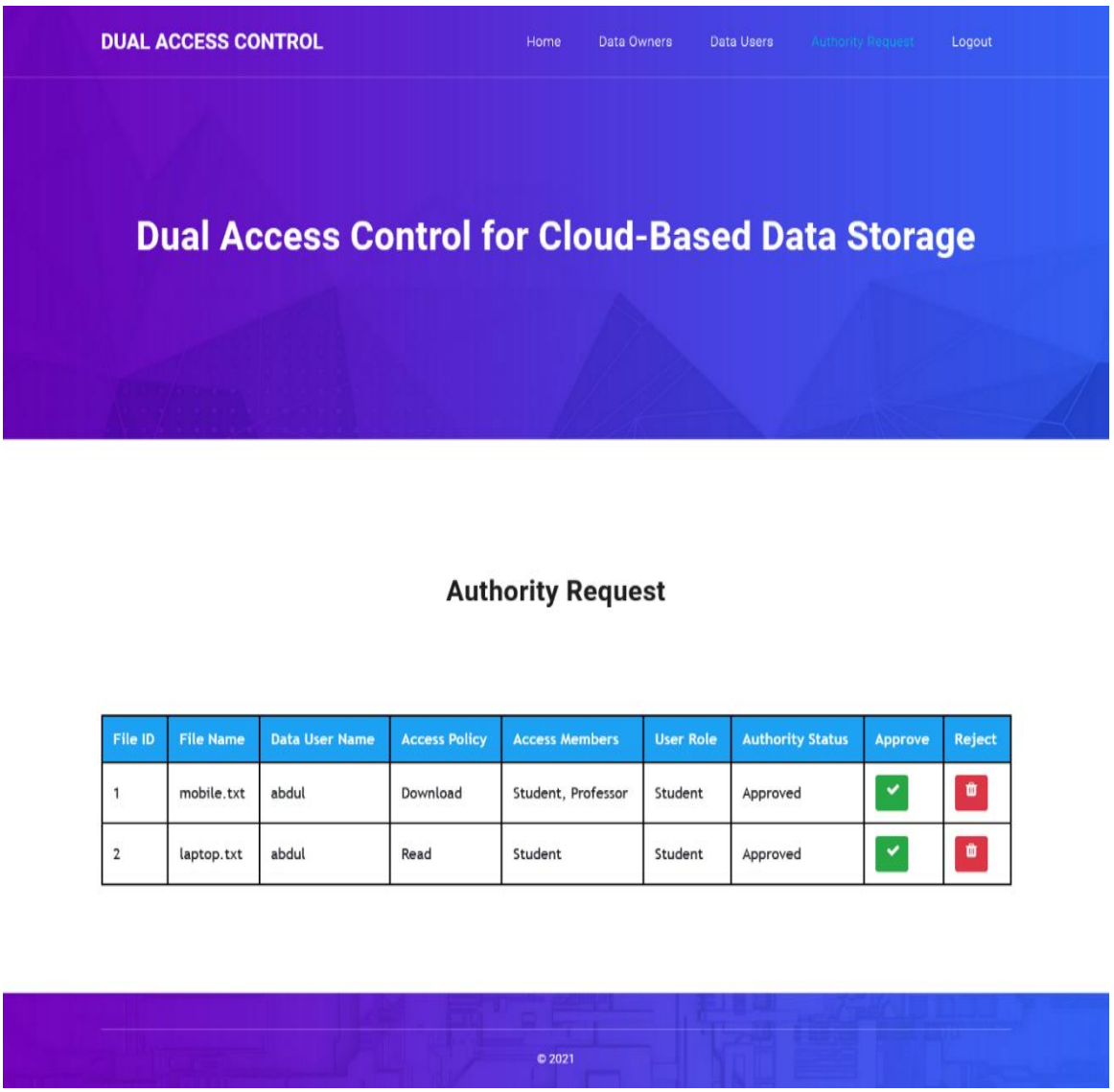
REQUESTED FILES



5.2.10 AUTHORITY CENTRE

Fig 5.10 AUTHORITY CENTRE

5.2.11

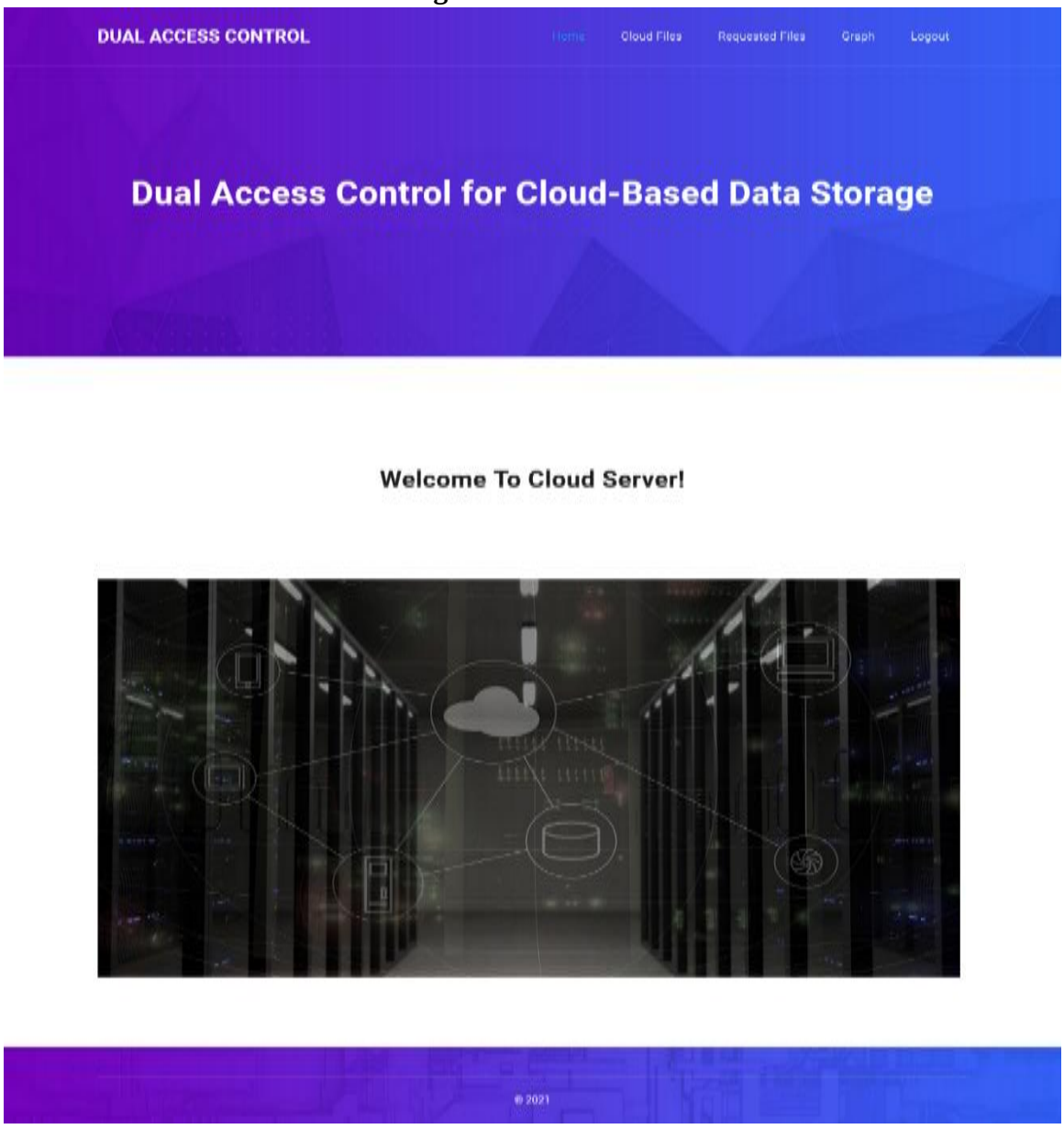


AUTHORITY REQUEST

Fig 5.11 AUTHORITY REQUEST

5.2.12 CLOUD SERVER

Fig 5.11 CLOUD SERVER



5.2.13 CLOUD FILES

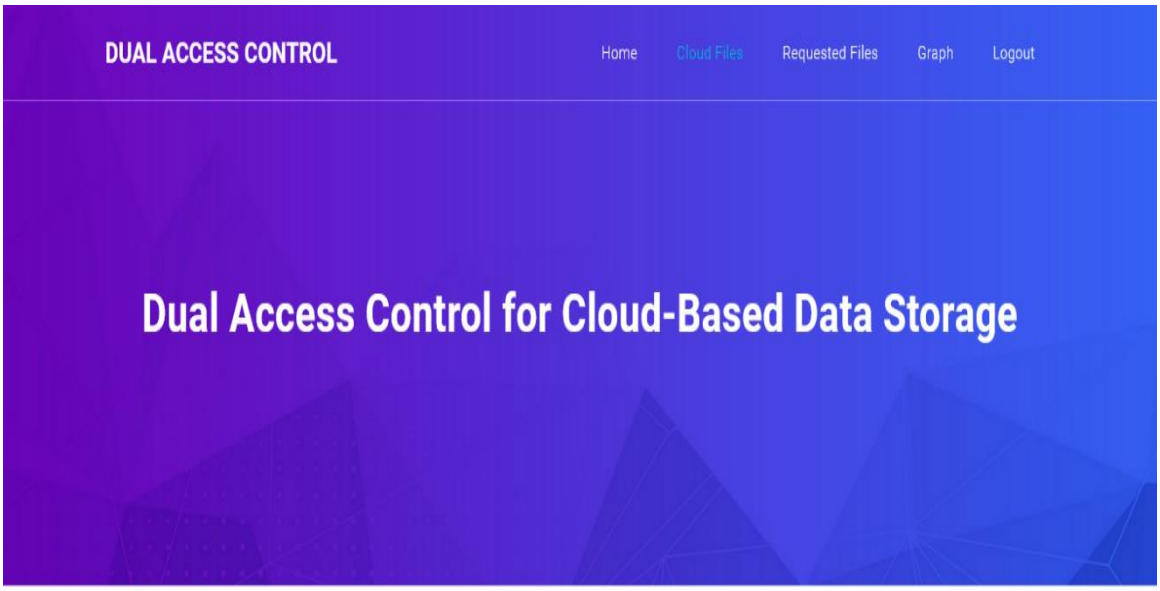


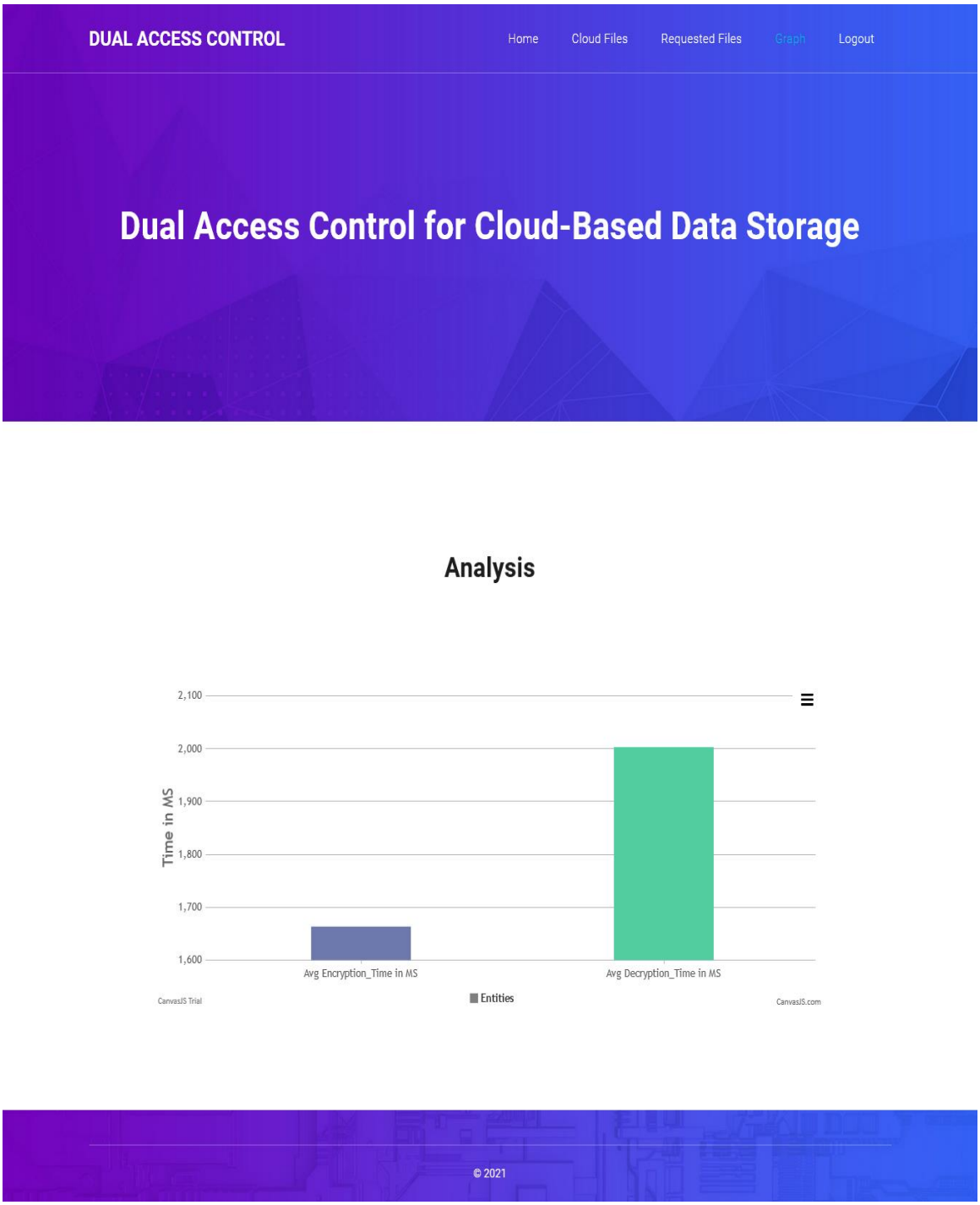
Fig 5.12 CLOUD FILES

Cloud Files

File ID	File Name	Access Policy	Access Members	Uploaded Time
1	mobile.txt	Download	[Student, Professor]	2021/04/21 10:43:41
2	laptop.txt	Read	[Student]	2021/04/21 12:49:43

5.2.14 ANALYSIS

Fig 5.14



ANALYSIS

6.1 CONCLUSION

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 amounts of its 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. 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.

7. REFRENCES

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.

[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.

[4] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[5] John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

[6] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.

[7] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.