IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⋇ Impact Factor 7.105 ⋇ Vol. 9, Issue 5, May 2022

DOI: 10.17148/IARJSET.2022.9540

An Efficient Attribute Based Encryption Scheme With Policy Update and File Update in Cloud Computing

Pradnya Mane[1], Bhavana Choudhari[2], Snehal Shinde[3], Rahul Patil[4], Sagar Mali[5]

Student, Computer Science, Adarsh Institute of Technology & Research Center, Vita, India[1 ,2,3,4]

Assistant Prof, Computer Science, Adarsh Institute of Technology & Research Center, Vita, India[5]

Abstract: Security and privacy are very important issues in cloud computing. Thus, with these versatile cloud services, when the weak data stored within the cloud storage servers, there are some challenging which has to be managed like its security issues, Data Privacy, Data Confidentiality, Data Sharing and its integrity over the cloud servers dynamically. In this vast environment, authenticity and data access control must also be maintained. In the cloud computing environment, attribute–based encryption (ABE) is a significant version of cryptographic technique. The basic technique for ABE is public key encryption, which provides one too many encryptions. Here, the private key of users and the cipher-text both rely on attributes, such that decryption is only possible when the set of attributes of users key matches the set of attributes of cipher-text with its corresponding access policy. Thus, an opponent could grant access to the sensitive information that holds multiple keys, if it has at least one individual key for accession. The techniques based on ABE consist of two types KP-ABE (Key policy ABE) where the user's personal key is linked to an access structure (or access policy) over attributes and cipher-text is connected to the set of attributes, and CP-ABE (cipher-text policy ABE) is vice versa. Finally, experiment simulation shows that the proposed scheme is highly efficient in terms of policy update and file update.

Keywords: Attribute-based encryption (ABE), Cipher text policy (CP), Cloud computing, File update, Policy update

I. INTRODUCTION

Cloud computing is a new trend of computing where resources like storage, computation poor, network, applications etc. are delivered as services. Pay as you consume cloud computing paradigm has turned out to be more pervasive, its advantages for consumers, including a large number of convenient services, relief of the burden for storage, adaptable in information access, decrease of expense on equipment and software. Many companies have their maintenance and they provide lots of cloud computing services. More and more sensitive data from consumers have been concentrated in to the cloud for its flexible management and economic savings. It is an exceptionally hard to look the most suitable services or products for ordinary consumers, as there are so many services and products in cloud. It is very general that before out sourcing the sensitive data it is encrypted. It is a typical observes to encrypt sensitive data before out sourcing. Hover data encryption makes existing search techniques on plain text not applied to cipher text, thus prompting an enormous challenge to effective knowledge utilization, it is difficult to encrypting full data first and then decrypting that data, due to the large bandwidth and computation burden. Consumers may need to retrieve only certain specific data less they are fascinated of the whole data collection. A most suitable way to solve this problems is searchable encryption, which can retrieve particular less through keyword-based search with protecting data and keyword privacy-preserving. Cloud services provide great conveniences for the users to enjoy the on demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other user for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. Several schemes employing attributes based encryption (ABE) have been proposed for access control of out sources data in cloud computing. It enables customers with limited computational resource to their large computation workloads to the cloud economically enjoy the massive computational poor, bandwidth, storage, and even appropriate software that can be shared in a pay-per use manner. Despite the tremendous benefits, security is the primary obstacle that prevents the wide adoption of this promising computing model, especially for customers when their confidential data are consumed and produced during the computation. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud performing any meaningful operation of the underlying cipher text-policy, making the computation over encrypted data a very hard problem. The proposed scheme not only achieves scalability due to its hierarchical structure. As a result, their do exit various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e. they may behave beyond the classical semi honest model. Data backed up to a cloud storage library can be de-duplicated. Deduplication eliminates redundant data segments from the backup and the storage target over WAN. Deduplication with cloud storage not only reduces the storage space requirements. In computing, data deduplication is a specialized data compression technique and can also be applied to network data transfer to reduce the number of bytes that must be sent. In the deduplication process, unique chunks of data, or byte patterns, are identified and stored during a process of analysis.

