International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252

Data Pool Share and Dispersion Securely With Attribute and Time Cases in Public Cloud

Dr.D.J.Samatha Naidu [#1], D.Sudhakar [*2], Mulla. Navitha [#3]
[1]*Professor & Principal, APGCCS, Rajampet, YSR Kadapa, India*
[2]*Assistant Professor, MCA Department, APGCCS, Rajampet, YSR Kadapa, India*
[3]*MCA Department, APGCCS, Rajampet, YSR Kadapa, India*

Date of Submission: 05-10-2022 Date of Acceptance: 15-10-2022

ABSTRACT—
Cloud computing has become increasingly popular among users and businesses around the world. Although cryptographic techniques can provide data protection for users in public cloud, several issues also remain problematic, such as secure data group dissemination and fine-grained access control of time-sensitive data. In this paper, we propose an identity based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. Security matters existing in public cloud motivate the requirement to appropriately keep data confidential.In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a re-encryption key to cloud server. The re-encryption conditions are associated with attributes and releasing time, which allows data owner to enforce fine-grained and timed-release access control over disseminated ciphertexts. The theoretical analysis and experimental results show our proposed scheme makes a tradeoff between computational overhead and expressive dissemination conditions.

Keywords—
Data Sharing , Cloud computing, conditional proxy re-encryption,attribute-based encryption,privacy conflict.

I.INTRODUCTION

The cloud computing benefits individual users and enterprises with convenient access, increased operational efficiencies and rich storage resources by combining a set of existing and new techniques from research areas such as service-oriented architectures and virtualization. Attribute-based encryption (ABE) is one of new cryptographic mechanisms used in cloud to reach flexible and fine-grained secure data group sharing. The proxy re-encryption (PRE) scheme in a manner could achieve efficient data dissemination in cloud by re-encrypting the ciphertext to other users. However, it may not meet the requirements when data owner doesn't expect all the authorized users who can view his data to disseminate data or allow the disseminators to disseminate all of his data.Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud, Microsoft's Azure and Amazon's S3 However, it also suffers from several security threats, which are the primary concerns of cloud users.Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the ciphertext periodically by using secret key. To update the ciphertext of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-reencrypt-upload. This process brings great

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252

communication and computation cost, and undesirable for cloud users with low capacity of computation and storage

.

Purpose

Data encryption for information stored on the cloud network ensures that even if the data is lost, stolen or mistakenly shared, the contents are virtually useless without the encryption key. Again, keys are only made available to authorized users.

Scope

In this paper ,I propose a new and more efficient algorithm that produces solutions which are very close to the optimal ones. Our contribution is efficient not only for the bursting of behavior-based compositions but also for architecture-based compositions of services

II RELATED WORK

Existing System

The cloud computing benefits individual users and enterprises with convenient access, increased operational efficiencies and rich storage resources by combining a set of existing and new techniques from research areas such as service-oriented architectures and virtualization the CSP which deprives data owners' direct control over their data is assumed to be honest-but-curious, that may prompt security concerns. These security matters existing in public cloud motivate the requirement to appropriately keep data confidential. Time-sensitive data such as a business plan and a tender, is a special data in cloud which requires time-based exposing, this solution forces the directors to repeatedly disseminate different versions of the same data, which brings unnecessary burden. From the perspective of cryptography, this goal of time-based exposing can be achieved by timed-release encryption some TRE-based systems incorporate the concept of time into a combination of CP-ABE or PRE to support fine-grained and time-based data exposing, whereas these approaches are failure to meet the above scenario of data dissemination.

Disadvantages

- Less collusion resistance
- Reduced performance
- Less flexibility and scalability

III. PROPOSED WORK

Proposed System

I propose an identity based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a re-encryption key to cloud server.CryptDB based on order preserving encryption and homomorphic encryption to guarantee data confidentiality of database in public cloud. Trusted time agent rather than data owner to uniformly release the access privilege at a specific time.

Advantages

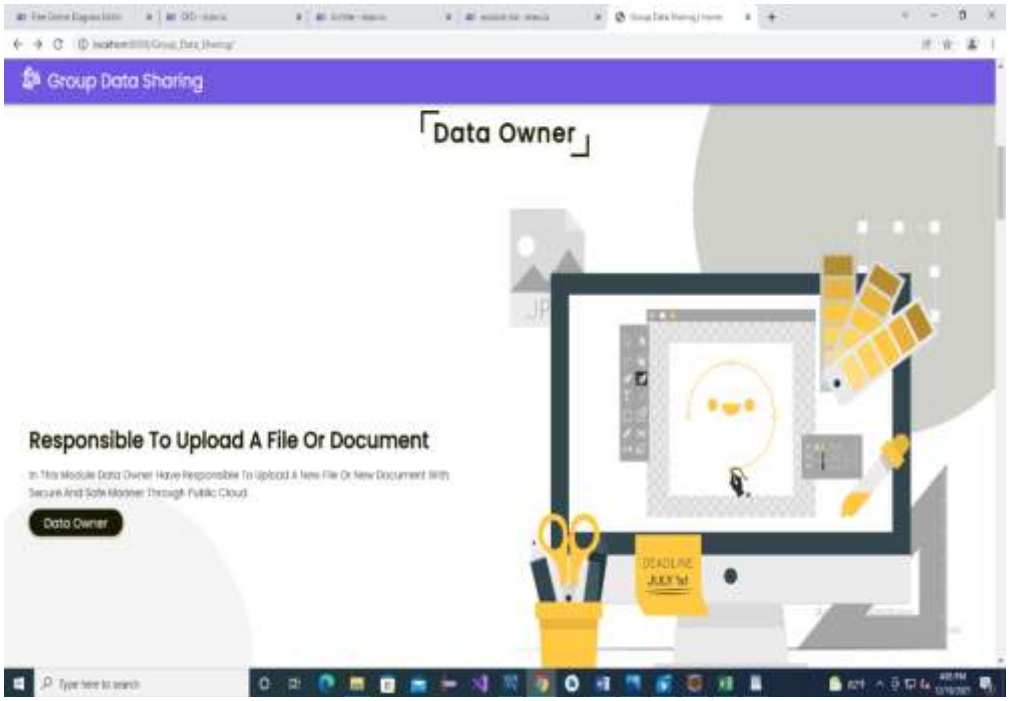
- Improved performance
- Confidentiality
- Collusion resistance
- Flexibility and scalability

Sample Screens & reports

Screen 1 :HOME PAGE

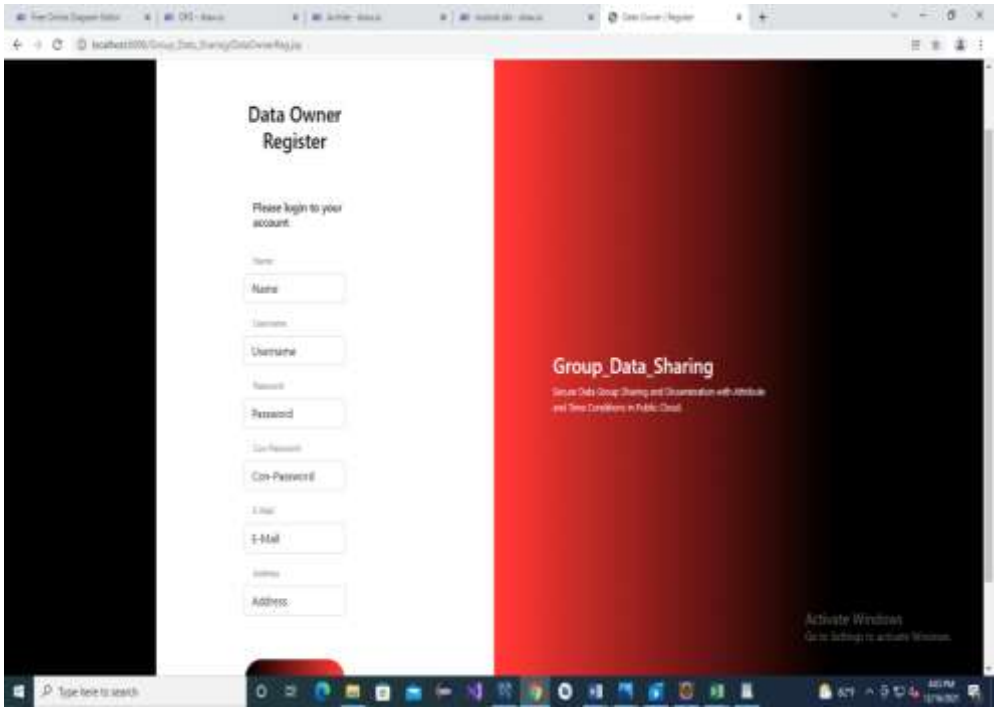
Description: This is my project home page. whenever we are connectedtotheserver then displayabovehome page.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen2 :DataOwnerHomePage

