IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

A Privacy-Preserving and Untraceable Group Data Sharing Scheme In Cloud Computing

Mrs .R. Jhansi Rani[1] , R. Praveen[2], T. Haribabu[3]

[1] Assistant Professor, Department of Computer Applications , Chadalawada Ramanamma Engineering College Tirupati , Andhra Pradhesh, India.

[2,3] Student, Department of Computer Applications, Chadalawada Ramanamma Engineering College
Renigunta Rd, Tirupati, Andhra Pradesh, India

Abstract:

With the development of cloud computing, large amounts of storage data require secure and efficient data exchange. When multiple parties share storage data, the confidentiality of the shared data is first ensured to achieve privacy protection. Second Security of stored data is guaranteed. In other words, if the stored common data is frequently accessed and manipulated, the address of the server Sequences or access patterns are hidden. Therefore, it is necessary to determine how untraceability of stored data can be guaranteed, or how data can be effectively hidden. Access patterns are difficult when sharing stored data. Use proxy re-encryption privacy-preserving and untraceable schemes have been proposed to support multiple users sharing data in cloud computing. In addition Group members and proxies, on the other hand, use the key exchange phase to obtain keys and, if necessary, resist collusion by multiple parties or the ciphertext obtained following the re-encryption phase of the proxy allows group members to implement access controls and store data. This completes the secure data sharing. On the other hand, this paper achieves data untraceability and hidden data access patterns. Moreover, based on the designed structure and a tuple of pointers to identify malicious users and prevent data tampering. Security analysis is based on protocols the features designed in this paper can meet proxy re-encryption.

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

2. **Literature Survey**:

Multiparty Access Control for Online Social Networks: Model and Mechanisms

Online social networks (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. To this end, we propose an approach to enable the protection of shared data associated with multiple users in OSNs. We formulate an access control model to capture the essence of multiparty authorization requirements, along with a multiparty policy specification scheme and a policy enforcement mechanism. Besides, we present a logical representation of our access control model that allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. We also discuss a proof-of-concept prototype of our approach as part of an application in Facebook and provide usability study and system evaluation of our method.

Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud Email

Peng Xu, Tengfei Jiao, Qianhong Wu, Wei Wang, Hai Jin

Recently, a number of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), Identity-Based PRE (IPRE) and Broadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a verstatile primitive referred to as Conditional Identity-based Broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple receivers by specifying these receivers' identities, and the sender can delegate a re-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, the re-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows the original sender to enforce access control over his remote ciphertexts in a fine-grained manner. We propose an efficient CIBPRE scheme with provable security. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption key are all in constant size, and the parameters to generate a re-encryption key is independent of the original receivers of any initial ciphertext. Finally, we show an application of our CIBPRE to secure cloud email system advantageous over existing secure email systems based on Pretty Good Privacy protocol or Identity-Based Encryption.

TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud

Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong

The new paradigm of outsourcing data to the cloud is a double-edged sword. On the one hand, it frees data owners from the technical management, and is easier for data owners to share their data with intended users. On the other hand, it poses new challenges on privacy and security protection. To protect data confidentiality against the honestbut-curious cloud service provider, numerous works have been proposed to support finegrained data access control. However, till now, no schemes can support both fine-grained access control and time-sensitive data publishing. In this paper, by embedding timed-release encryption into CP-ABE (Ciphertext-Policy Attribute-based Encryption), we propose a new time and attribute factors combined access control on time-sensitive data for public cloud storage (named TAFC). Based on the proposed scheme, we further propose an efficient approach to design access policies faced with diverse access requirements for time-sensitive data. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for time sensitive data storage in public cloud.

Towards Secure Data Distribution Systems in Mobile Cloud Computing

Jiang Zhang, Zhenfeng Zhang, and Hui Guo

Though the electronic technologies have undergone fast developments in recent years, mobile devices such as smartphones are still comparatively weak in contrast to desktops in terms of computational capability, storage etc, and are not able to meet the increasing demands from mobile users. By integrating mobile computing and cloud computing, mobile cloud computing (MCC) greatly extends the boundary of the mobile applications, but it also inherits many challenges in cloud computing, e.g., data privacy and data integrity. In this paper, we leverage several cryptographic primitives such as a new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC, which provides data privacy, data integrity, data authentication, and flexible data distribution with access control. Compared to traditional cloud-based data storage systems, our system is a lightweight and easily deployable solution for mobile users in MCC since no trusted third parties are involved and each mobile user only has to keep short secret keys consisting of three group elements for all cryptographic operations. Finally, we present extensive performance analysis and empirical studies to demonstrate the security, scalability, and efficiency of our proposed system.