II. WORKFLOW AND METHODOLOGY

1. Registration

User enter its own information such as name, email id, mobile no, login name, password register to cloud and password must be eight characters long, and also password include alphabets, numbers then it's account is created on cloud. If user wants to cancel this registration, then user cancels this registration.

2. Login

If user is already registered then, user login on cloud using login name and password so he gets access of his account. If user is new then first user registered to cloud using name, email id, mobile no, login name, password

3. Upload

When user login on cloud then user want to upload any text or documents file by entering description such as name of file and browse file from where it is stored, then this file is stored in his account on cloud.

4. Download

If user wants to access any file from his account then there is present information of all files such as file id, title, and file name uploaded data and time and also secret key which is used for encrypting file then the select those files that he want and download.

5. Share

If user wants to share any files then share files with session using mobile number to other user. Then secrete key of that file which is used for encryption is sent to e-mail of another user. Using that key, file is decrypted by that another user. If the session is expired then key is not useful for that file. So, again request for the new key.

6. De-duplication

At the time if uploading file, the file is uploaded on cloud with avoiding duplication. In that de-duplication, an effective data compression approach that exploits data redundancy, partition large data object into smaller parts, called chunks, represents these chunks by their fingerprints, replace the duplicate chunks with their fingerprints after chunk fingerprint index lookup, and only transfer or stores the unique chunks for the purpose of communication or storage efficiency.

