

PRIVACY PROTECTION BASED ACCESS CONTROL SCHEME IN CLOUD BASED SERVICES

K. Rambabu ¹, B. Sudha,

¹**Assistant professor(HOD) , PG DEPT, Dantuluri Narayana Raju College, Bhimavaram, Andhrapradesh**

Email:- kattarambabudnr@gmail.com

²**PG Student of MCA, Dantuluri Narayana Raju College, Bhimavaram, Andharapradesh**

Email:- sudhabonam13@gmail.com

ABSTRACT

With the rapid development of the computer technology, cloud-based services have become a hot topic. Cloud based services not only provide users with convenience, but also bring many security issues. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature (IABS) which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based service.

1 INTRODUCTION

With the rapid development of cloud computing, big data and public cloud services have been widely used. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, we need to develop an effective access control solution. Since the traditional access control strategy cannot effectively solve the security problems that exist in data sharing. Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed. In 2007, Bethencourt et al. first proposed the ciphertext policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. In 2011, Hur et al. put

forward a fine-grained revocation scheme but it can easily cause key escrow issue. Lewko et al. used multi authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not flexible. Li et al presented data sharing scheme based on systemic attribute encryption, which endows different users' different access rights. But it is not efficient from the complexity and efficiency.

Literature Survey

Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

With the rapid development of cloud computing, big data and public cloud services have been widely used. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. Therefore, we need to develop an effective access control solution. Since the traditional access control strategy cannot effectively solve the security problems that exist in data sharing. Data security issues brought by data sharing have seriously hindered the development of cloud computing.

Disadvantages:

1. Compared with the MAH-ABE scheme which does not refer to the write access control, we exploit an Improved Attribute-based Signature (IABS) scheme to enforce write access control in the PSD. In this way, the user can pass the cloud server's signature verification without disclosing the identity, and successfully modify the file.
 2. In Chen's MAH-ABE scheme, the CP-ABE is used to achieve the read access permission, but there are some defects to be considered.
-

Proposed System & algoriththam

We propose a novel access control system called PSACS, which is privilege separation based on privacy protection. The system uses Key-Aggregate Encryption (KAE) scheme and Hierarchy Attribute-based Encryption (HABE) scheme to implement read access control scheme in the PSD and PUD respectively. The KAE scheme greatly improves access efficiency and the HABE scheme largely reduces the task of a single authority and protects the privacy of user data.

4.1 Advantages:

1. We provide a thorough analysis of security and complexity of our proposed PS-ACS scheme. The functionality and simulation results provide data security in acceptable performance impact, and prove the feasibility of the scheme.
2. we proposed the write access permission in the PSD. For the user, the public key and file class label are all known, we can implement the algorithm to encrypt the files after he modified, and then upload them to the cloud.

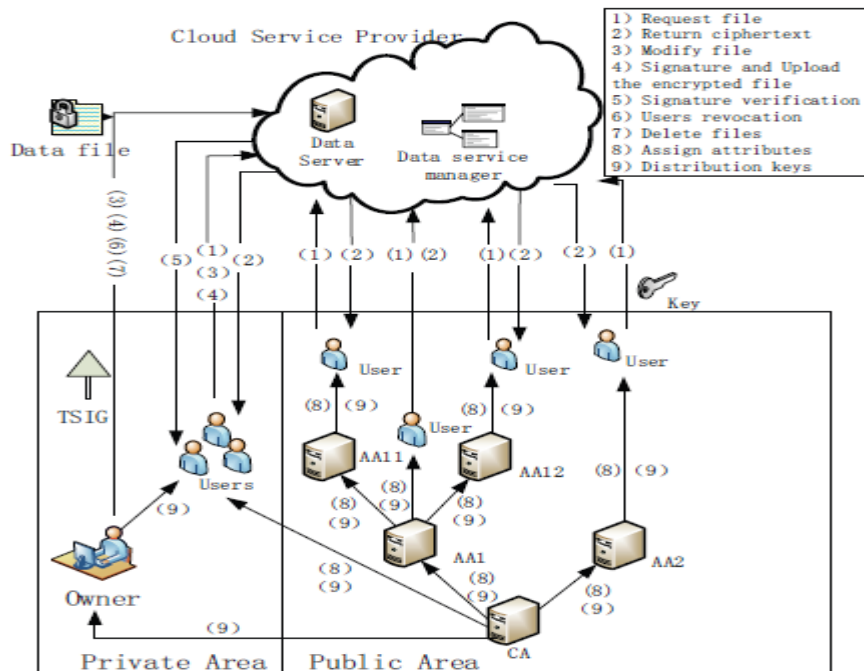


Fig:3.1 System Architecture

IMPLEMENTATION

Modules:

Data owner:

Data Owner, based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server.

CSP:

The cloud service provider consists of two parts: data storage server and data service management. Data storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding cipher text.

CA manages multiple AA, and AA each manages attributes in their own field. The attributes owned by the user are issued by different authority.

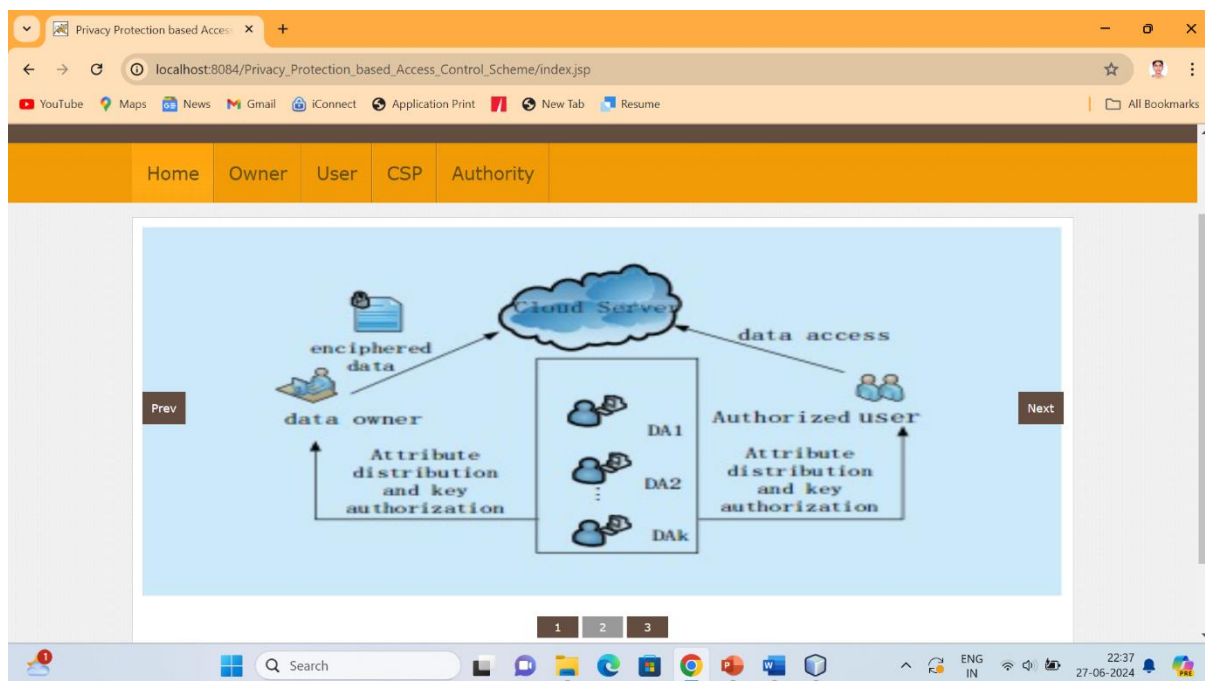
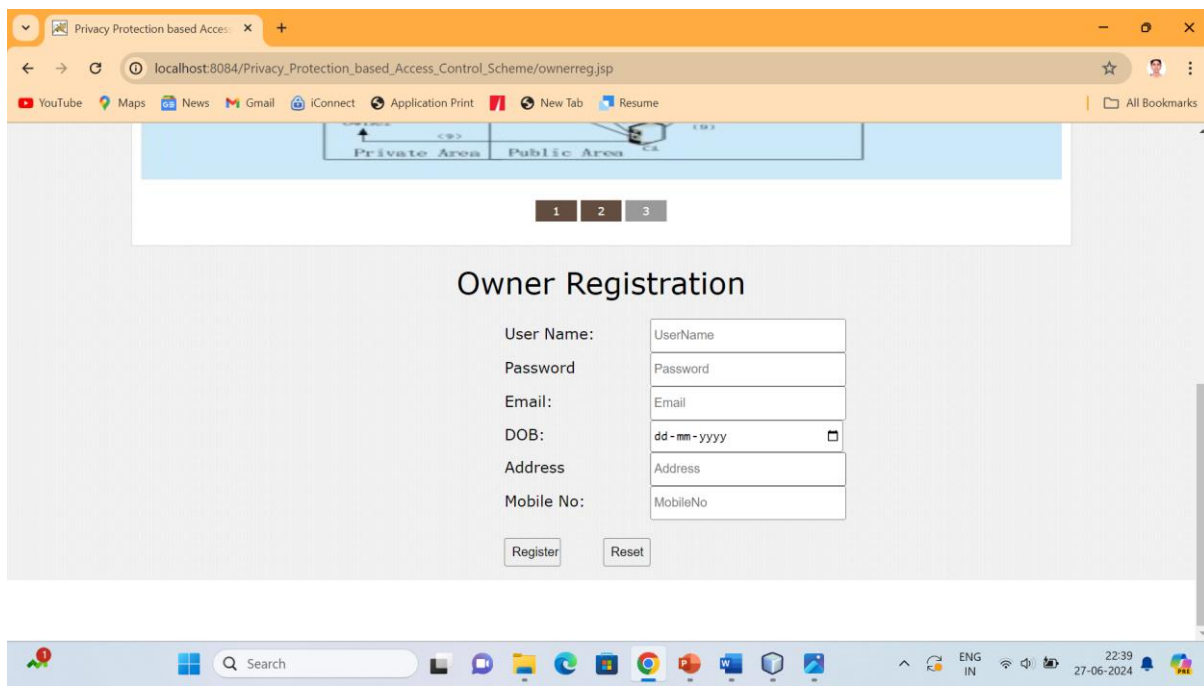
5 RESULTS AND DISCUSSION**SCREENSHOTS**