3. System Analysis

Existing System:

Data sharing in cloud computing can be utilized in many fields to solve some difficult problems, but it also brings about some security issues. On the one hand, it is difficult to ensure the confidentiality of the ciphertext to preserve data privacy. Moreover, group data sharing in a many-to-many mode is a challenge. The scheme is based on bilinear mapping, but some problems cannot resist collusion attacks and encounter difficulty in revoking malicious users. It is difficult to ensure that data are not tracked and access patterns are not exposed to the server. However, the data storage structure used on the proxy or server side will affect the security and overhead of the entire data storage process. Thus, most researchers reduce communication and storage overhead by designing a reasonable data storage structure to achieve secure and efficient data storage.

Disadvantages:

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

Proposed System

In this proposed proxy re-encryption privacy-preserving and untraceable schemes have been proposed to support multiple users sharing data in cloud computing. In additionGroup members and proxies, on the other hand, use the key exchange phase to obtain keys and, if necessary, resist collusion by multiple parties orthe ciphertext obtained following the re-encryption phase of the proxy allows group members to implement access controls and store data.This completes the secure data sharing. On the other hand, this paper achieves data untraceability and hidden data access patterns.Moreover, based on the designed structureand a tuple of pointers to identify malicious users and prevent data tampering. Security analysis is based on protocolsthe features designed in this paper can meet proxy re-encryption.

Advantages

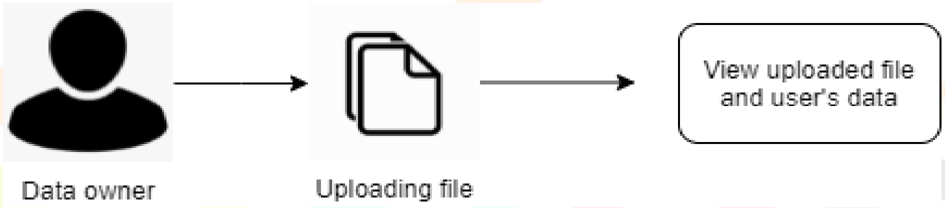
- Improved performance
- Confidentiality
- Collusion resistance
- Flexibility and scalability

4. Implementation

- Data owner uploads and view files
- Data user View file and give request to access file
- Authority distribute file to disseminator
- Disseminator re-encrypt the file
- Cloud server stores data

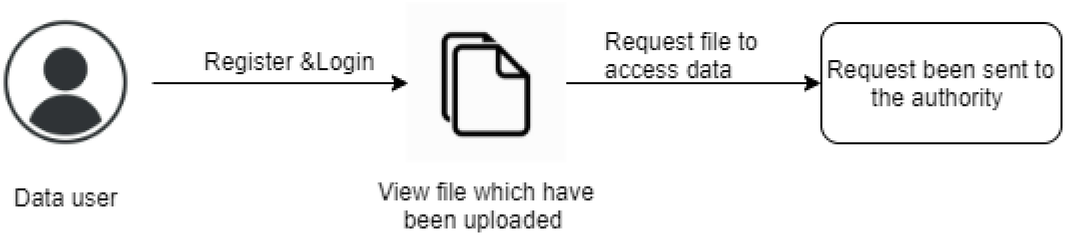
Data Owner Uploads and View Files

Data owner register and login & uploads file which is stored in database in encrypted form and also view files and user’s data.