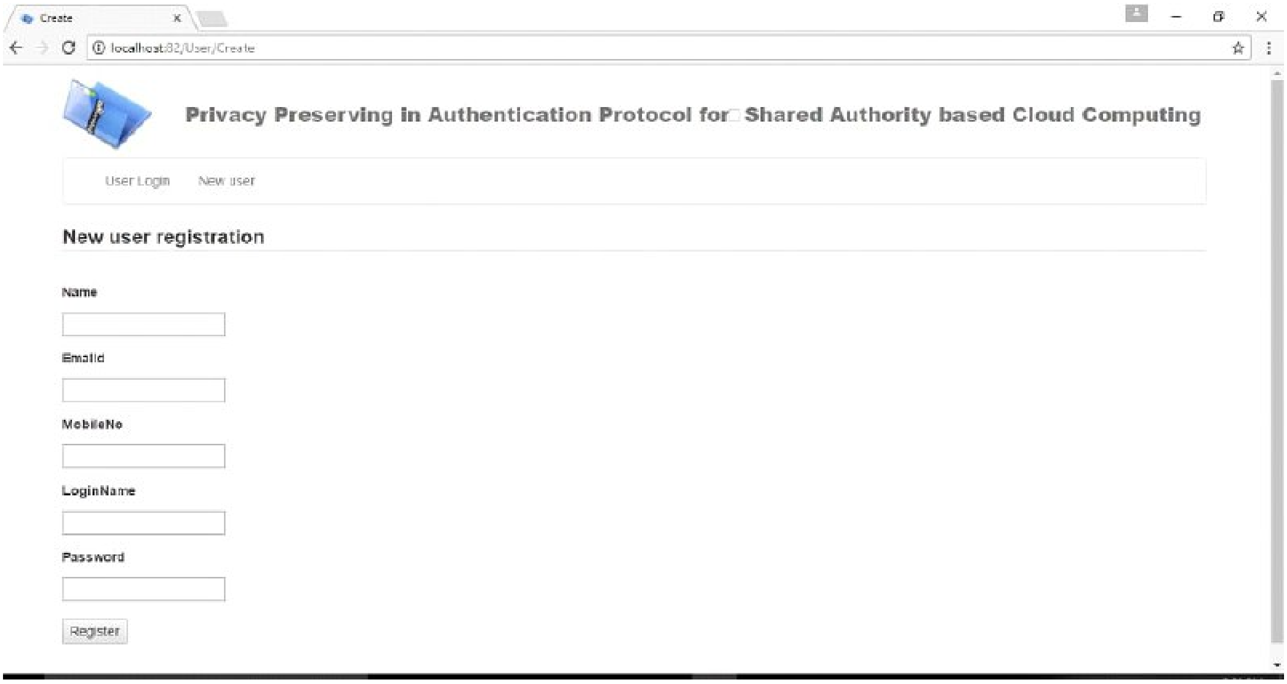
7. Logout

First user register to cloud by entering its own information, then user login to cloud the he gets access to his own account, then user want to upload any file, then it uploaded on his account and if user want to access any file, then he select the file and downloaded that file and if user want to delete any file, then he deleted and finally all operations of user is completed then user logout from cloud.

III. RESULT

There are already well-known existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user privacy. The existing system define shared authority based privacy-preserving authentication protocol which allows security and policy in the cloud storage. In this, shared access authority is achieved by anonymous access request matching mechanism with security and privacy consideration. Attribute based access control adopted to realize that the user can only access its own data fields; proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

DOI: 10.17148/IARJSET.2022.9540



Privacy Preserving in Authentication Protocol for Shared Authority based Cloud Computing

New user registration

Name

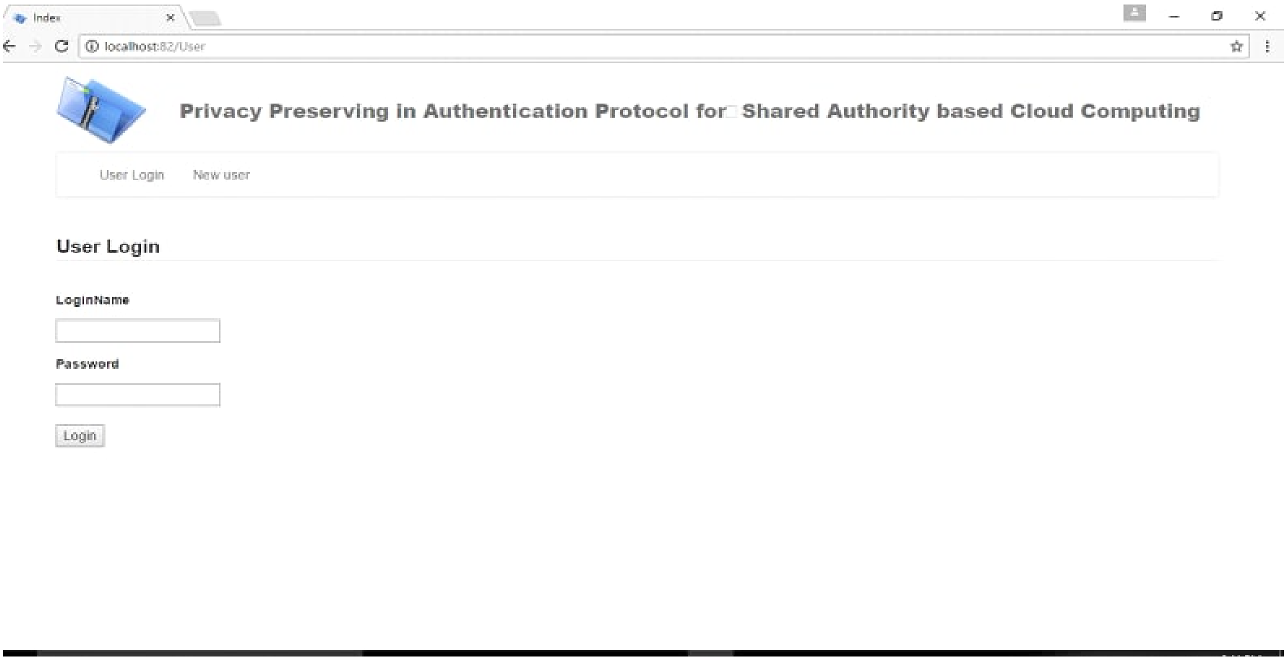
EmailId

MobileNo

LoginName

Password

Fig.1: User register with basic information such as name, mobile no, Email id, login-name and password.