Fig 5.1

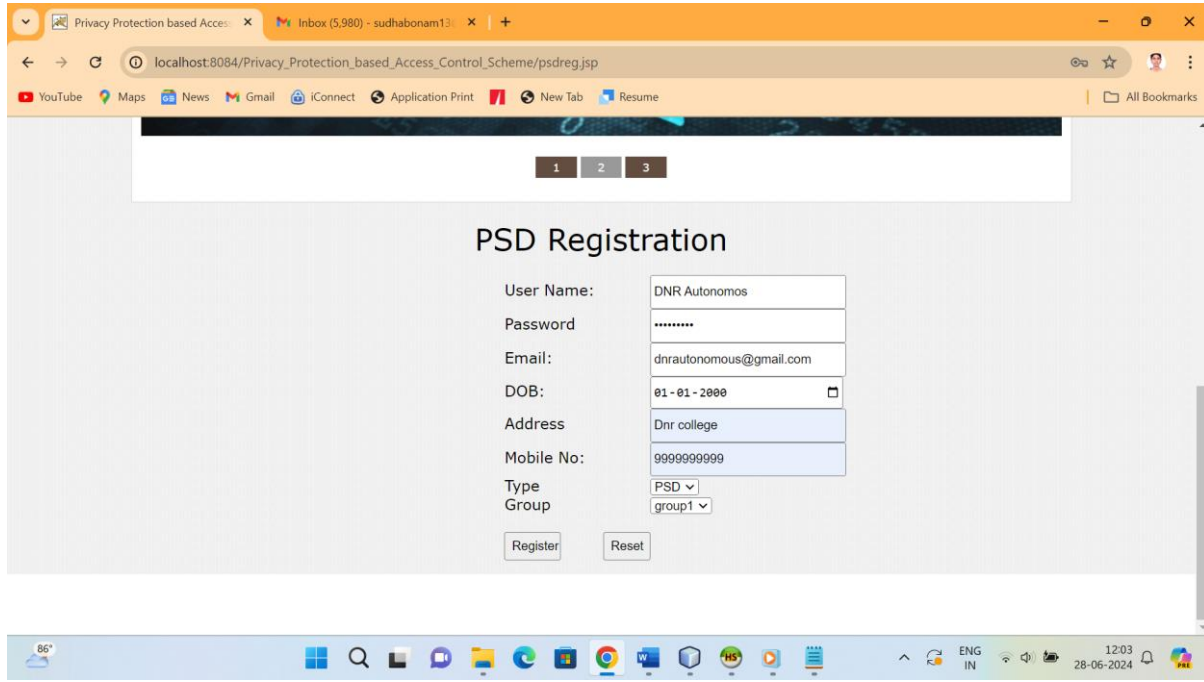
Once you run the project, home page will display like this.



The screenshot shows a web browser window with the address bar displaying 'localhost:8084/Privacy_Protection_based_Access_Control_Scheme/ownerreg.jsp'. The page features a navigation bar with 'Private Area' and 'Public Area' links. Below the navigation bar is a tabbed interface with three tabs labeled '1', '2', and '3'. The main content area is titled 'Owner Registration' and contains a form with the following fields: 'User Name:' (UserName), 'Password' (Password), 'Email:' (Email), 'DOB:' (dd-mm-yyyy), 'Address' (Address), and 'Mobile No:' (MobileNo). There are 'Register' and 'Reset' buttons at the bottom of the form. The Windows taskbar at the bottom shows the date as 27-06-2024 and the time as 22:39.

Fig 5.2

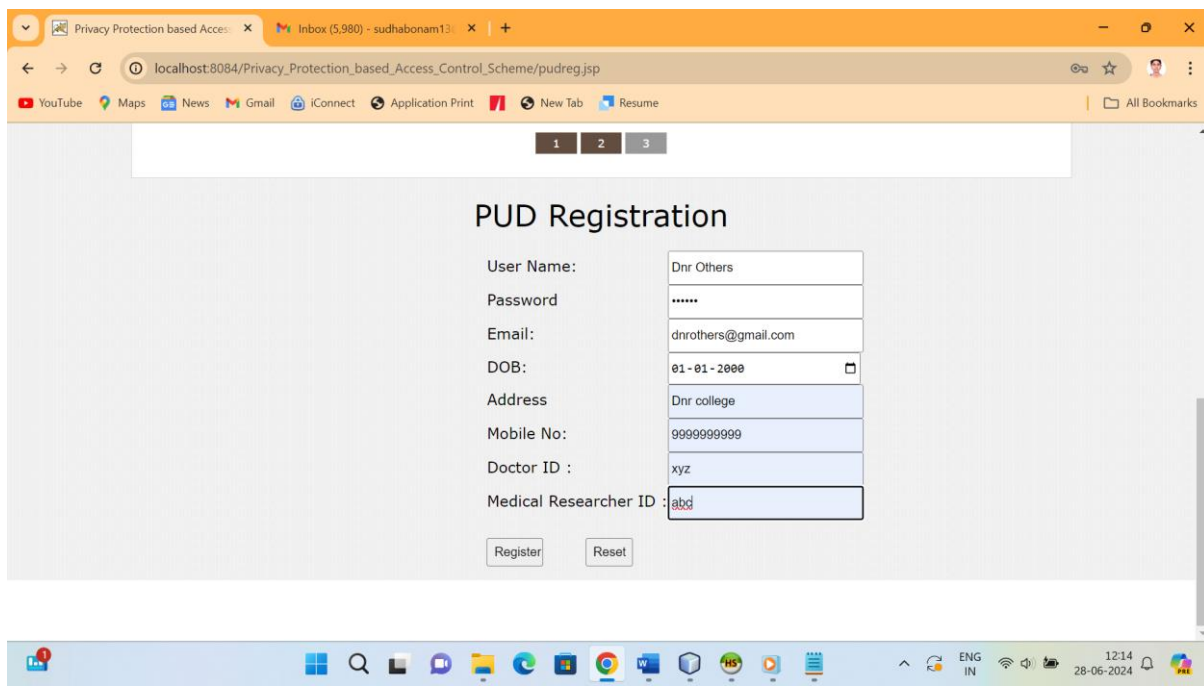
If you enter into the Owner tab, its shows two options login for already registered users and new registration form for new users.



The screenshot shows a web browser window with the address bar displaying 'localhost:8084/Privacy_Protection_based_Access_Control_Scheme/psdreg.jsp'. The page features a navigation bar with 'Private Area' and 'Public Area' links. Below the navigation bar is a tabbed interface with three tabs labeled '1', '2', and '3'. The main content area is titled 'PSD Registration' and contains a form with the following fields: 'User Name:' (DNR Autonomos), 'Password' (*****), 'Email:' (dnrautonomous@gmail.com), 'DOB:' (01-01-2000), 'Address' (Dnr college), 'Mobile No:' (9999999999), 'Type' (PSD), and 'Group' (group1). There are 'Register' and 'Reset' buttons at the bottom of the form. The Windows taskbar at the bottom shows the date as 28-06-2024 and the time as 12:03.