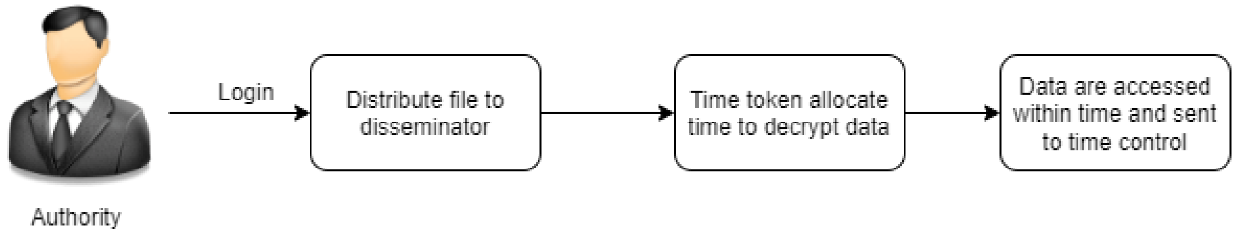
Data User View File and Give Request to Access File

Data user register and login & can view uploaded file and request file to access the data to the authority. The re-encrypted data are received from the disseminator and control time using time control then send to authority with time token. After receive from time token user can decrypt the file and access data within time.


Register &Login
Request file to access data
Request been sent to the authority
Data user
View file which have been uploaded

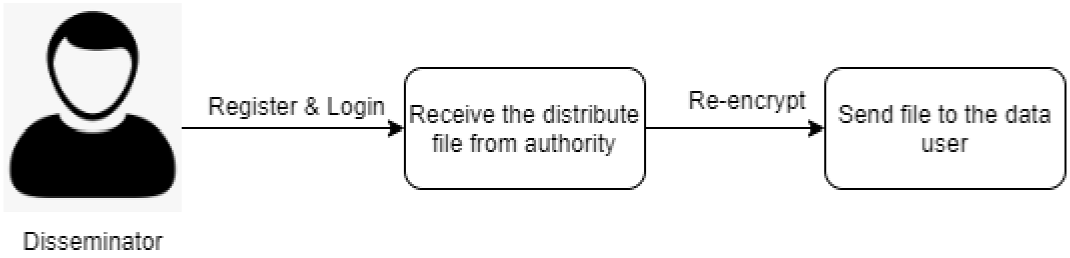
Authority distribute file to disseminator

Authority login and distribute file to disseminator. The time token allocate time for the data user to decrypt the data and access within time and send to time control.


Authority
Login
Distribute file to disseminator
Time token allocate time to decrypt data
Data are accessed within time and sent to time control

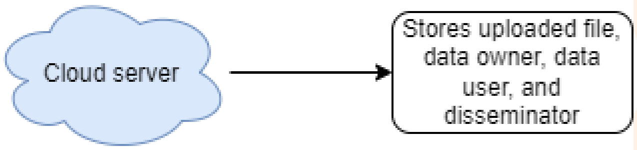
Disseminator re-encrypt the file

Disseminator register and login then receive the distributed file then re-encrypt and send the file to data user.


Disseminator
Register & Login
Receive the distribute file from authority
Re-encrypt
Send file to the data user

Cloud server stores data

Cloud server stores data of uploaded files, data owner, data user, and disseminator