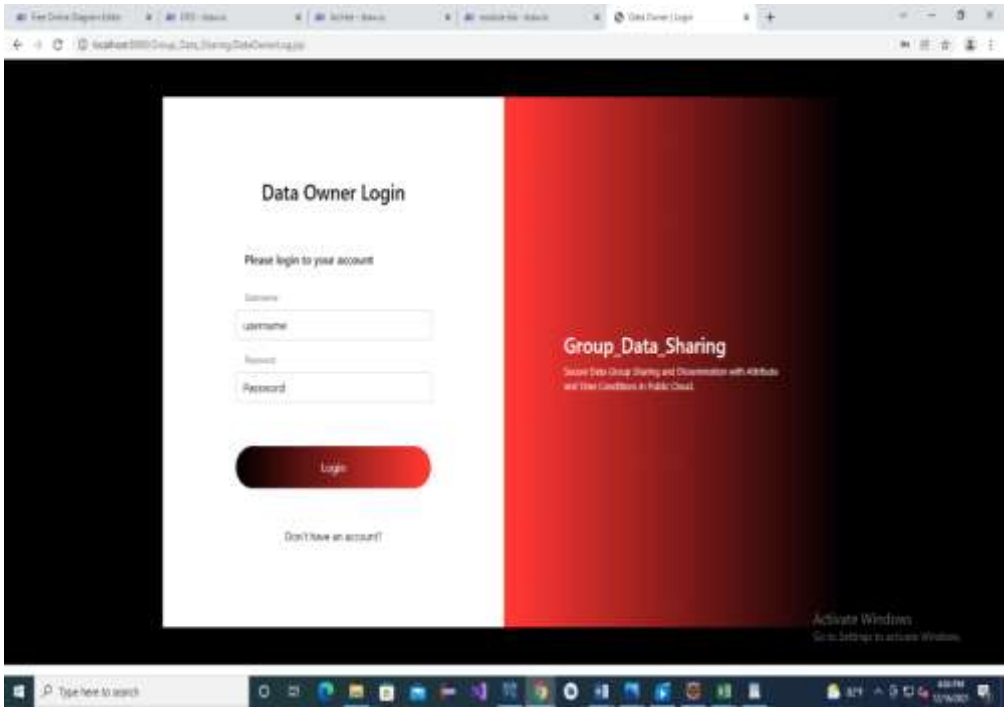
Description: Here we are entering into our first module data owner home page



Screen3:Data OwnerRegister

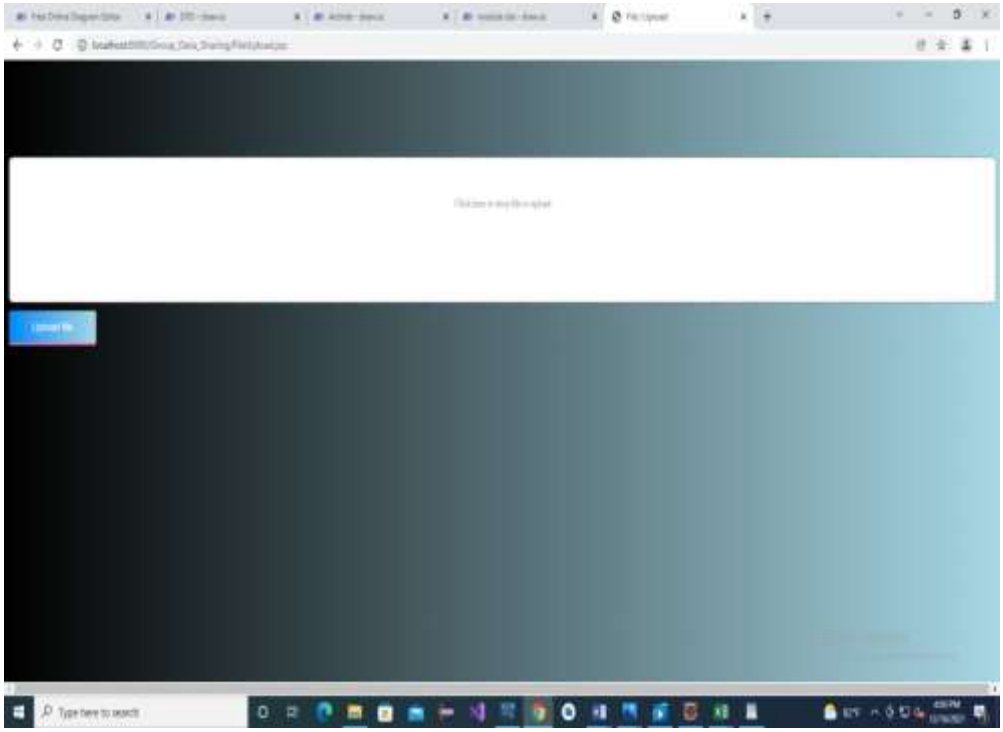
Description: Data owner must and should to register to enter the server.The username and password are same or different we cannot face anyissues.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



ScreenNo4:Data Owner Login

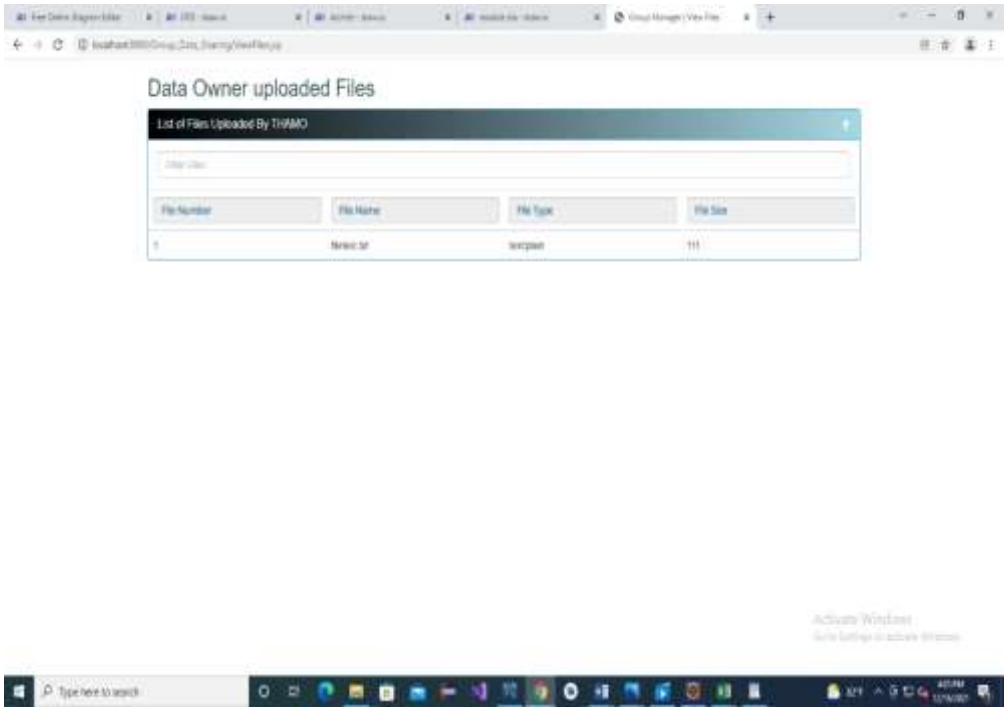
Description: After Register we can login by using the register details



Screen5:Upload Files

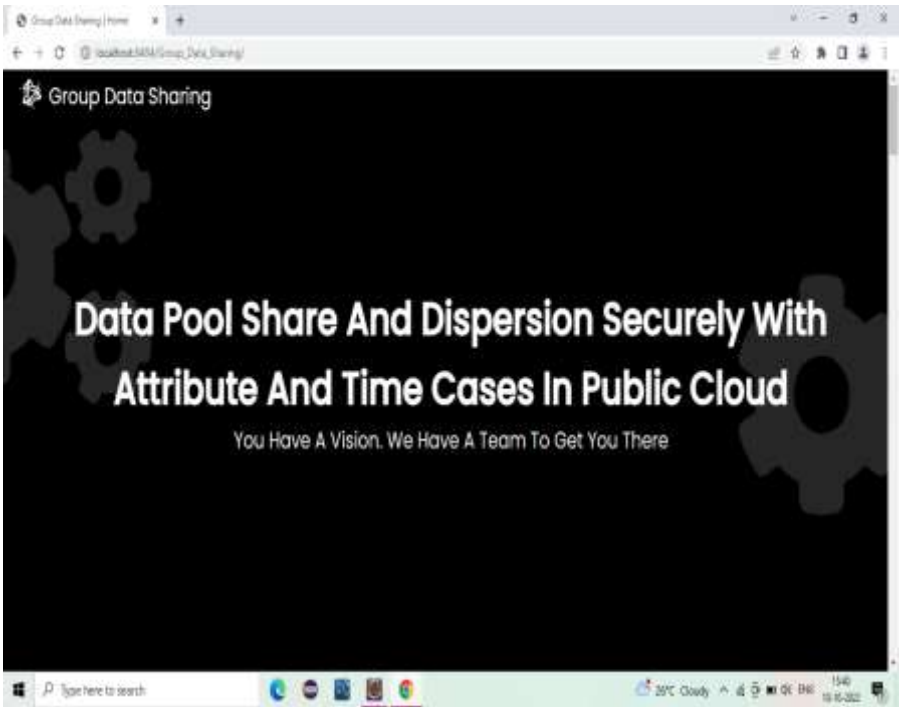
Description: After login which we can send the data to user the data owner can we uploaded the files.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