Privacy Preserving in Authentication Protocol for Shared Authority based Cloud Computing

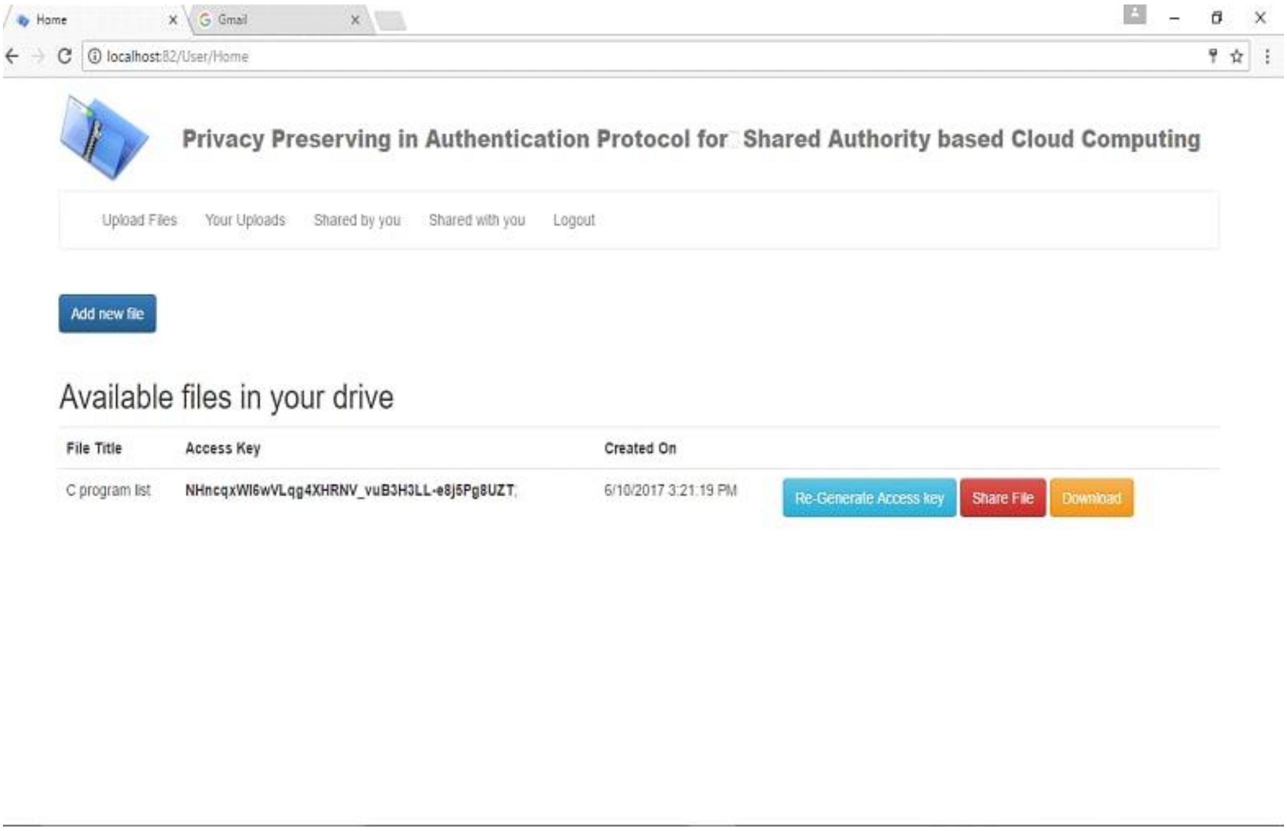
User Login

LoginName

Password

Fig.2: After registration user login to his own account

DOI: 10.17148/IARJSET.2022.9540

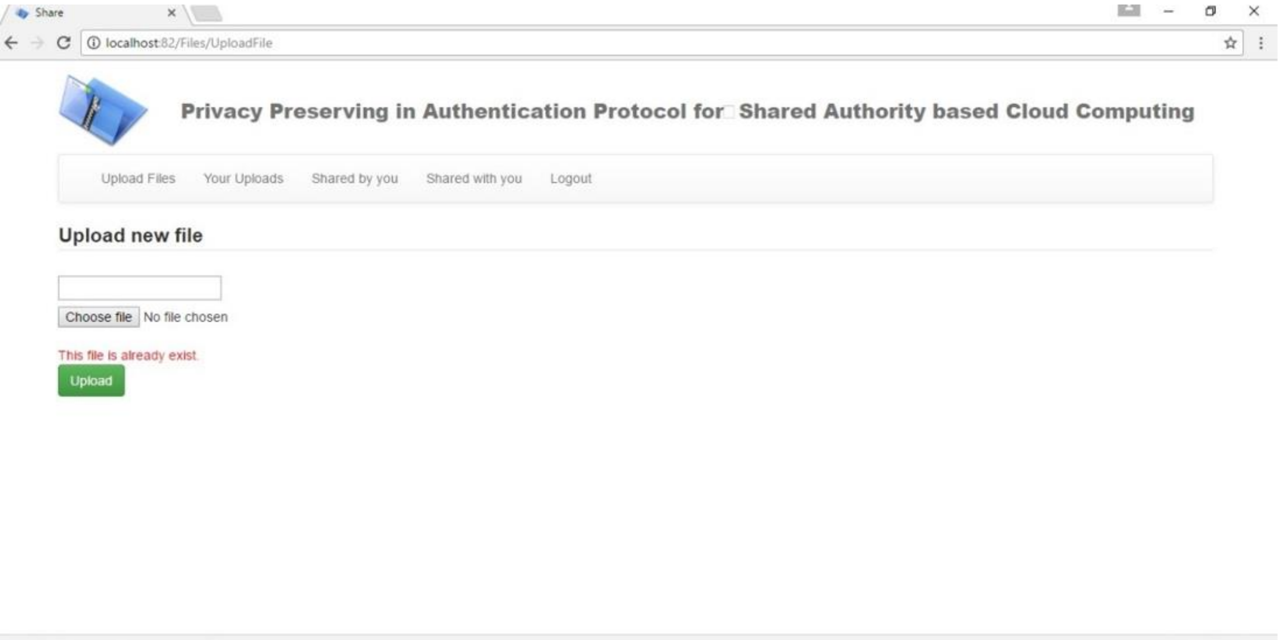


Privacy Preserving in Authentication Protocol for Shared Authority based Cloud Computing

Available files in your drive

File Title	Access Key	Created On
C program list	NHncqxWI6wVLqg4XHRNV_vuB3H3LL-e8j5Pg8UZT,	6/10/2017 3:21:19 PM

Fig.3: After login user homepage



Privacy Preserving in Authentication Protocol for Shared Authority based Cloud Computing