Cloud server
Stores uploaded file, data owner, data user, and disseminator

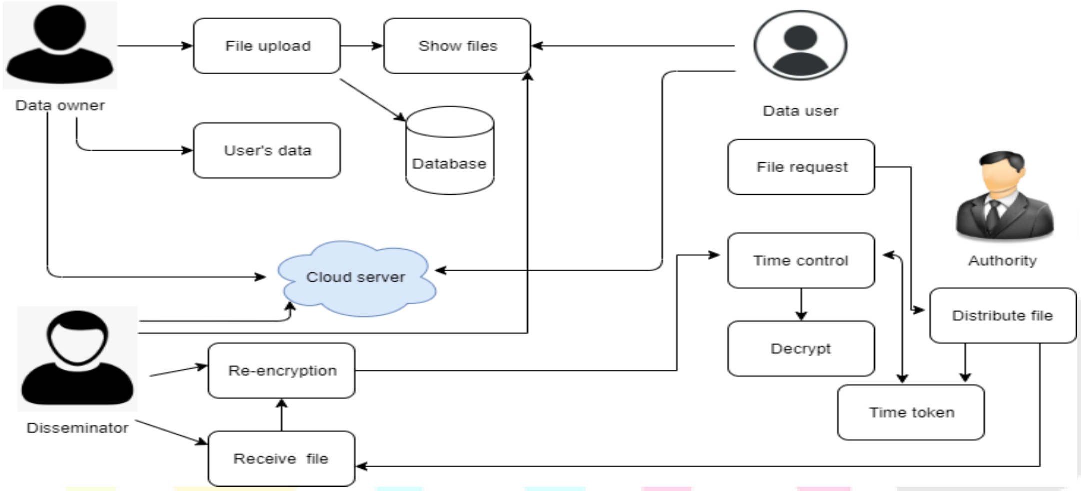
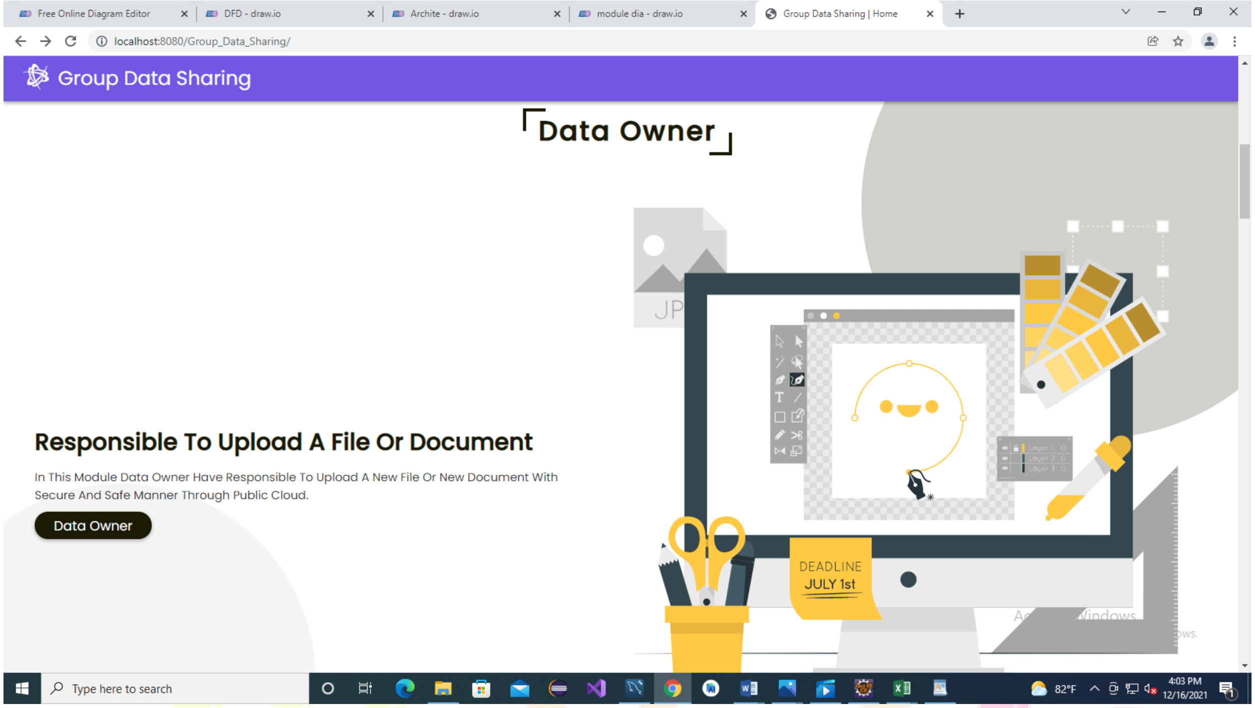