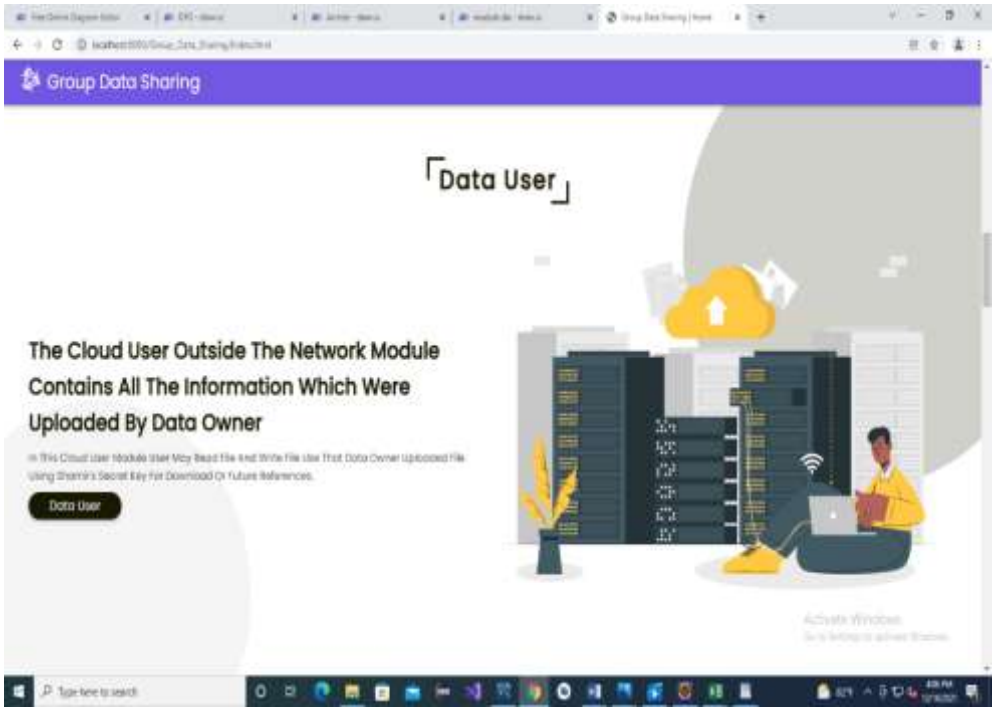
Screen6:Show Files

Description: Which we can upload the file we can show that files



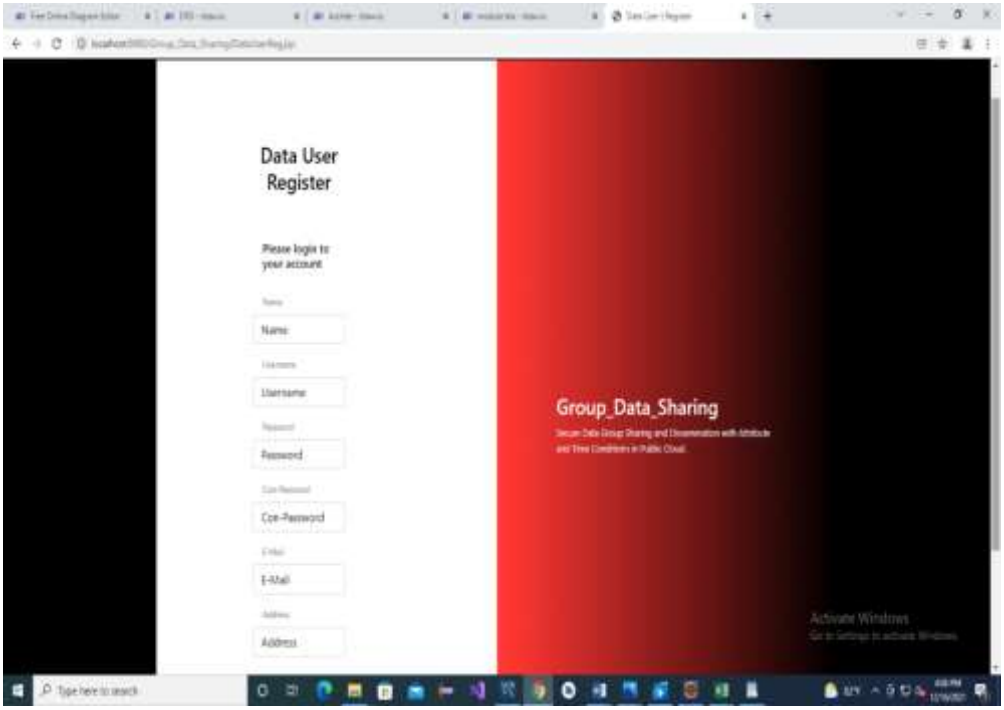
Screen 7 : Home Page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen8:Data User Home Page

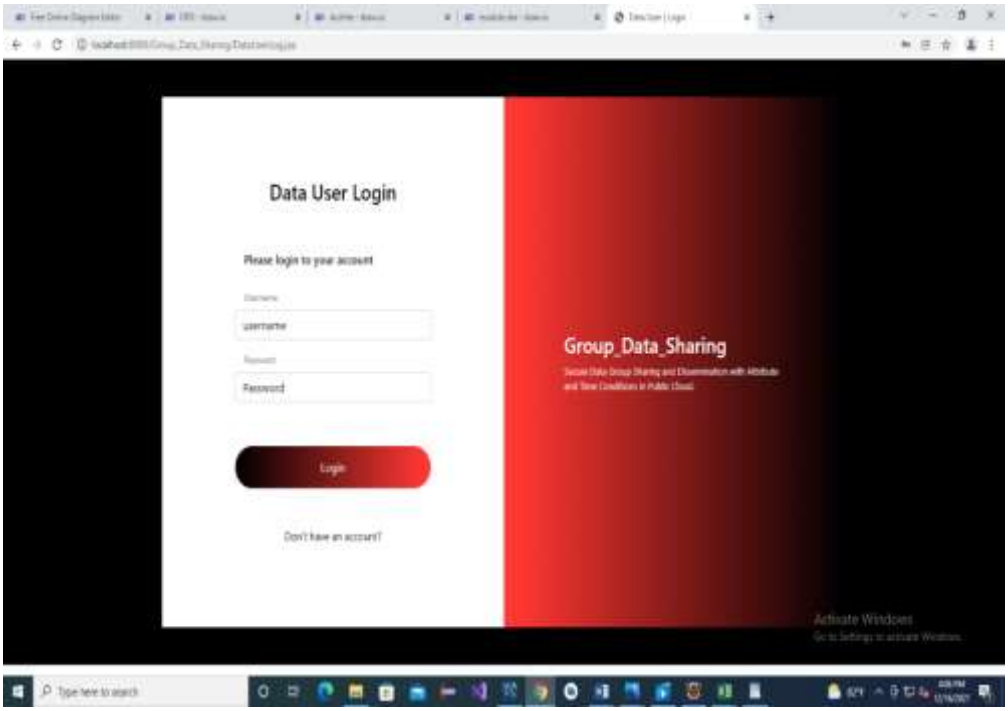
Description: Here we are entering into our second module data user home page



Screen9:Data UserRegister

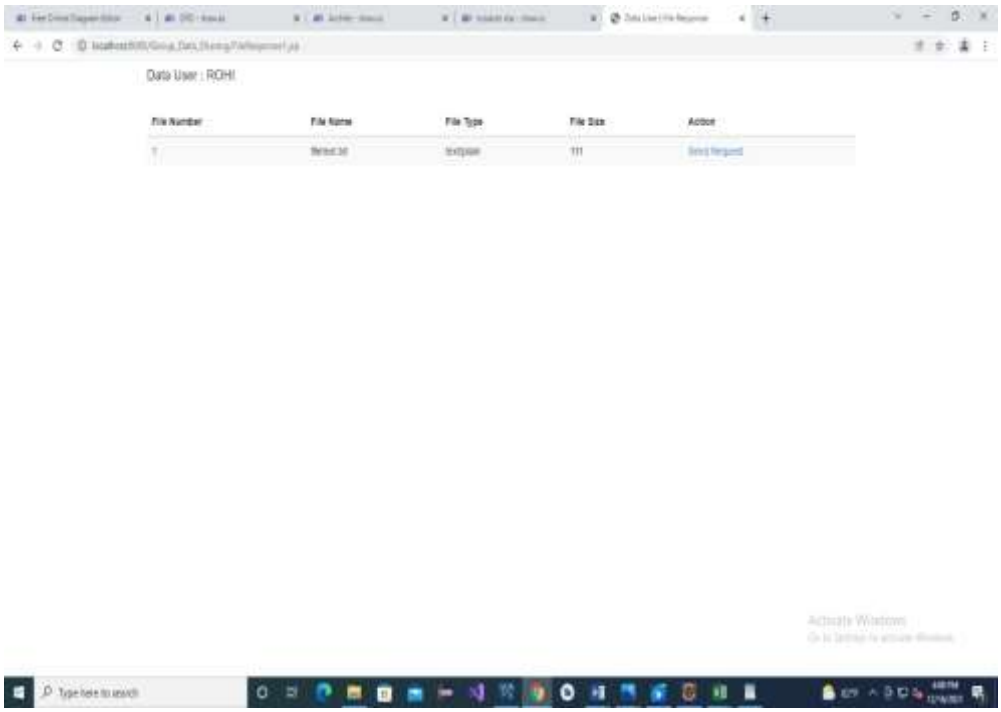
Description: Data user must and should to register to enter the server.The username and password are same or different we cannot face any issues.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen10: Data UserLogin