Fig 5.3

If you enter into the user tab, there are two types of users present, Personal User(PSD) and Public User(PUD). For PSD you can register with required credentials.



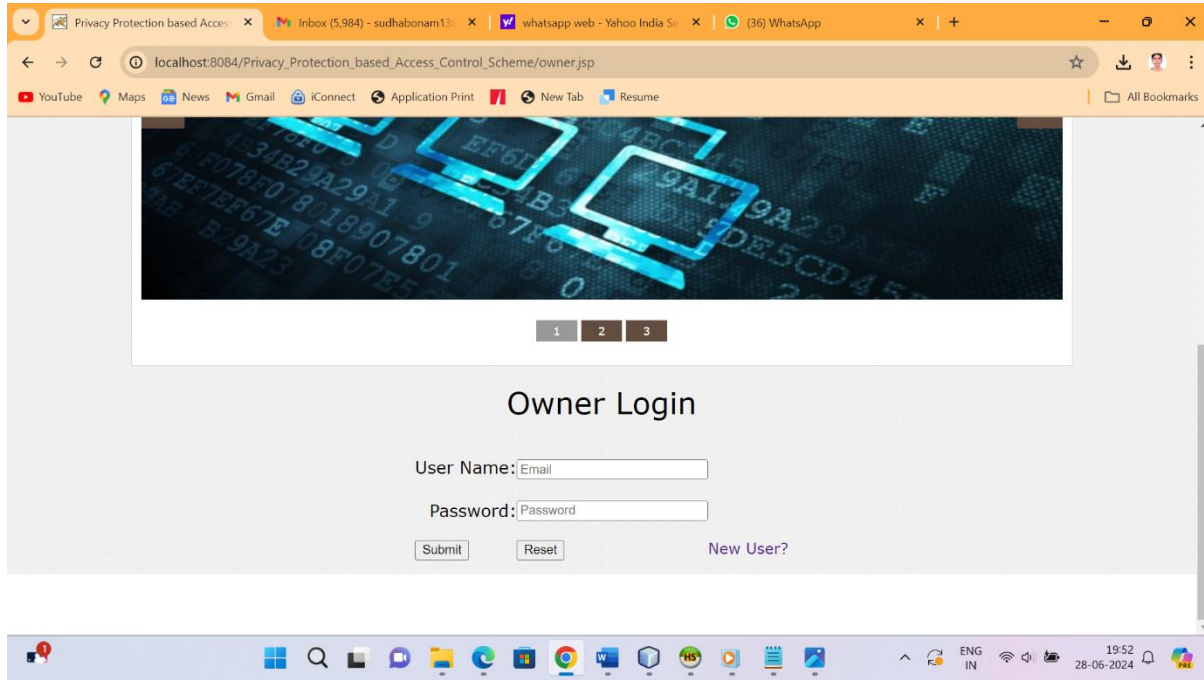
The screenshot shows a web browser window with the address bar displaying 'localhost:8084/Privacy_Protection_based_Access_Control_Scheme/pudreg.jsp'. The page title is 'PUD Registration'. The form contains the following fields and values:

Field	Value
User Name:	Dnr Others
Password	*****
Email:	dnrothers@gmail.com
DOB:	01-01-2000
Address	Dnr college
Mobile No:	9999999999
Doctor ID :	xyz
Medical Researcher ID :	abc

At the bottom of the form are two buttons: 'Register' and 'Reset'.

Fig 5.4

For Public domain users (PUD) also you can register with required credentials.
Once you successfully registered, you can login to this domain.



The screenshot shows a web browser window with the address bar displaying 'localhost:8084/Privacy_Protection_based_Access_Control_Scheme/owner.jsp'. The page features a header image with a blue and black background and white text. Below the image, the title 'Owner Login' is displayed. The form contains the following fields and values:

Field	Value
User Name:	Email
Password:	Password

At the bottom of the form are two buttons: 'Submit' and 'Reset'. To the right of the 'Reset' button is a link labeled 'New User?'.

Fig 5.5

Once you completed Owner registration , you can login with your valid credentials.

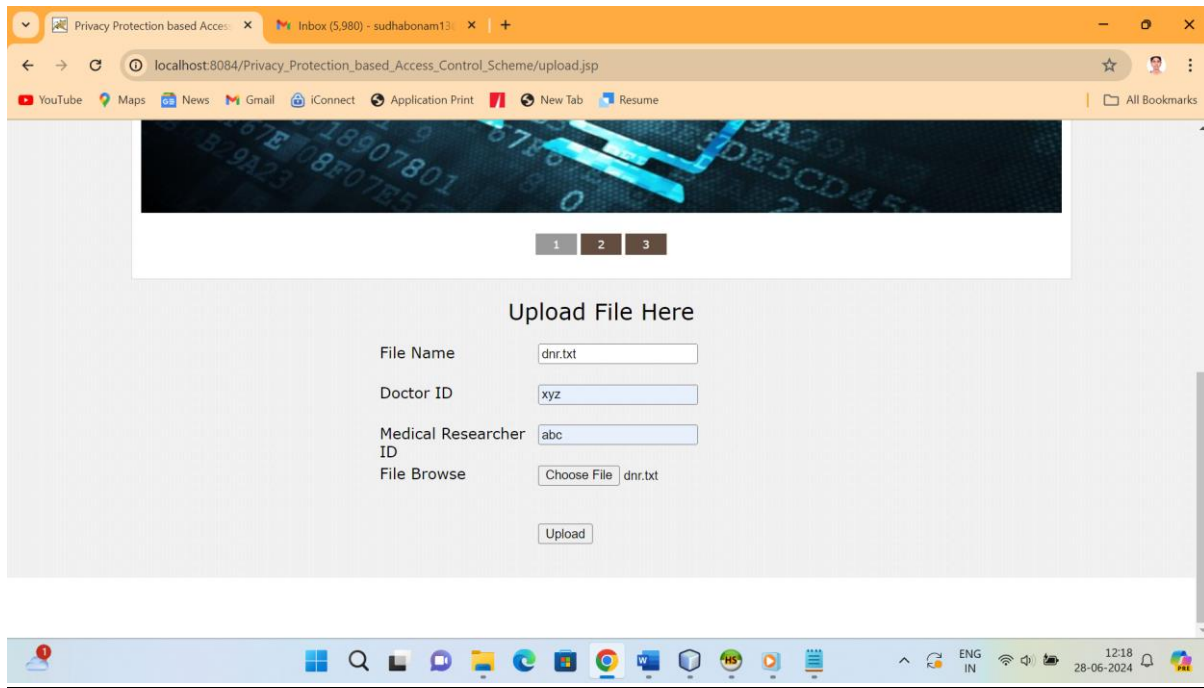


Fig 5.6

Once you login into the owner tab, you can upload your files or folders.

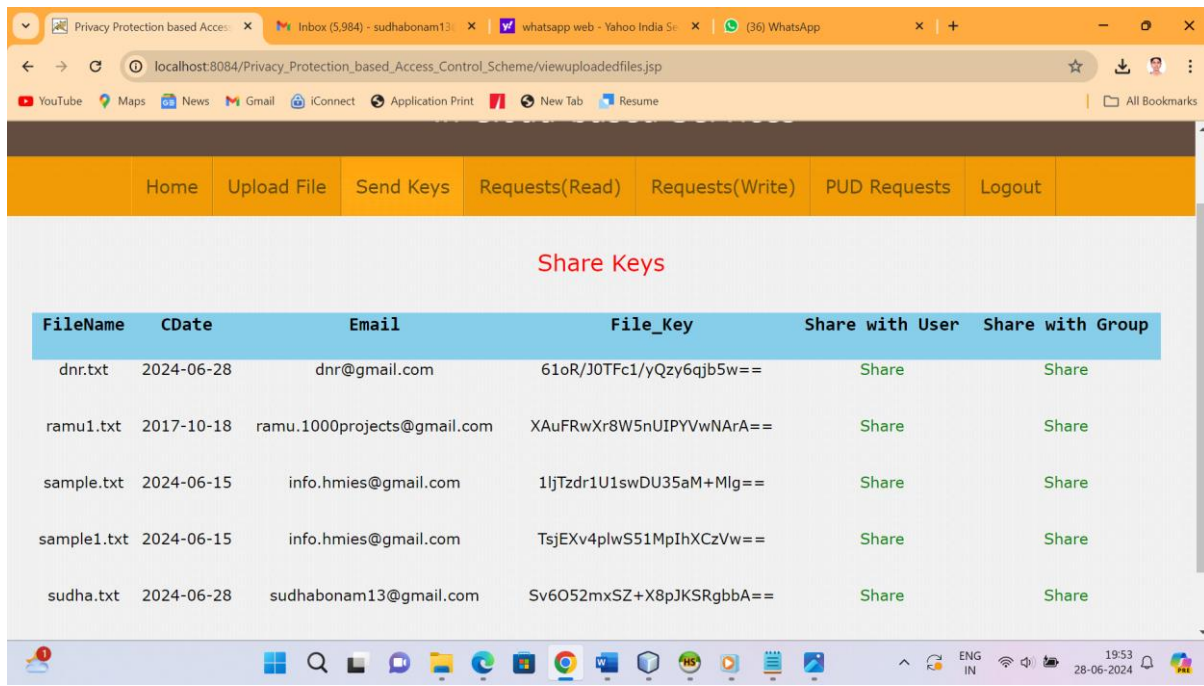


Fig 5.7

Once you upload the file, you can share with authorised persons.