Fig 1 Architecture

5. Screenshots



Group Data Sharing

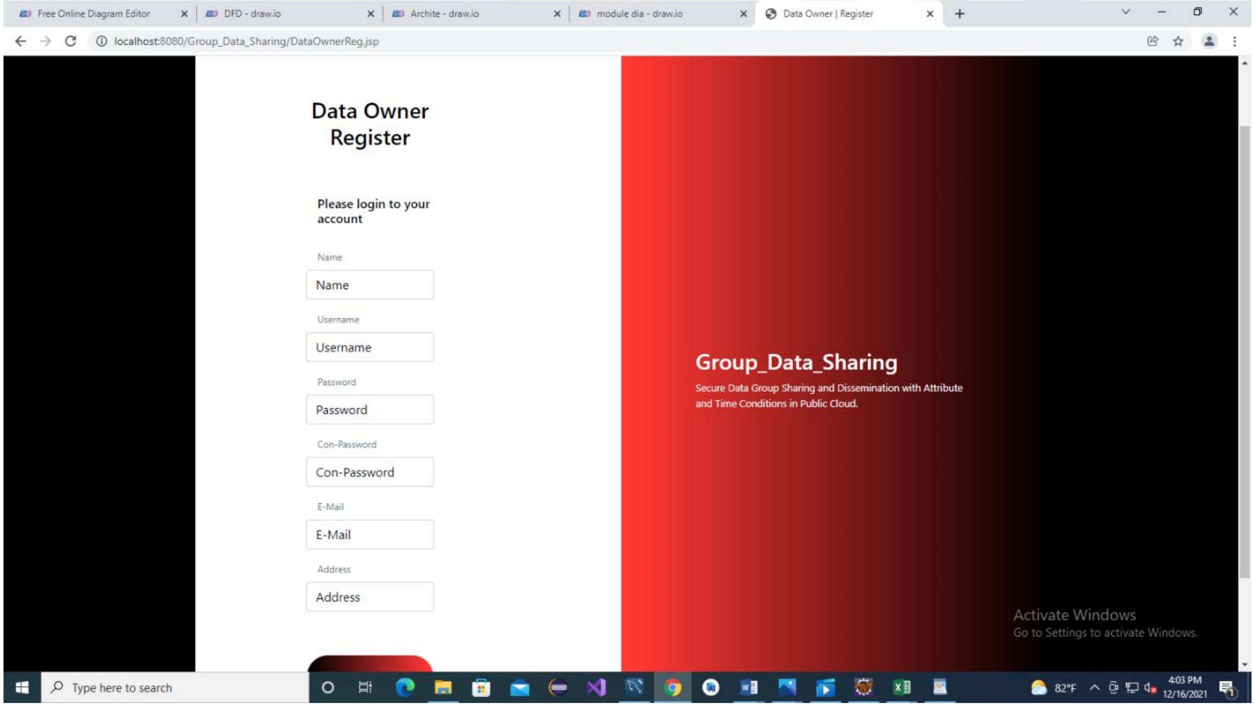
Data Owner

Responsible To Upload A File Or Document

In This Module Data Owner Have Responsible To Upload A New File Or New Document With Secure And Safe Manner Through Public Cloud.