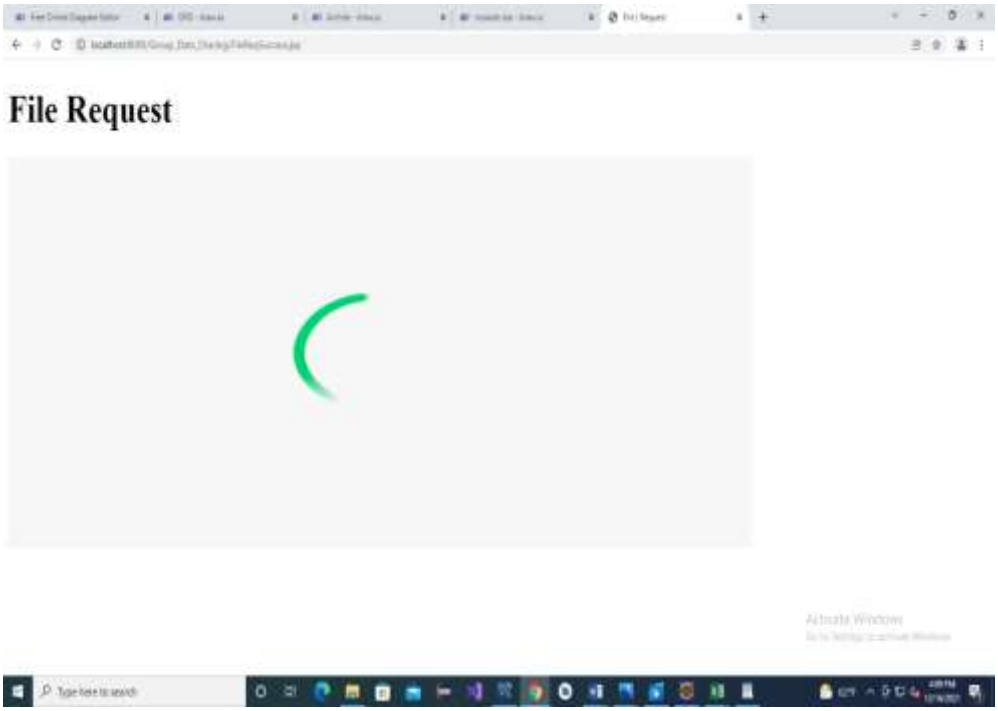
Description: After Register we can login by using the register details



Screen11:Send Request

Description: After login the user can send the file request to authority

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252

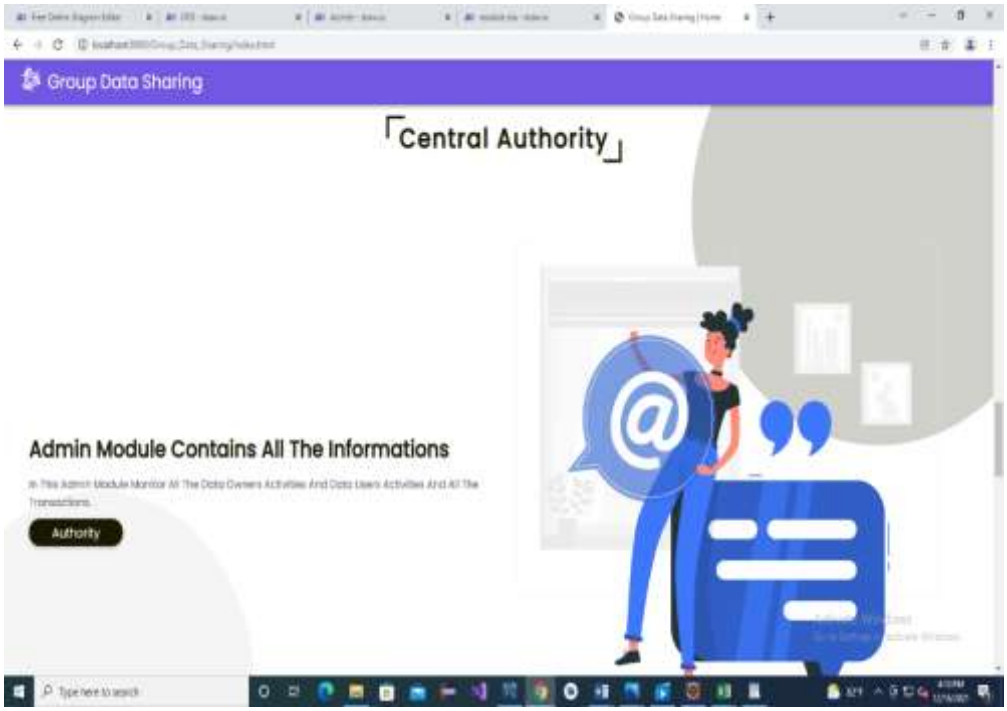


Screen 12 : Send request successfully

Description: After send the request it shows the send request successfully

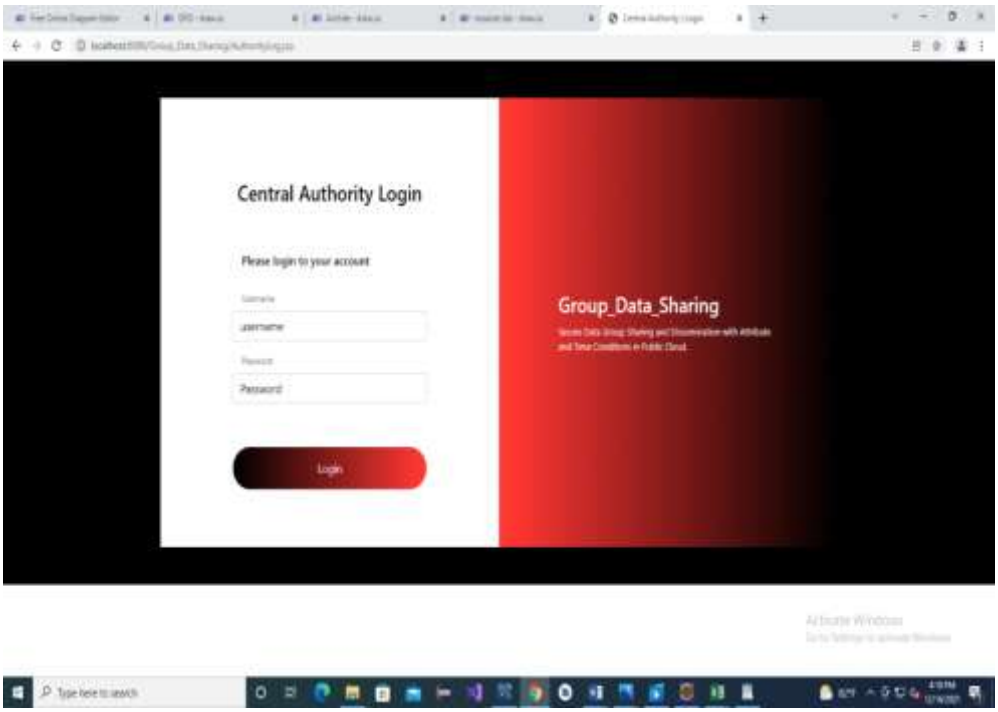
Screen 13:HOME PAGE

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen14: Central Authority

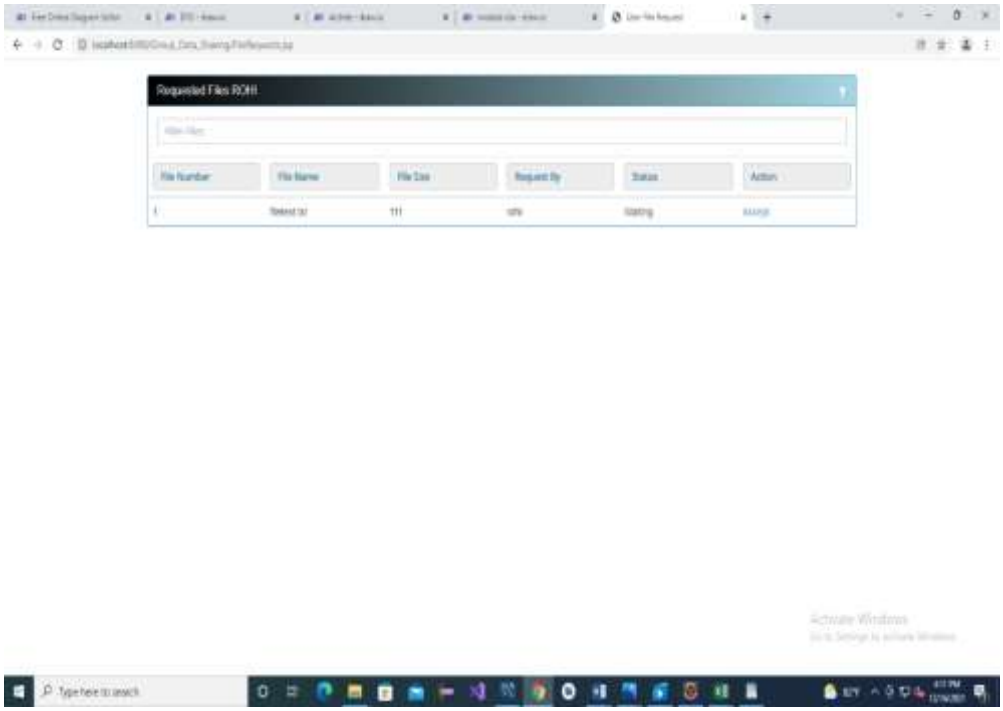
Description: Here we are entering into our third module central author homepage.