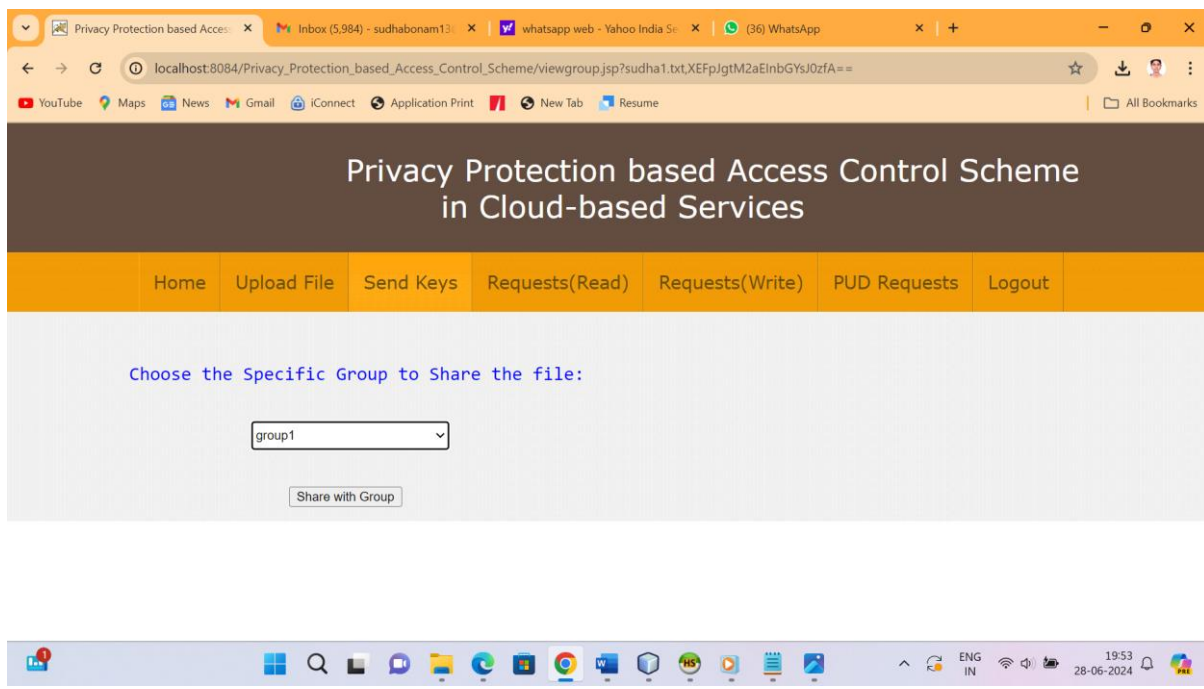


Fig 5.8

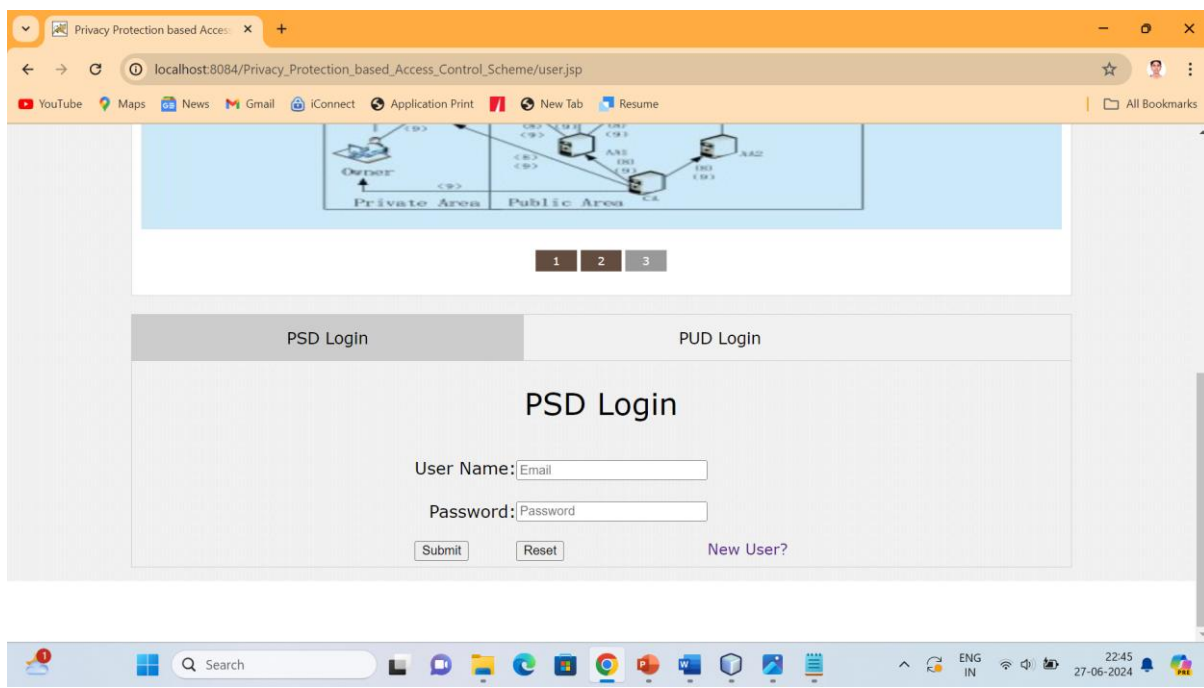


Fig 5.9

You can login into the personal user domain with valid credentials.

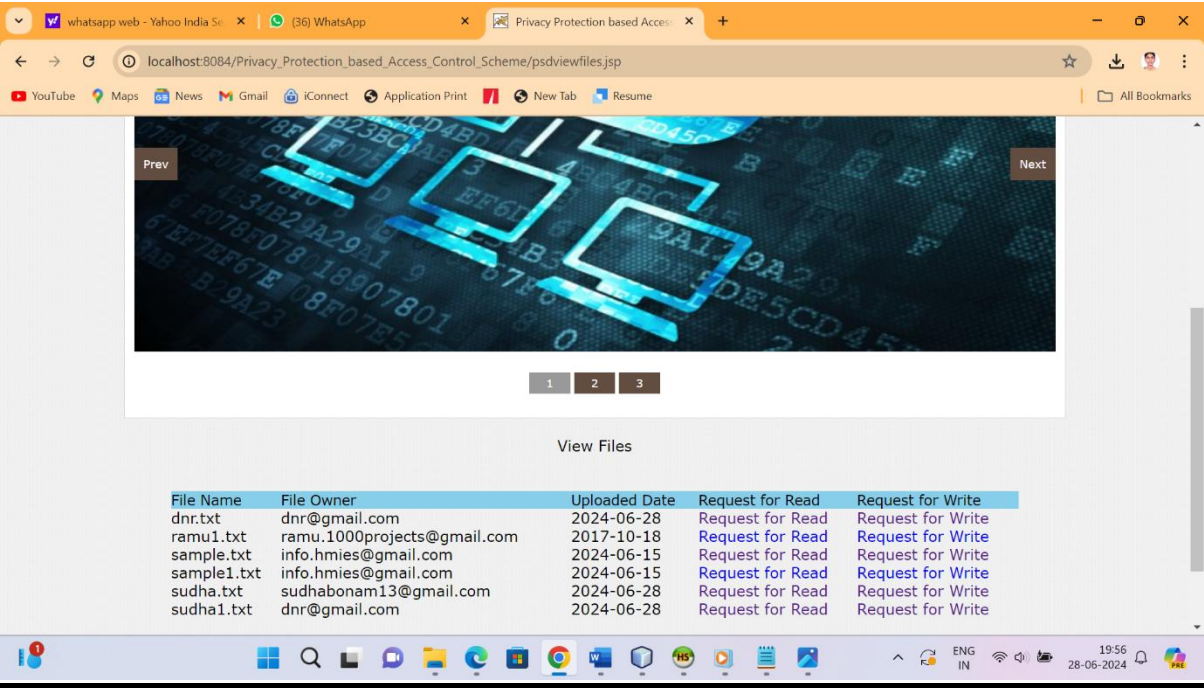


Fig 5.10

You can raise requests for read and write.