Data Owner

Fig 2: Home Page



Data Owner Register

Please login to your account

Name

Name

Username

Username

Password

Password

Con-Password

Con-Password

E-Mail

E-Mail

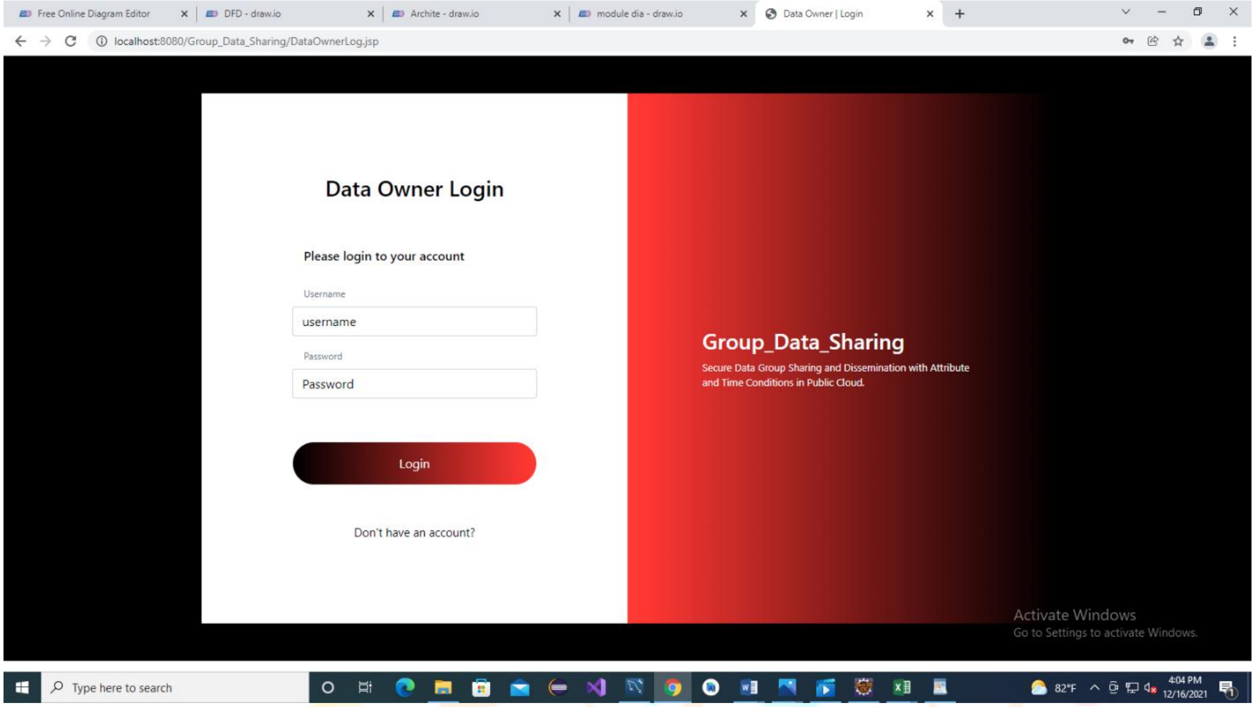
Address

Address

Group_Data_Sharing

Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud.