Screen 15:Central Authority Login

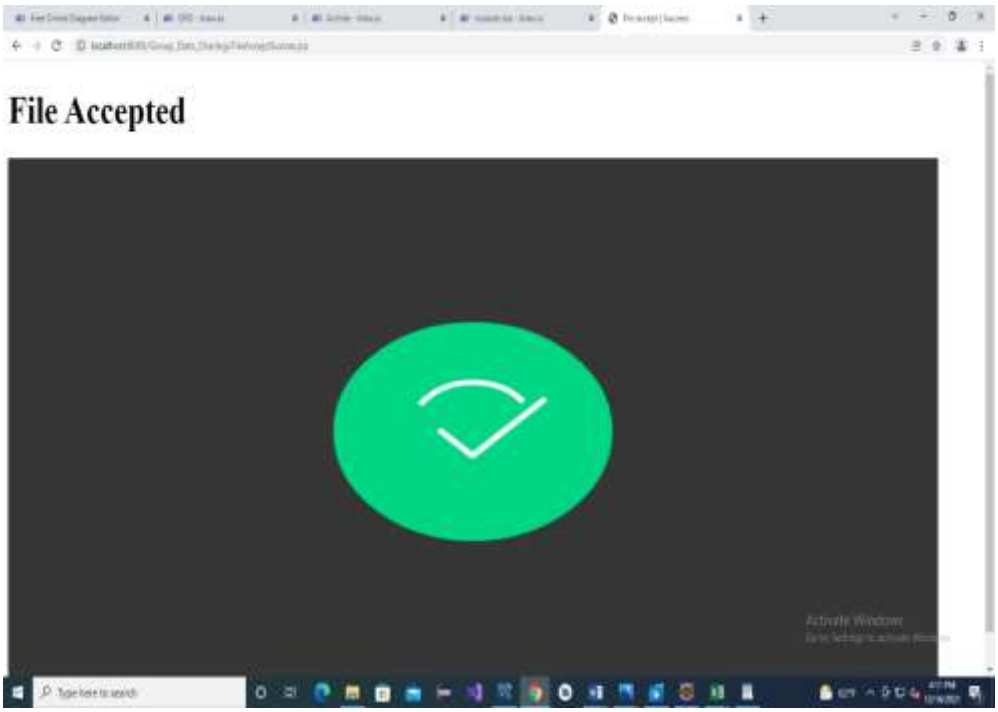
Description: We can login to the backend details, we already give the serve page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen 16:Accept File

Description: Authority accept the request who can send that

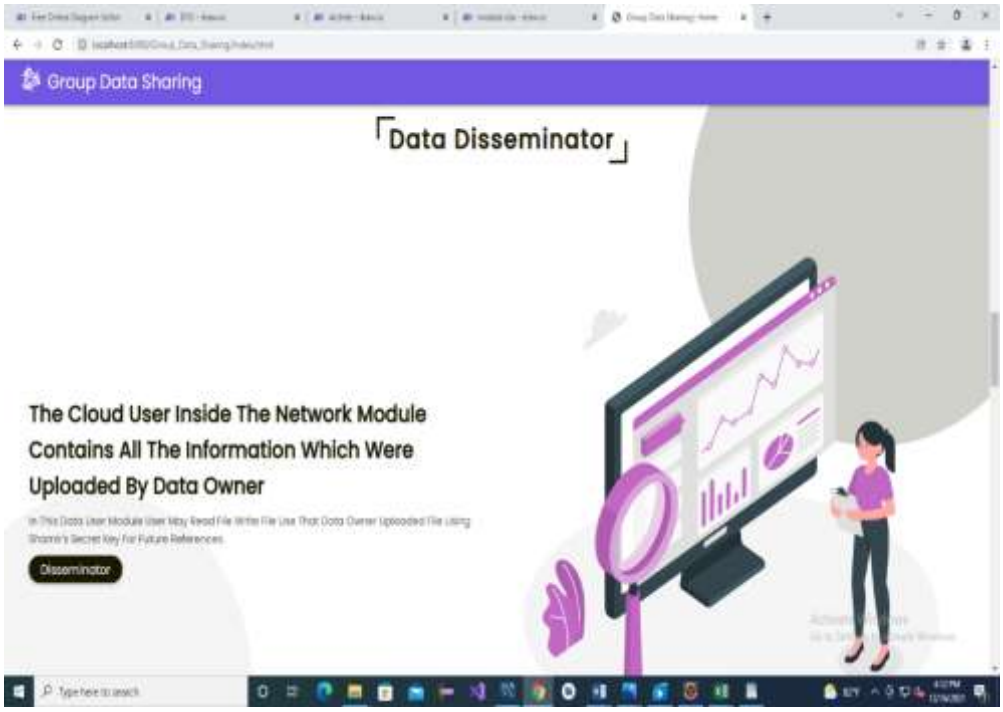


Screen 17 : File accepted successfully

Description: After authority accept the files it shows file accepted successfully