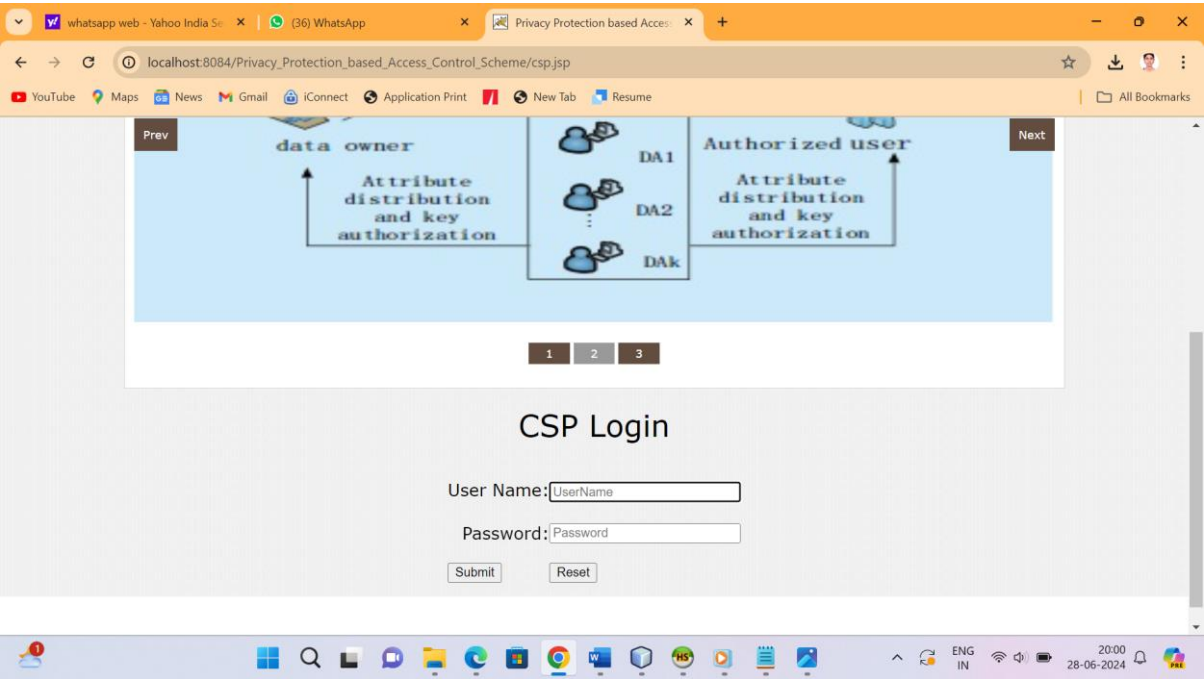


Fig 5.11

You can login into the cloud portal.

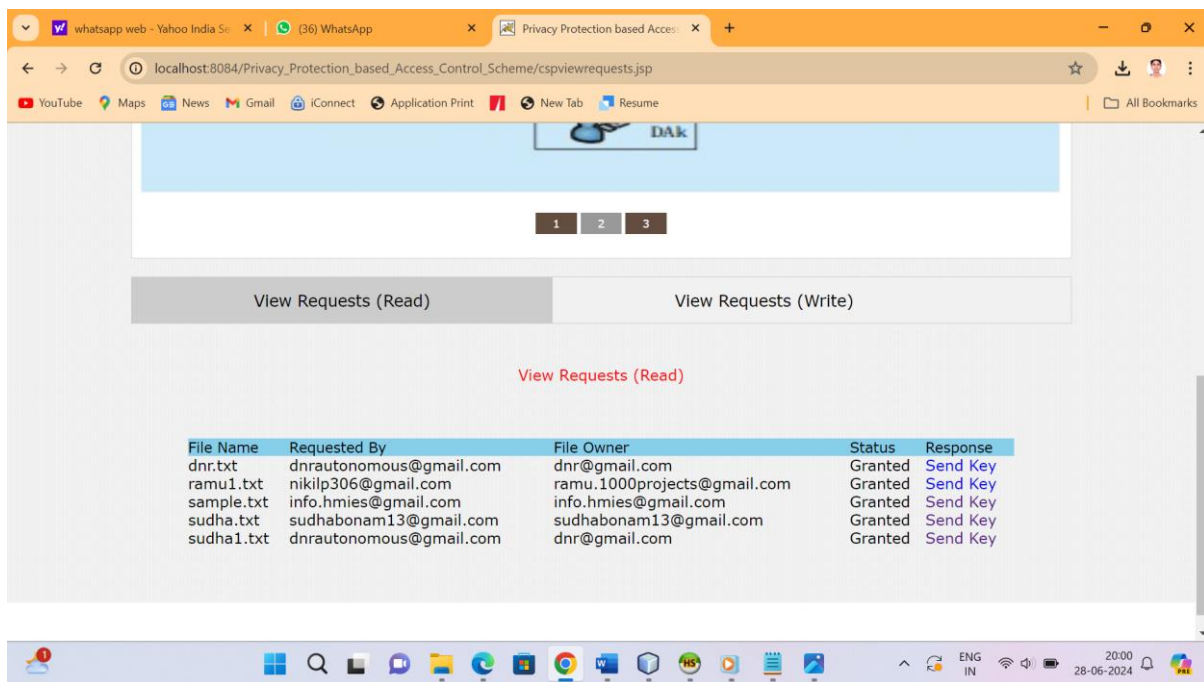


Fig 5.12

See the requests raised for Read and Write and approve.

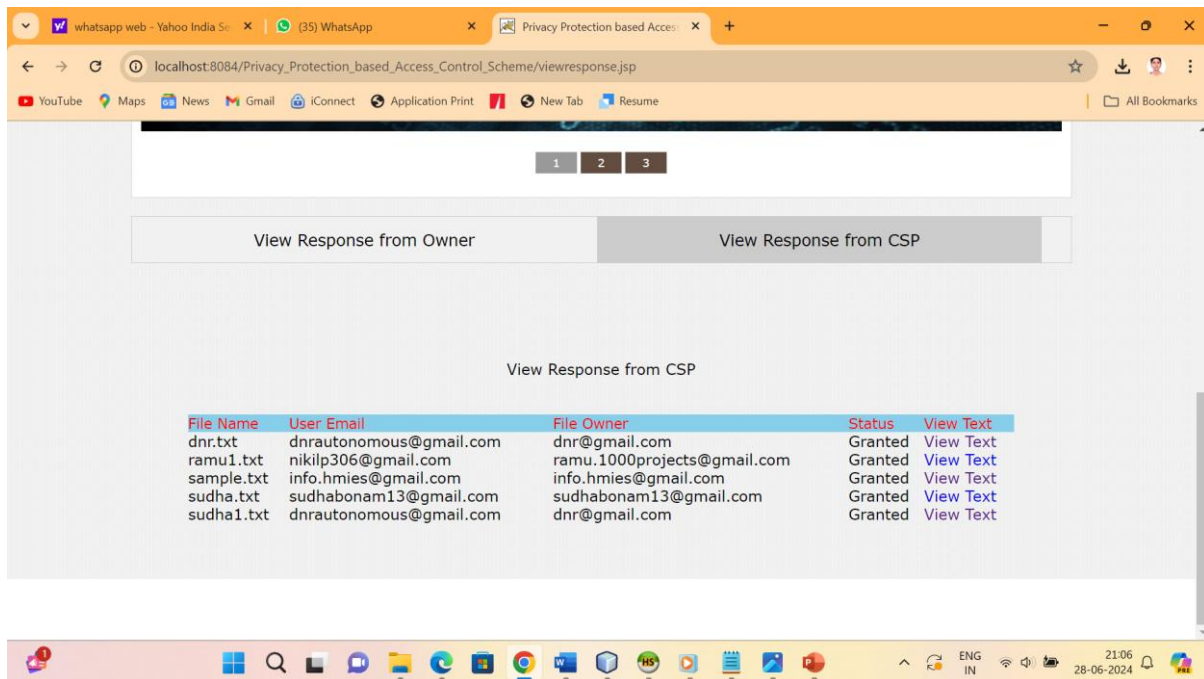


Fig 5.13

By login to PSD user, you can view response from CSP.