Fig 3: Owner Page



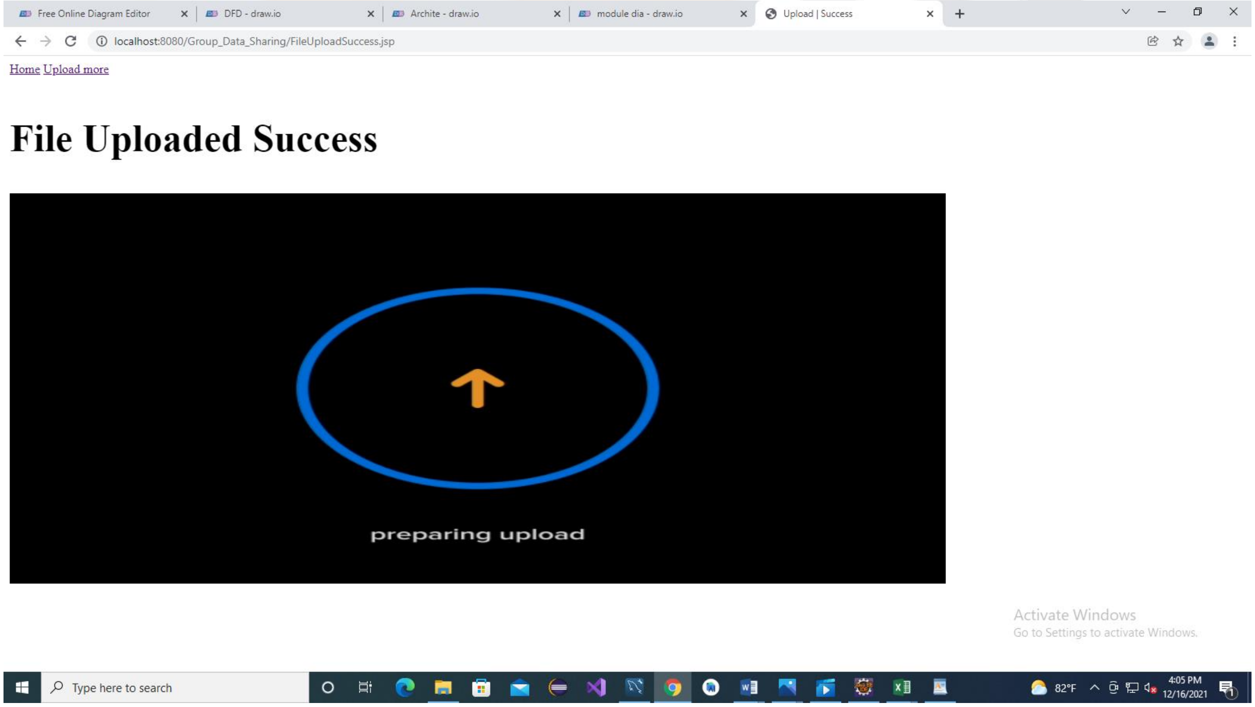
Data Owner Login

Please login to your account

Group_Data_Sharing

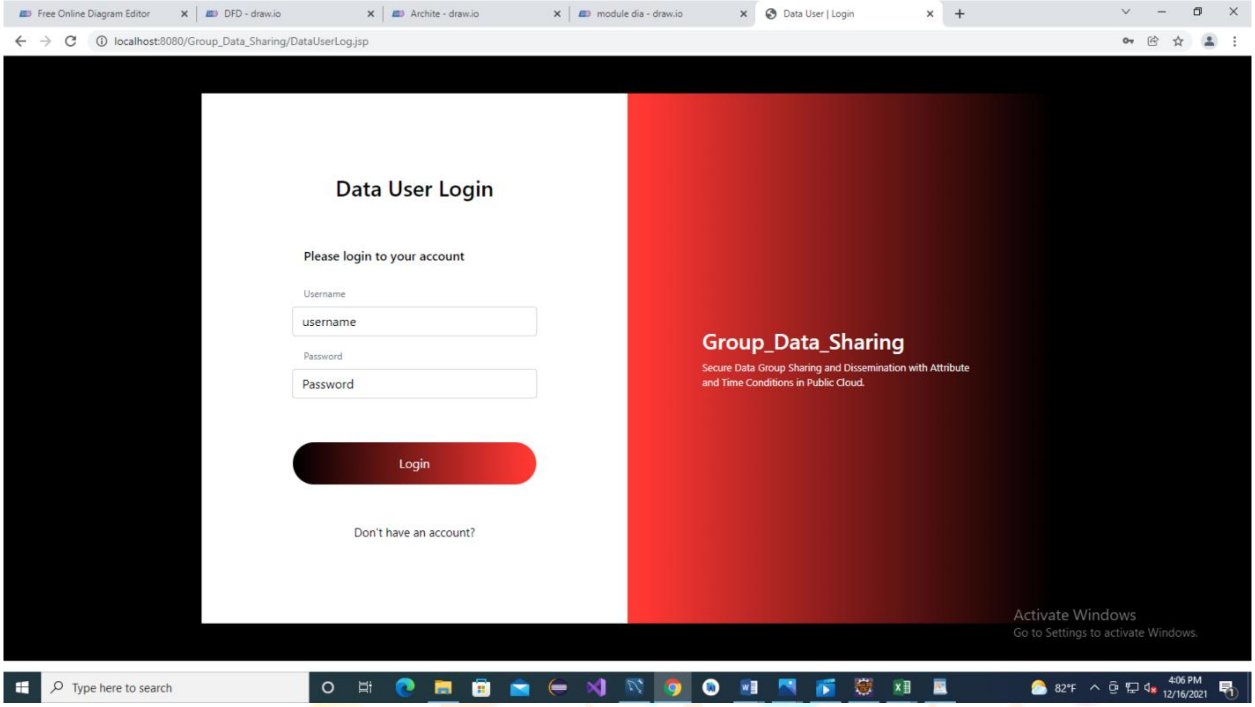
Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud.