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252

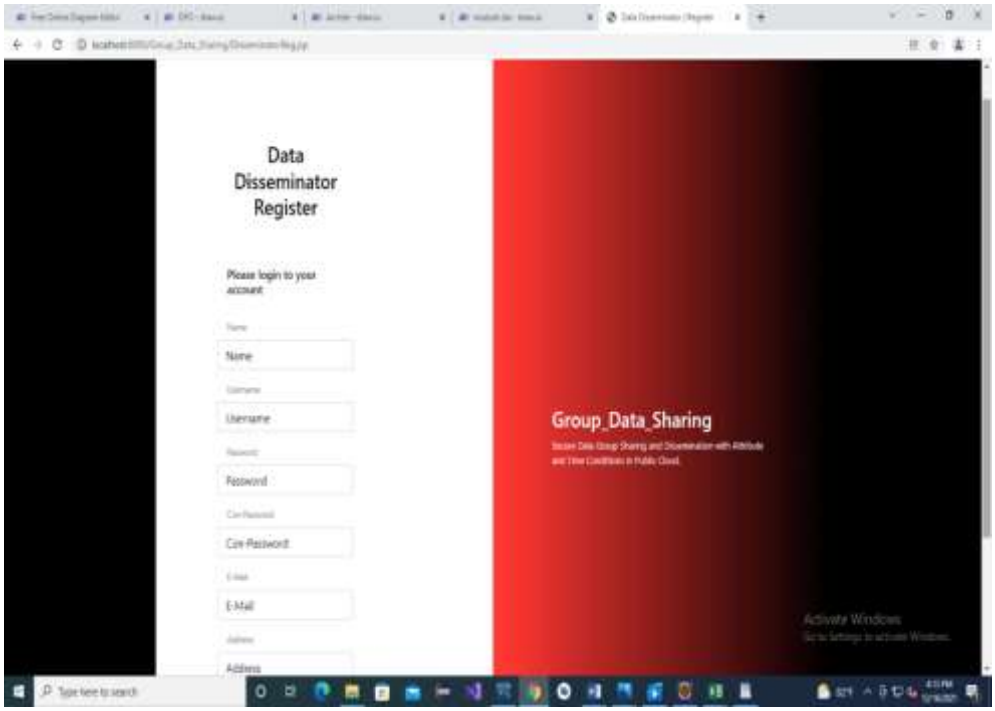
Screen 18 :Home page



Screen 19:Data Disseminator Home Page

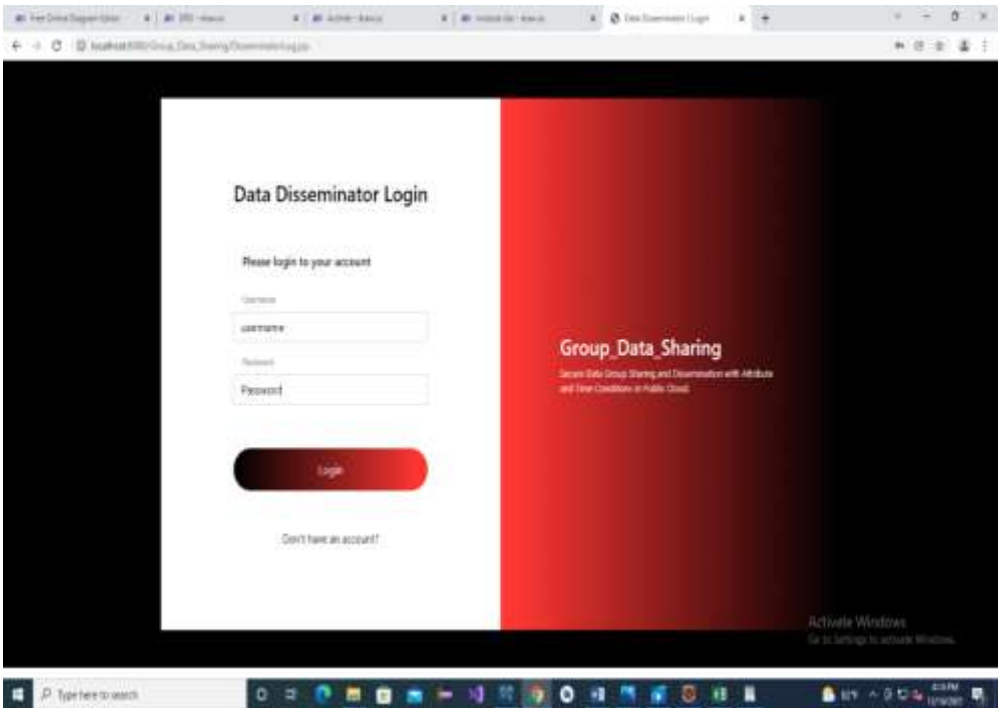
Description: Here we are entering into our last module Data disseminator homepage

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen 20:Data Disseminator Register

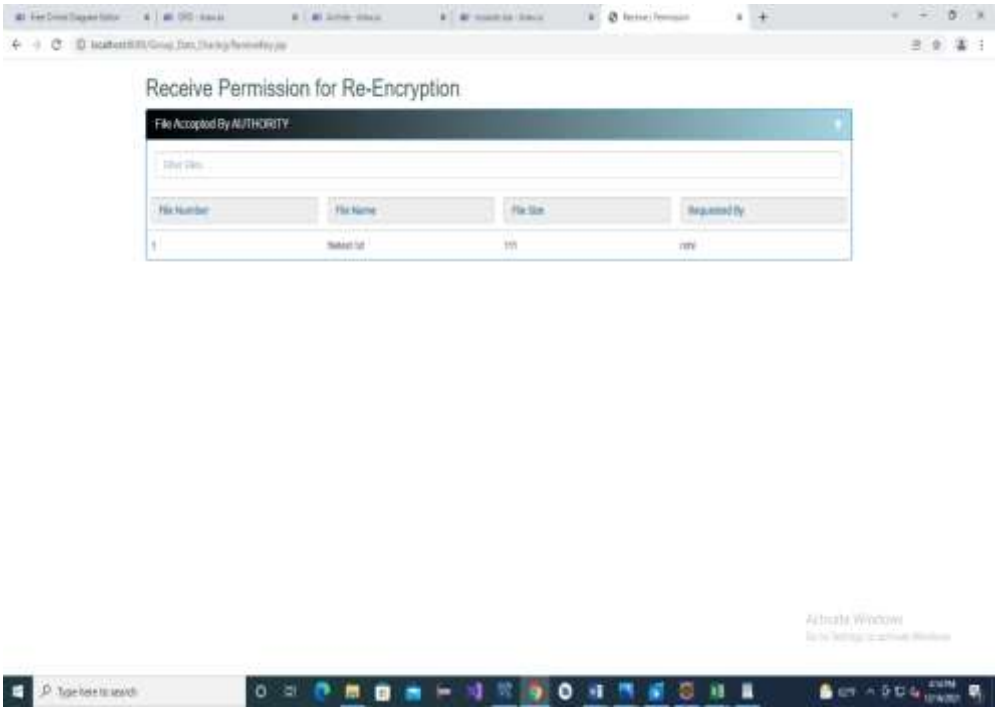
Description: Data disseminator must and should to register to enter theserver. The username and password is same or different we cannot faceanyissues.



Screen 21: Data Disseminator Login

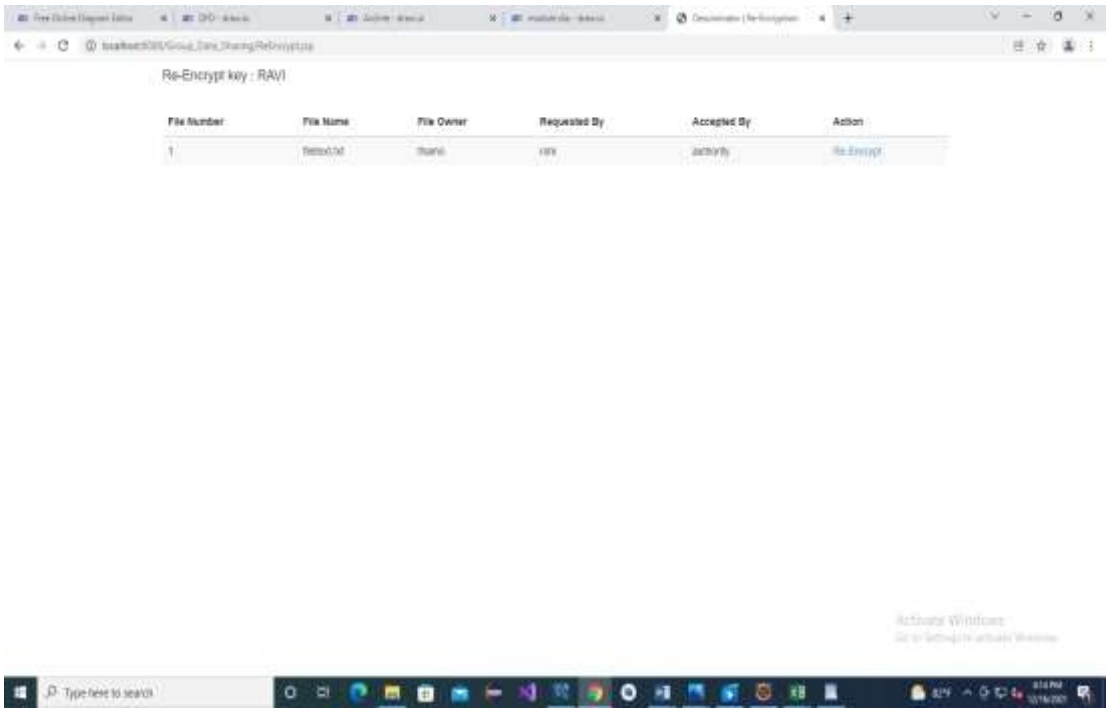
Description: After Register we can login by using the register details

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen22:Receive Permission for Re-Encryption

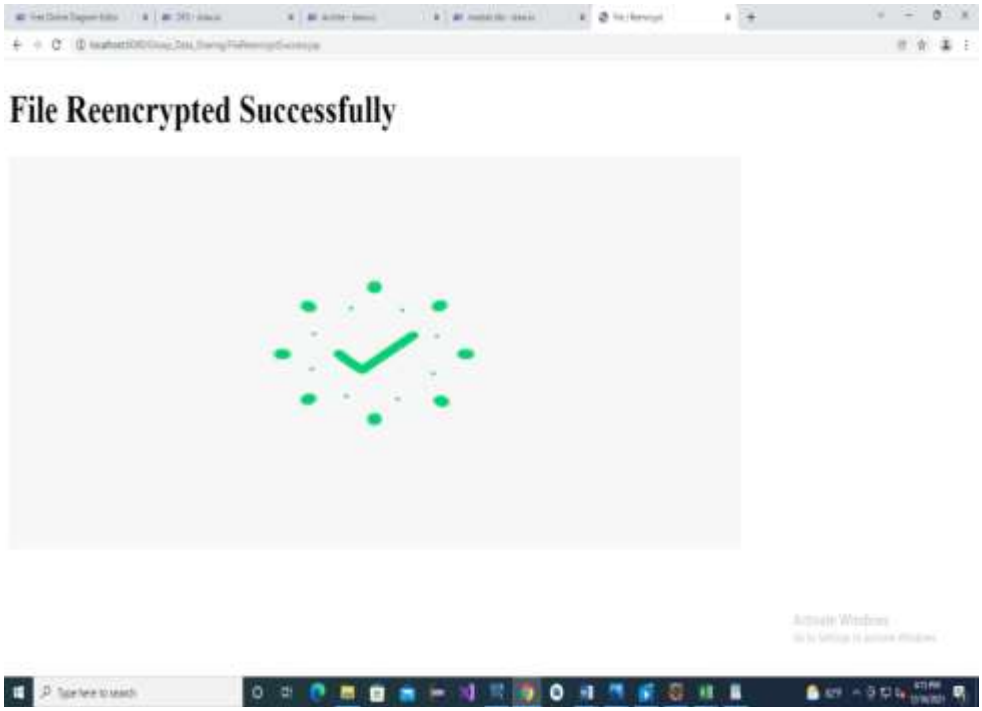
Description: After login we have Receive permission for Re-encryption the data.