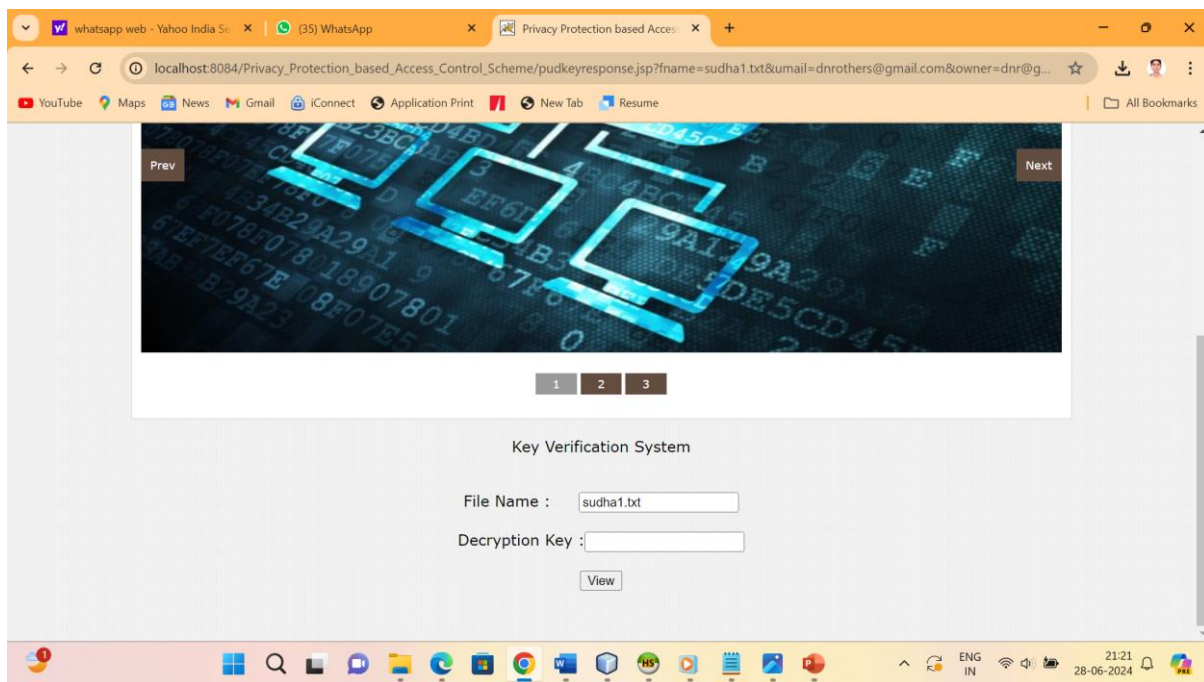


Fig 5.14

By entering decryption key, you can access the file securely.

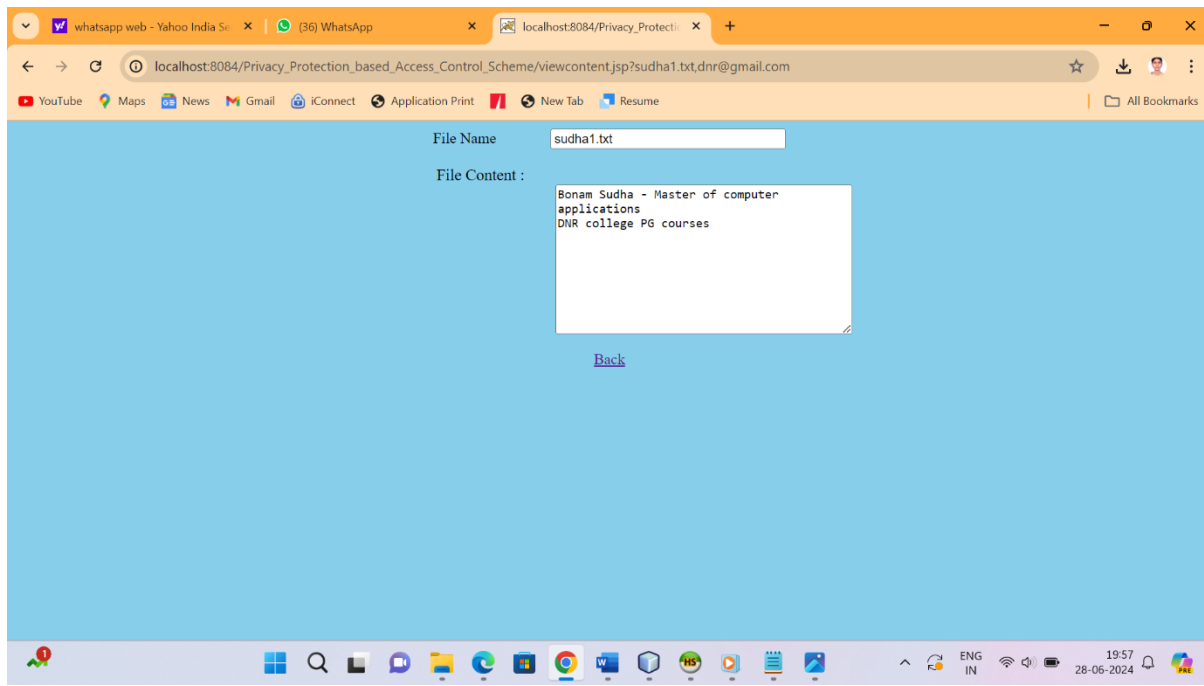


Fig 5.15

Like this, you are able to see content of uploaded file. You can have read and write permissions.

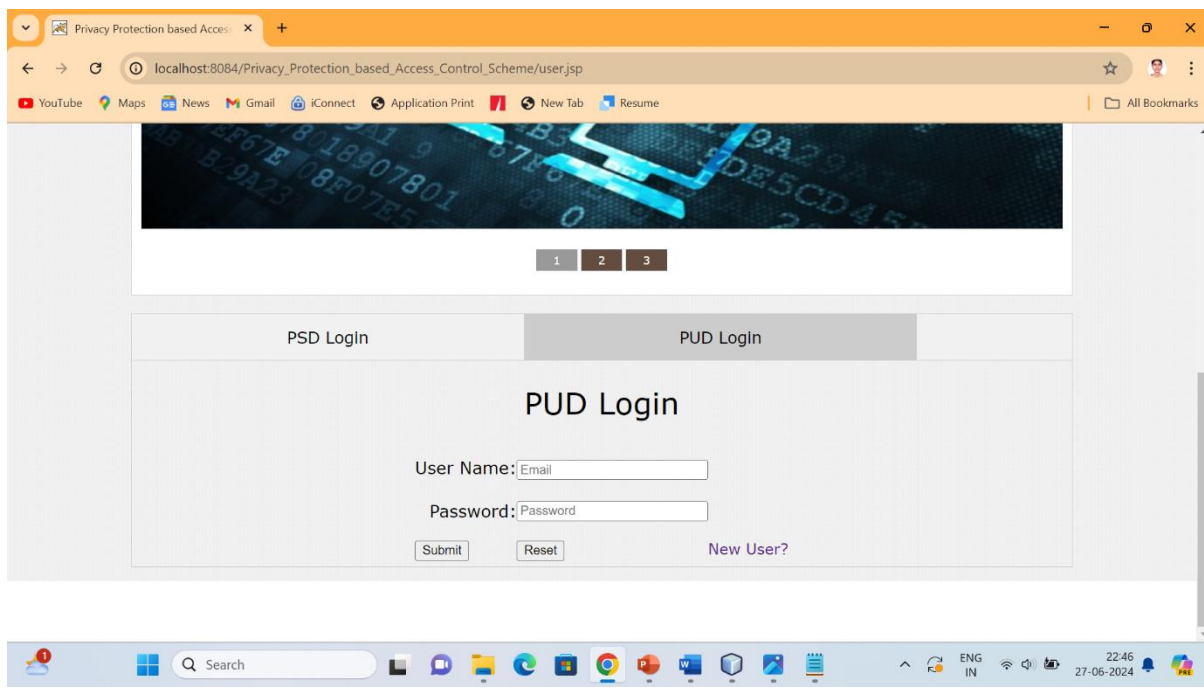


Fig 5.16

You can login into the Public domain users(PUD).