Fig 4 Login Page



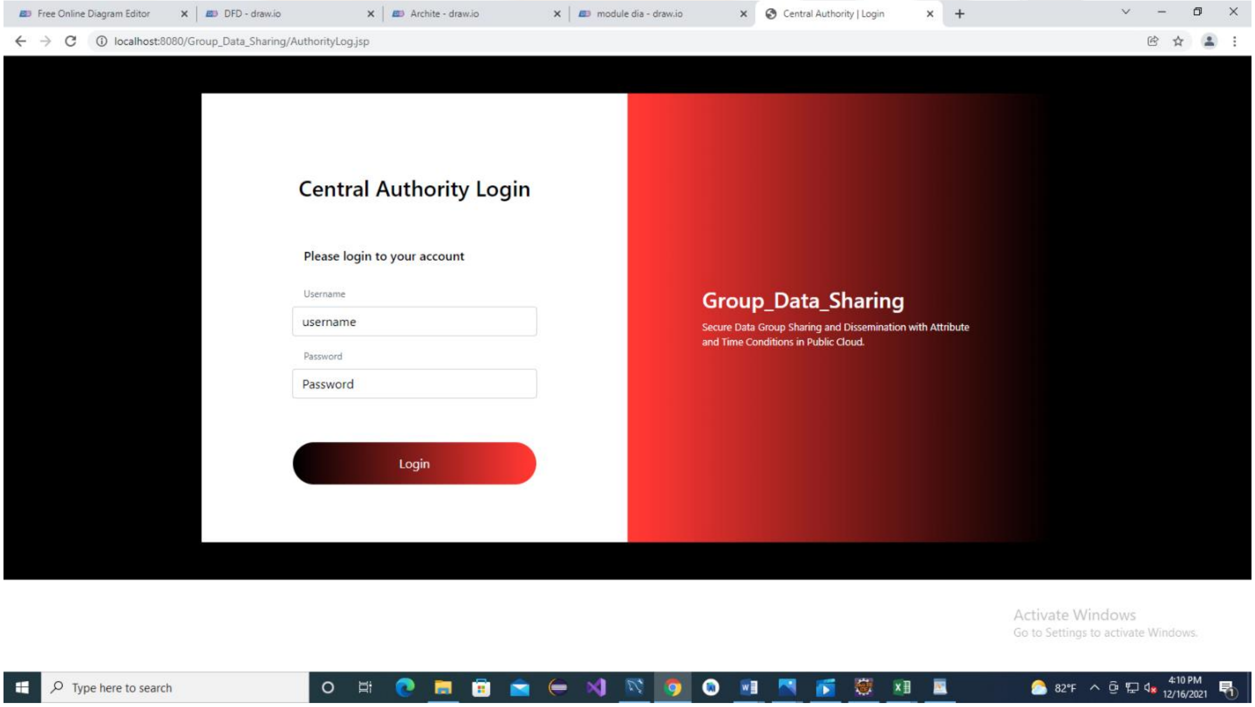
File Uploaded Success

Fig 5 Uploading the data



Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud.

Fig 6 User page



Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud.

Fig 7 Central Authority page

6. **Conclusion**:

In this project, we propose a secure data group sharing and dissemination scheme in public cloud based on attribute-based and timed-release conditional identitybased 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 ciphertext which could limit the dissemination conditions when outsourcing their data. The CSP will re-encrypt the ciphertext 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. Delerablée, “Identity-based Broadcast Encryption with Constant Size 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. Meul, and B. Preneel, “Practical Identity-based Private Sharing for Online Social Networks,” Computer Communications, vol. 73, pp. 243-250, 2016.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy Attributebased 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. Ahn, 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. Bleumer, and M. Strauss, “Divertible Protocols and Atomic Proxy Cryptography,” Proc. Advances in CryptologyEUROCRYPT 1998 (EUROCRYPT '98), pp.127-144, 1998.

[8] D. Tran, H. Nguyen, W. Zha, and W. Ng, “Towards Security in Sharing Data on Cloud-based Social Networks,” Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011), pp. 1-5, 2011.

[9] J. Weng, R. Deng, X. Ding, C. Chu, and J. Lai, “Conditional Proxy ReEncryption Secure Against Chosen-ciphertext Attack,” Proc. the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (CCS 2009), pp. 322-332, 2009.

[10] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, “Conditional Identitybased Broadcast Proxy Re-encryption and its Application to Cloud Email,” IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79, 2016.

[11] Y. Yang, H. Lu, J. Weng, Y. Zhang, and K. Sakurai, “Fine-grained Conditional Proxy Re-encryption and Application,” Proc. the 8th International Conference on Provable Security (ProvSec 2014), pp. 206-222, 2014.

[12] J. Hong, K. Xue, W. Li, and Y. Xue, “TAFC: Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud,” Proc. 2015 IEEE Global Communications Conference (GLOBECOM 2015), pp. 1-6, 2015.

[13] R. Rivest, A. Shamir, and D. Wagner, “Time Lock Puzzles and Timed-release Crypto,” Massachusetts Institute of Technology, MA, USA, 1996.

[14] J. Zhang, Z. Zhang, H. Guo, “Towards Secure Data Distribution Systems in Mobile Cloud Computing,” IEEE Transactions on Mobile Computing, 2017, doi: 10.1109/TMC.2017.2687931

[15] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, “A Survey of Proxy Reencryption for Secure Data Sharing in Cloud Computing,” IEEE Transactions on Services Computing, 2016, doi: 10.1109/TSC.2016.2551238.