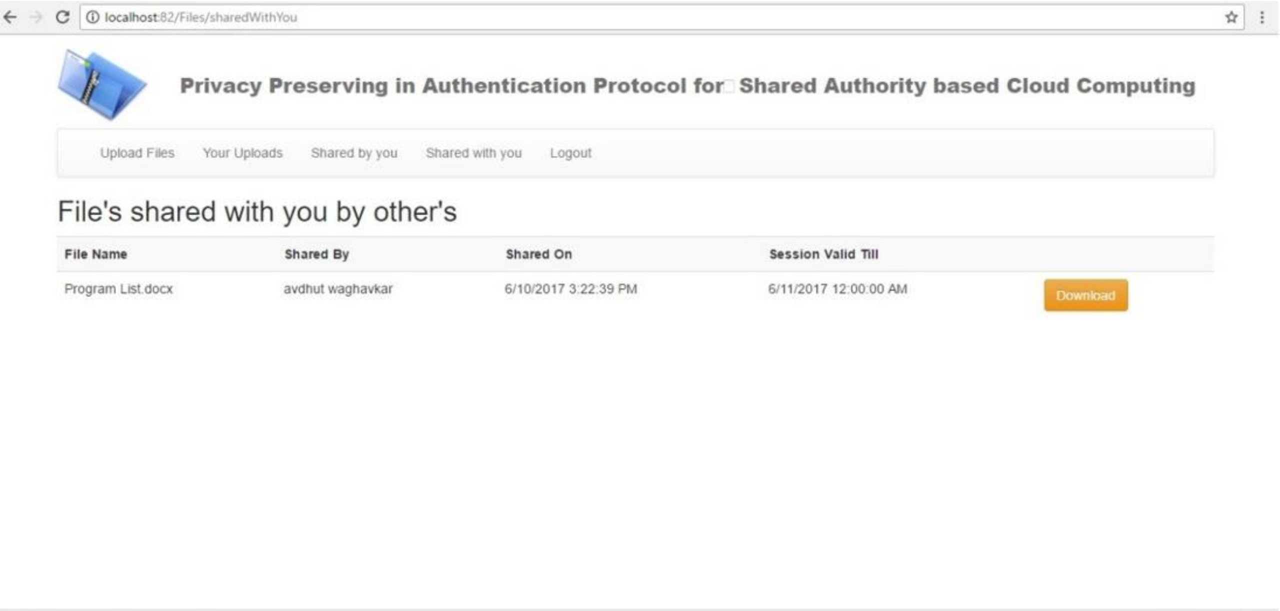
Upload new file

No file chosen

This file is already exist.

Fig 4: After login user uploading new file

DOI: 10.17148/IARJSET.2022.9540


localhost:82/Files/sharedWithYou
Privacy Preserving in Authentication Protocol for Shared Authority based Cloud Computing
Upload Files
Your Uploads
Shared by you
Shared with you
Logout
Download

File's shared with you by other's

File Name	Shared By	Shared On	Session Valid Till	
Program List.docx	avdhut waghavkar	6/10/2017 3:22:39 PM	6/11/2017 12:00:00 AM	Download

Fig .5 After uploading file own his account

IV. CONCLUSION

In this article, an efficient CP-ABE scheme is proposed that can support the policy update and file update in cloud computing. The policy update is obtained by using the initial encryption data to generate the update parameters. It can effectively reduce the communication cost, storage, cost, and computing cost of the system. Meanwhile, the file update model is also constructed, which can enhance the system security and reduce the computational cost of data owner. In addition, we provide that the proposed scheme is secure under the assumption of the decision q-parallel BDHE. In the further, the proposed system motivates some interesting open problems. For example, how to further reduce the file update time cost and how to use block chain technology to solve the policy update and file update.

V. ADVANTAGES

1. We provide the security for the data stored on the cloud
2. Files are stored on cloud in encrypted format.
3. User also shares the file to another user with session. If sessions expired the key is not useful for that file.
4. In result, with the help of ABE and AES algorithm privacy preserve for each single user.
5. Because of this system shoulder surfing can remove.
6. Upload big files may takes some server millisecond time but it negligible but security and privacy is achieved.

REFERENCES

1. IEEE Transactions on Industrial Information, VOL.15 NO.12, December 2019.
2. 2020 IEE International Conference on Power, Intelligent Computing and System (ICPICS).
3. Jingwei Li, Dongging Xie and Zhang CAI "Secure Auditing and Deduplication Date in cloud" TC DOI 10.1109/TC.2015.2389960, IEEE Transactions on Computers 2015.
4. J.Bethencourt, A. Sahai, and B. Waters. "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, 2007, pp.321-334.
5. Amol D Shelkar, prof. Rucha. R. Galgali, "Data Access Privilege with Attribute Based Encryption and user Revocation," International Research Journal of Engineering and Technology (IRJET), Nov 2016.