Screen 23 :Re-Encrypt Accept Page

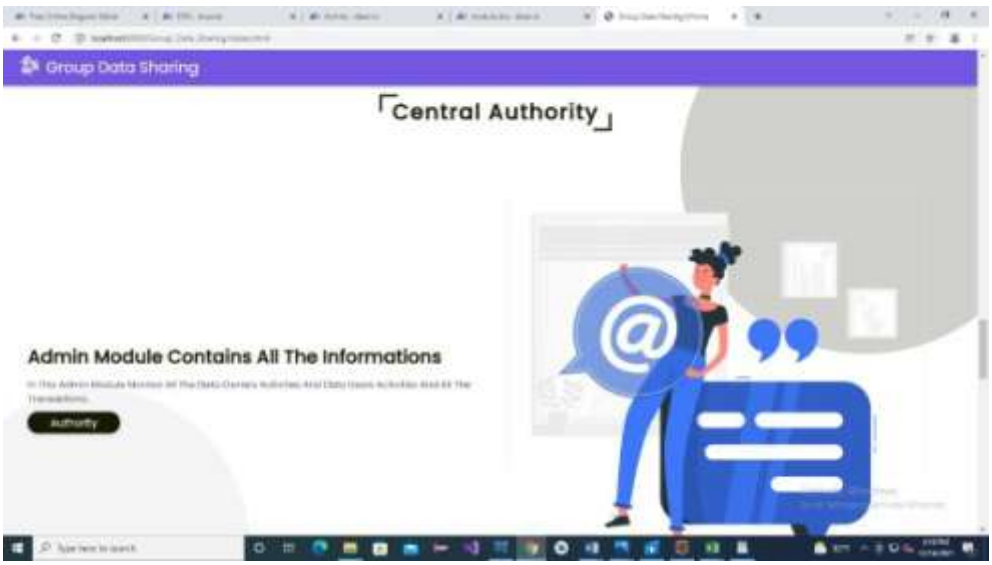
Description: This is the Accept page of Re-encryption

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen24: File re-encrypted successfully

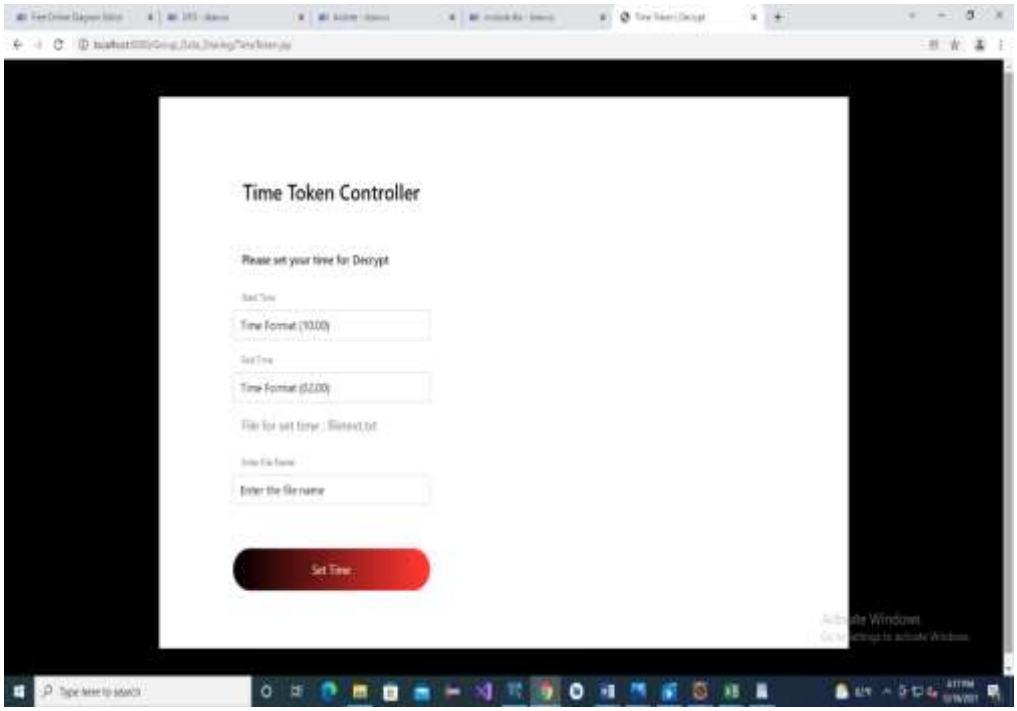
Description: After re-encryption it shows re encrypted successfully



Screen25:Central Authority HomePage

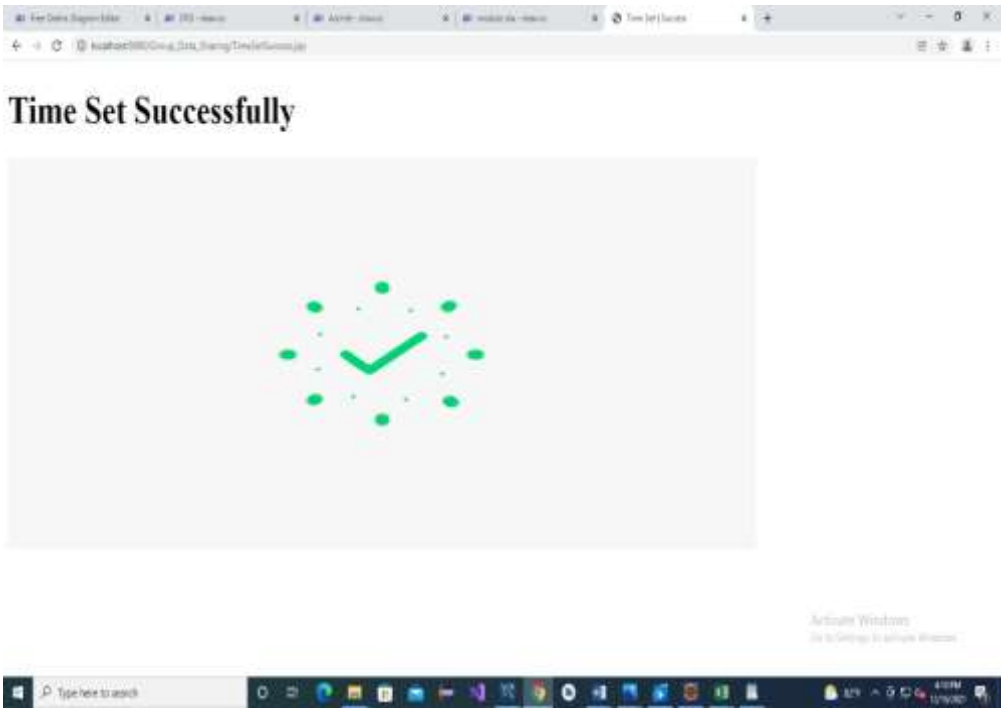
Description: Again, we are come to authority page

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen 26: Time Token Controller

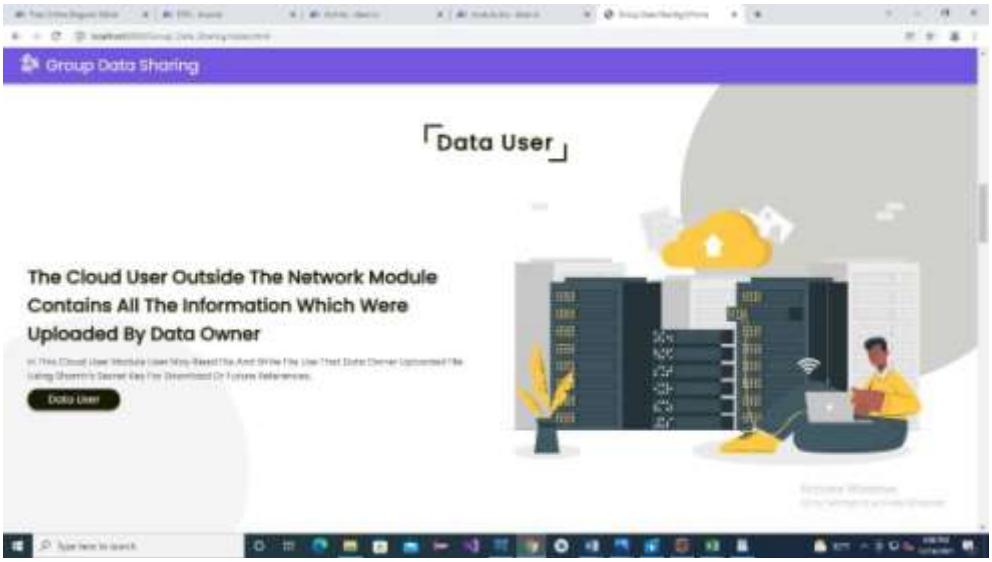
Description: Authority to allocate the time for user can decrypt the data