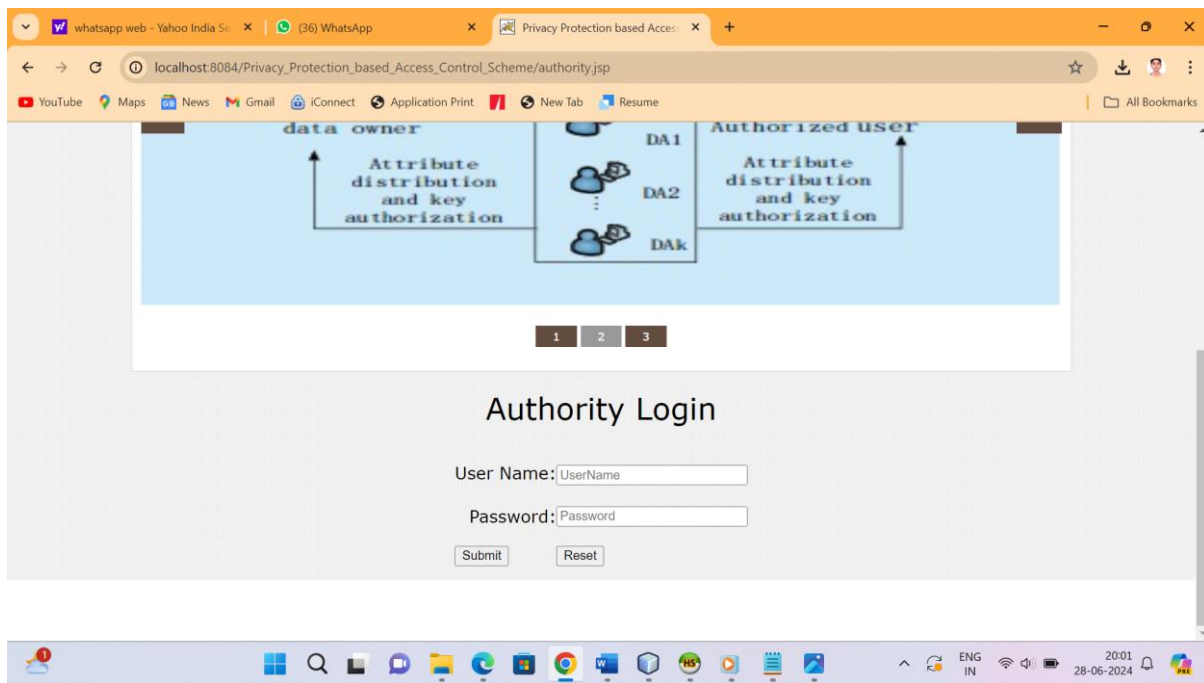


Fig .5.17

You can login into the authority page.

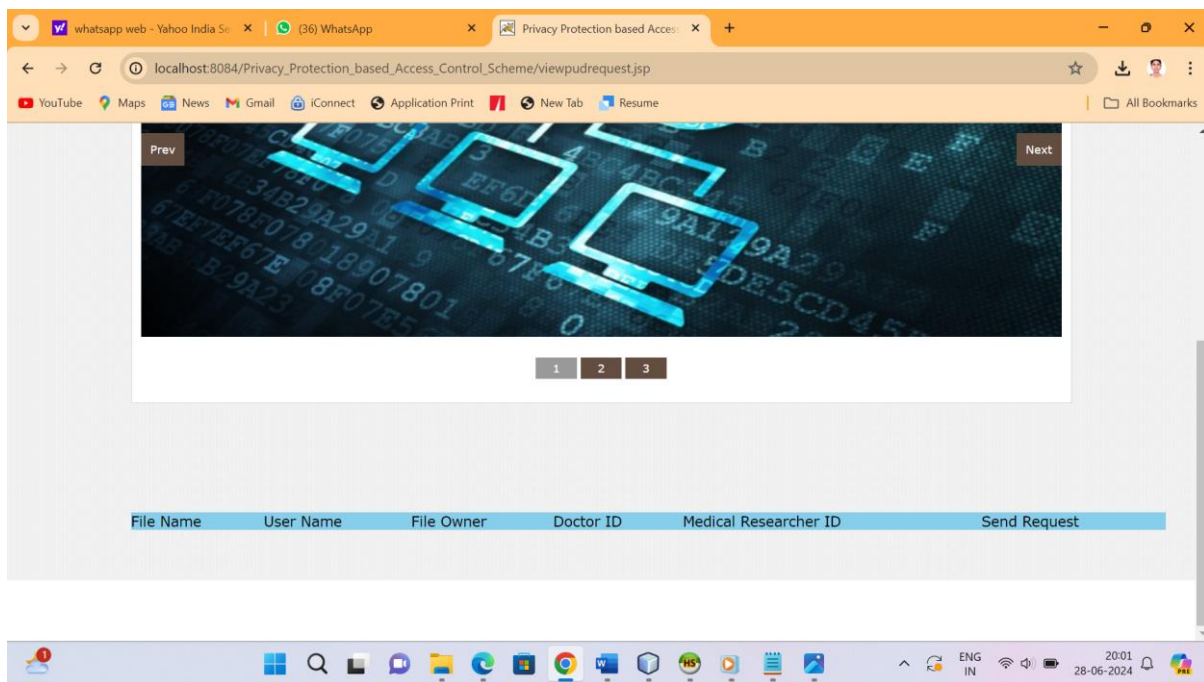


Fig 5.18

In the authority page, we can raise request for access file.

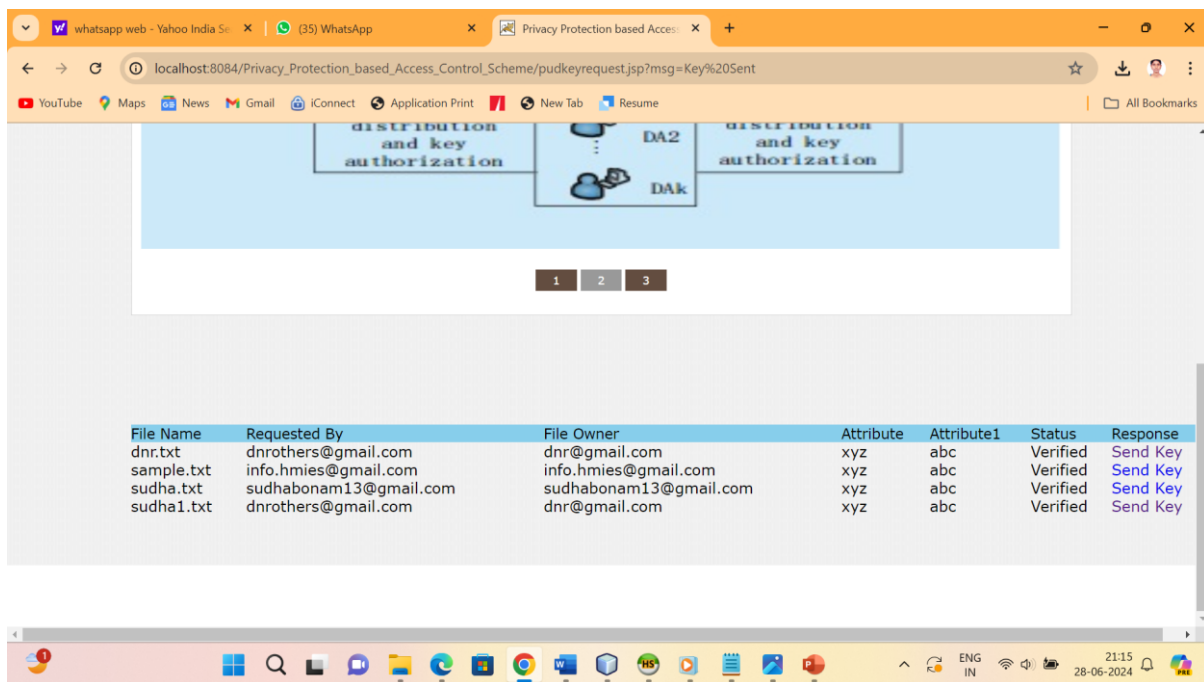


Fig 5.19

In the owner tab, we can send keys for permission for read and write permissions.