Screen 27 : Time set successfully

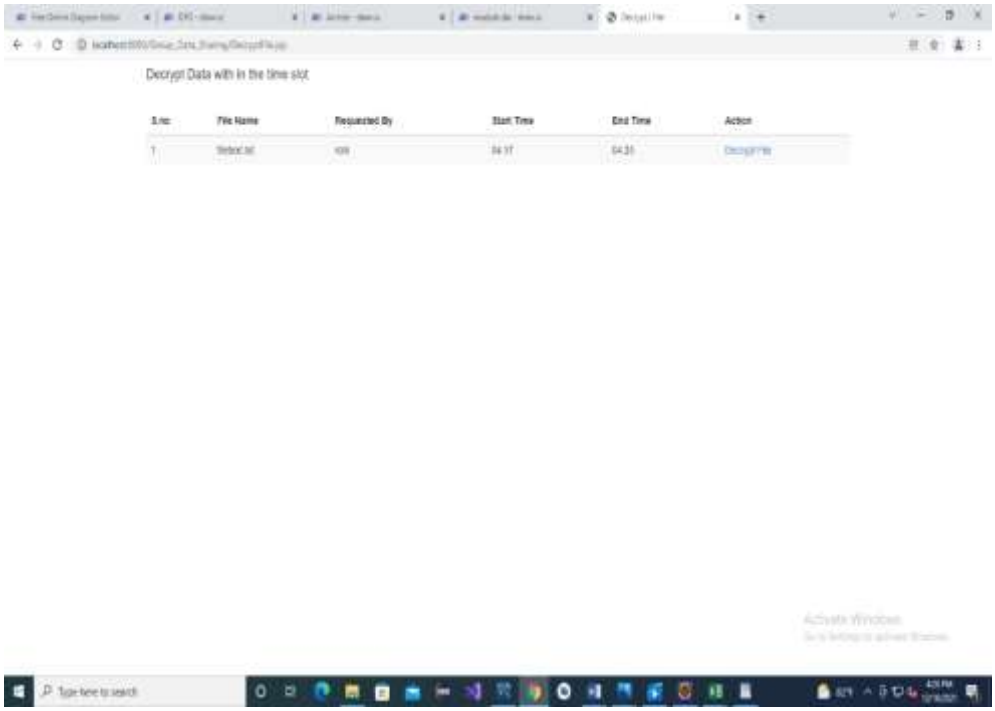
Description: It shows times lot set successfully

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen28 : Data User HomePage

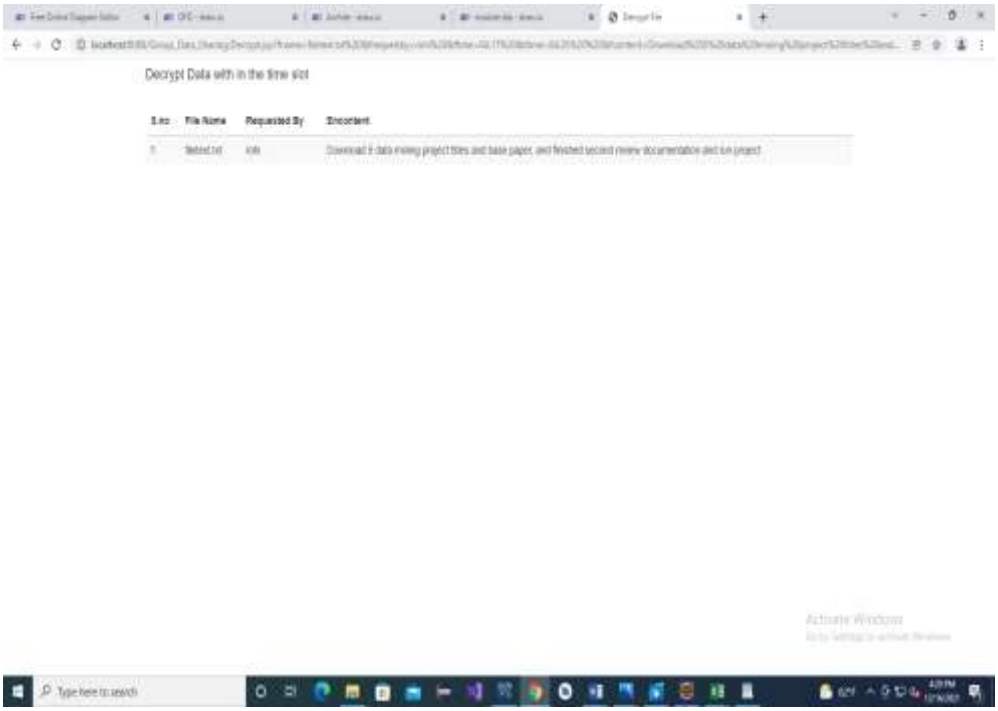
Description: Again, we are come to data user homepage



Screen 29 : Decrypt Data with In the Time slot

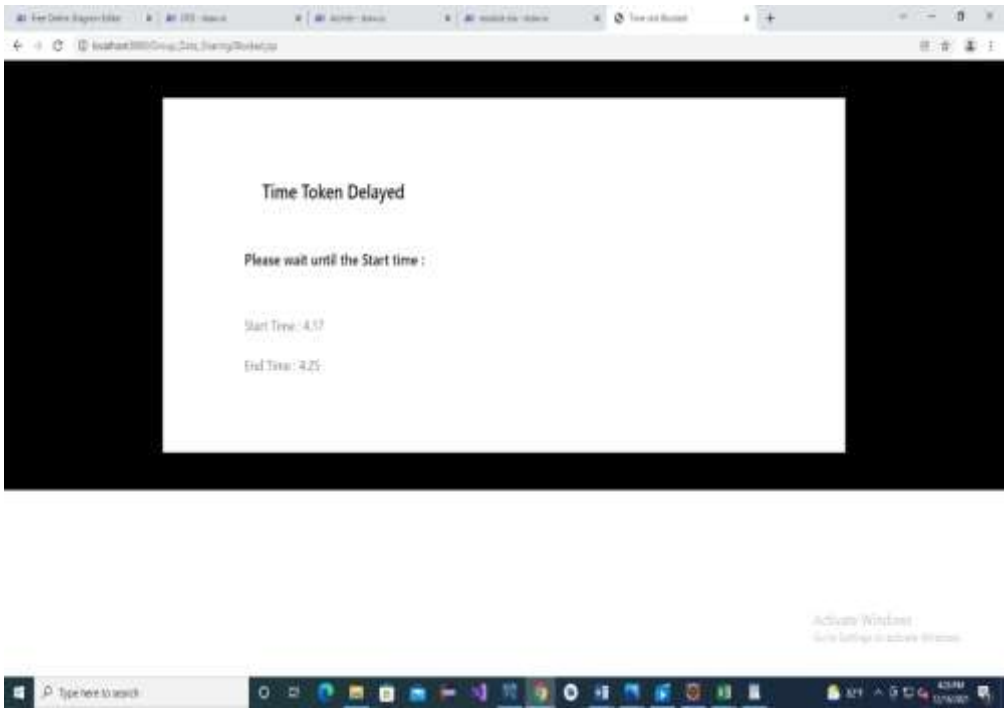
Description: User can decrypt the data within the time slot

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 10 Oct. 2022, pp: 741-758 www.ijaem.net ISSN: 2395-5252



Screen 30 :Display the Output

Description: After user can decrypt the data it shows the output



Screen 31:Time Token Delayed

Description: The data user can not open the file with in the time it showsthetimedelayed.After thetime delay theusercannot seethe data file

IV. CONCLUSION

Finally I conclude that , A Data Pool Share And Dispersion Securely With Attribute And Time Cases in Public Cloud based on attribute-based and timed-release conditional identity-based broadcast PRE. Our scheme allows users to share data with a group of receivers by using identity such as email and username at one time, which would guarantee data sharing security and convenience in public cloud. Besides, with the usage of fine-grained and timed-release CPRE, our scheme allows data owners to custom access policies and time trapdoors in the cipher text which could limitthed is semination conditions when out sourcing their data. The CSP will re encrypt the cipher text successfully only when the attributes of data disseminator associated with the re-encryption key satisfy access policy.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[2] C.Delegable,"Identity-basedBroadcastEncryptionwithConstantSize Ciphertexts and Private Keys," Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215,2007.

[3] F. Beato, S. Maul, and B. Prenell, "Practical Identity-based Private Sharing for Online Social Networks," Computer Communications, vol vol. 73, pp. 243-250,2016.

[4] J. Bettencourt, A. Sahai, and B. Waters, "Ciphertext-policy Attribute based Encryption," Proc. the 28th IEEE Symposium on Security and Privacy (S&P 2007), pp. 321-334,2007.

[5] Z. Wan, J. Liu, and R. Deng, "HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754,2012.

[6] H. Hu, G. An, and J. Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 7, pp. 1614-1627,2013.

[7] M.Blaze,G.Blumer,andM.Strauss,"DivertibleProtocolsandAtomic Proxy Cryptography," Proc. Advances in Cryptology EUROCRYPT .