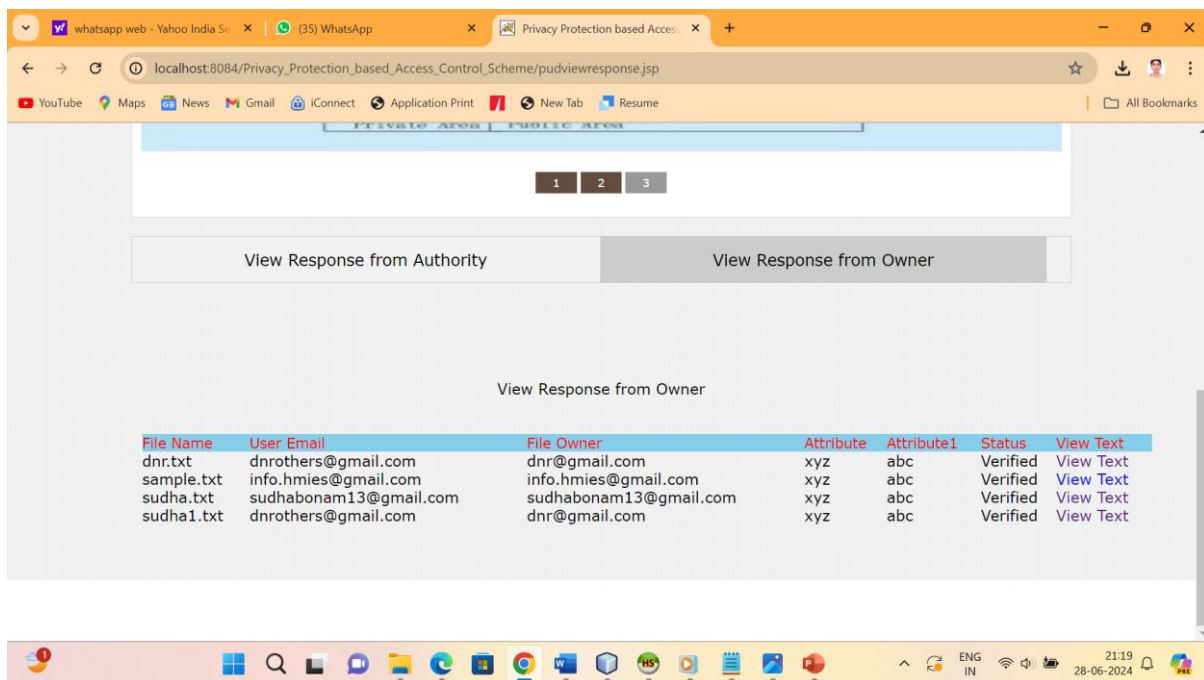


Fig 5.20

In the PUD , you can able to view response from Authority and owner

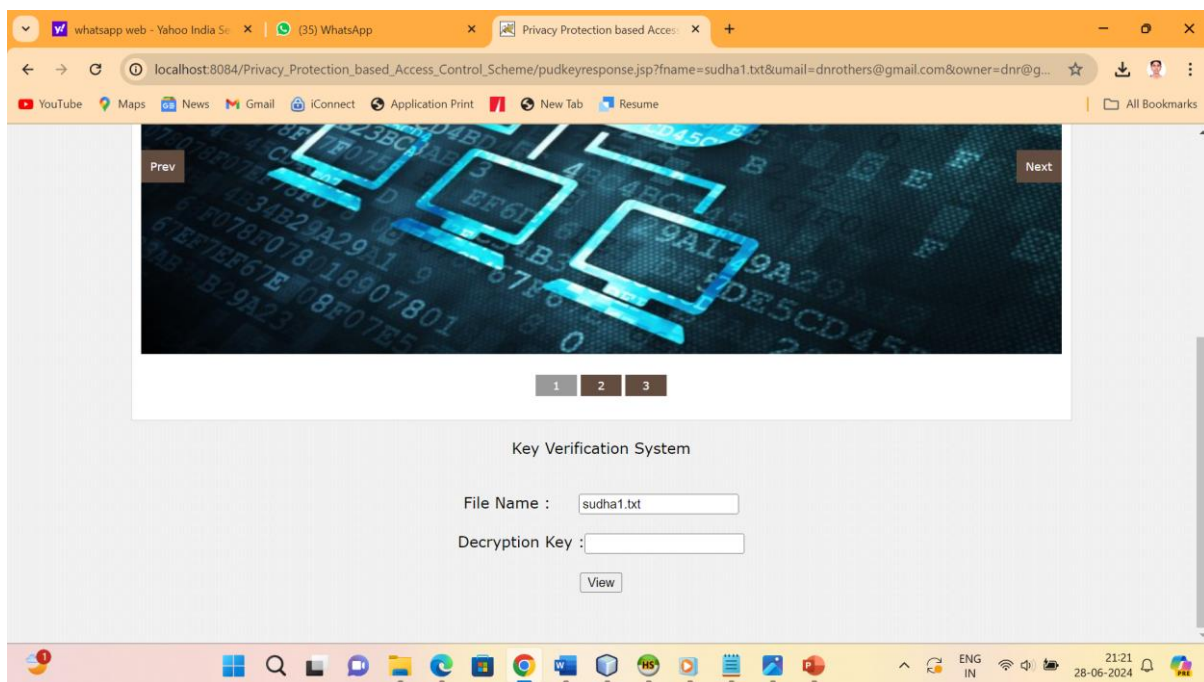


Fig 5.21

By click on view test, this page will appear, give the decryption key and access the file.

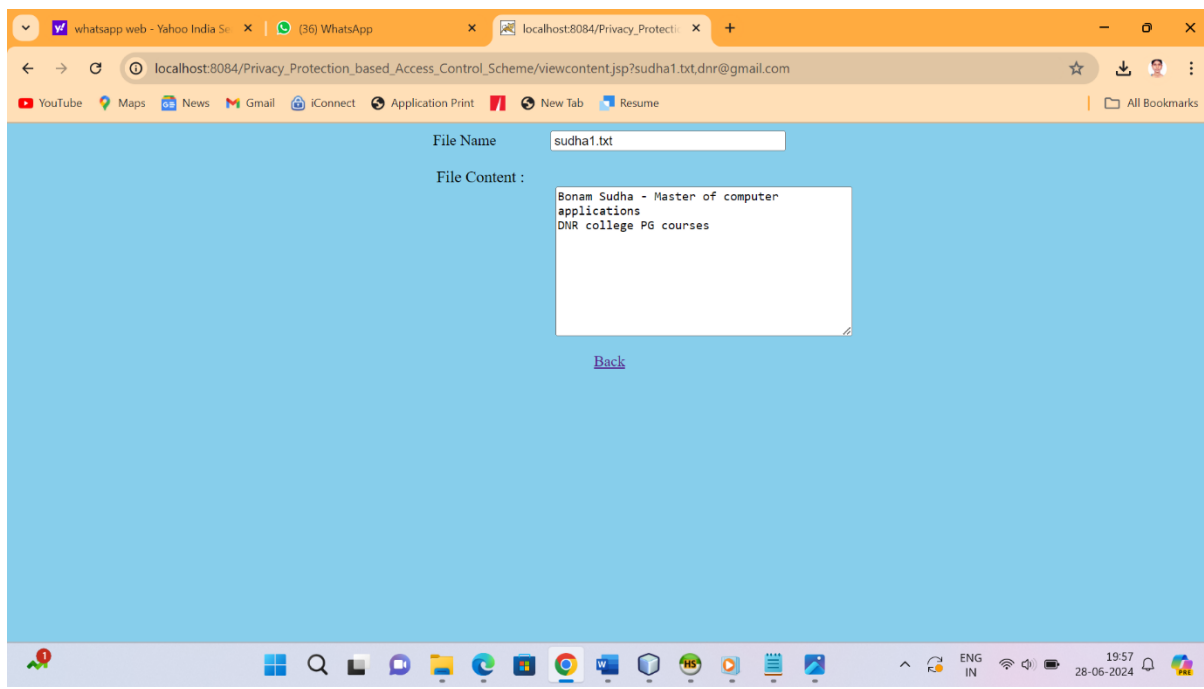


Fig 5.22

Now, you can able to access the file securely.

6. CONCLUSION AND FUTURE WORK

CONCLUSION

In this paper, we propose access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the user, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, the KAE algorithm is applied to implement users read access permissions and greatly improved efficiency. The IABS scheme is employed to achieve the write permissions and the separation of read and write permissions to protect the privacy of the user's identity. In the PUD, we use the HABE scheme to avoid the issues of single point of failure and to achieve data sharing. Furthermore, the paper analyzes the scheme from

security and efficiency, and the simulation results are given. By comparing with the MAH-ABE scheme, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services.

7. REFERENCES

- S. Yu, C. Wang, K. Ren, "Achieving secure, scalable, and fine-grained data access control in cloud computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.
- [2] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," Proc. Security and Privacy, pp. 321-334, 2007.
- [3] J. Hur, D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.
- [4] A. Lewko, B. Waters, "Decentralizing attribute-Based encryption," Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.
- [5] M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption," IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131- 143, 2013.
- [6] C.K. Chu, S.S.M. Chow, W.G. Tzeng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014.
- [7] J. Li, K. Kim, "Hidden attribute-based signatures without anonymity revocation," Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.
- [8] H.K. Maji, M. Prabhakaran, M. Rosulek, "Attribute-Based Signatures," Proc. Topics in Cryptology - CT-RSA, pp. 376-392, 2011.
- [9] S. Kumar, S. Agrawal, S. Balaraman, "Attribute based signatures for bounded multi-level threshold circuits," Proc. Public Key Infrastructures, Services and Applications, pp. 141-154, 2011.
-