International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 3 230- 236

Robust Multiple Authority and ABE for Access Control in Cloud Computing

Ms. Mona Padole, Prof. Nutan Dhande

Department of Computer Science and Engineering

ACE Nagthana Wardha Maharashtra

***Abstract*:** Data access control is a challenging issue in public cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Users may be stuck in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. Although multi authority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point bottleneck and low efficiency, due to the fact that each of the authorities still independently manages a disjoint attribute set. In this paper we propose a system that improves the approach of CP-ABE from text based asymmetric to Image based symmetric approach for faster encryption as well as access to data. We also propose a multiple access policy generation for single user where we will be able to implement one to many and many to many methodology.

***Keywords**: Cloud storage, Access control, CPABE. AES Encryption*

*****

INTRODUCTION

Cloud storage is a promising and important service paradigm in cloud computing [1–4]. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to name just a few. Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which is a critical issue to ensure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, finegrained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labeled with his/her own attributes. Only if the attributes associated with the user's secret key satisfy the access structure, can the user decrypt the corresponding ciphertext to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario [5–9], and multiauthority scenario [10–12]. Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation. Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set.

A definition for internet privacy would be the ability to control (1) what information one reveals about oneself, and (2) who can access that information. Essentially, when the data is collected or analyzed without the knowledge or consent of its owner, privacy is violated. When it comes to the usage of the data, the owner should be informed about the purposes and intentions for which the data is being or will be used. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone.

Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings. However, existing proposals for automating privacy settings appear to be inadequate to address the unique

privacy needs of images due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed. The privacy of user data can be given by using two methods.

1. The user alone can enter the privacy preferences
2. Usage of recommendation systems which assist users for setting the privacy preferences.

Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources viz. various types of networks, storage, servers, services and applications, without physically acquiring. So it saves managing cost and time for organizations. In present days cloud computing is one of the greatest platform that provides storage of data at very low cost and is available at any time over the internet. But it has various critical issue in security, load management and fault tolerance. Data sharing refers to storing data at a place where it can use by multiple users, at the same time ensuring the security of data. In this project data is shared using a secured mechanism that makes use of encryption for ensuring security of data as well as it also contains mechanisms for authentication of users.The different security mechanisms used in this project are encryption and compression. The Infrastructure as a Service (IaaS) is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it.

RELATED WORK

2.1 Cloud Computing Security: From Single To Multi-Clouds:

Authors: Cachinet al., Garfinkel

One of the outcomes that they propose is to use a Byzantine blemish tolerant replication tradition inside the cloud. Hendricks et al. express that this outcome can sidestep data pollution made by a couple parts in the cloud. On the other hand, Cachinet al. declare that using the Byzantine blemish tolerant replication tradition inside the cloud is inadmissible in light of the way that the servers having a spot with cloud suppliers use the same structure foundations and are physically set in the same spot [1]. According to Garfinkel, another security danger that may happen with a cloud supplier, for instance, the Amazon cloud organization, is a hacked mystery key or data intrusion. If some person becomes acquainted with an Amazon account mystery key, they will have the ability to get to most of the account's events and resources.

In spite of the way that cloud suppliers are aware of the noxious insider risk, they expect that they have essential responses for alleviate the issue [1]. Rocha and Correia [1] center possible aggressors for Iaas cloud suppliers. For outline, Grosse et al. [1] propose one outcome is to keep any physical access to the servers. In any case, Rocha and Correia [1] battle that the aggressors depicted in their work have remote get to and needn't trouble with any physical access to the servers. Grosse et al. [1] propose a substitute result is to screen OK to get access to the servers in a cloud where the customer's data is secured. In any case, Rocha and Correia [1] declare that this segment is profitable for watching laborer's behavior to the extent whether they are after the assurance course of action of the association or not, in any case it is not fruitful in light of the way that it distinguishes the issue after it has happened.

2.2 Reliable Re-Encryption in Unreliable Clouds:

Authors: Olfa Nasraoui

A substitute technique to secure dispersed registering is for the data holder to store mixed data in the cloud, and issue deciphering keys to endorsed customers. By then, when a customer is denied, the data supervisor will issue re-encryption requests to the cloud to re- scramble the data, to keep the repudiated customer from disentangling the data, and to deliver new unscrambling keys to generous customers, so they can continue getting to the data. Of course, since a conveyed registering environment is included various cloud servers, such summons may not be gotten and executed by most of the cloud servers in view of hazardous framework correspondences [3].

2.3 Ensuring Data Integrity and Security in Cloud Storage:

Authors: Olfa Nasraoui

A substitute way to deal with secures the data using various pressing and encryption computations and to disguise its region from the customers that stores and recuperates it. The primary complexity is that the system presented by OlfaNasraoui [2] is an application based structure like which will keep running on the clients own system. This application will allow customers to exchange record of different associations with security quirks including Encryption and Compression. The exchanged records may be gotten to from wherever using the application which is given.

The security of the OlfaNasraoui [2] model has been examination on the reason of their encryption estimation and the key organization. It has been watched that the encryption count have their own specific qualities; one computation gives security to the detriment of fittings, other is strong however uses more number of keys, one takes also taking care of time. This region exhibits the diverse parameters which accept a vital part while selecting the cryptographic computation. The Algorithm found most ensuring is AES Algorithm with 256 bit key size (256k) [2].

2.4 Key-Aggregate Cryptosystem for Scalable Data Sharing In Cloud Storage:

Authors: Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng

A rule trick of cloud is data advertising. Cheng-Kang Chu, Sherman S. M. Chow, Wen- GueyTzeng, Jianying Zhou, and Robert H. Deng [5] exhibit to securely, adequately, and adapt ably grant data to others in circulated stockpiling. We depict new open key cryptosystems which convey consistent size figure messages such that capable task of unscrambling rights for any arrangement of figure works are possible. The interest is that one can add up to any arrangement of riddle keys and make them as minimized as a lone key, yet wrapping the power of each and every one of keys being collected. Toward the day's end, the puzzle key holder can release a reliable size aggregate key for versatile choices of figure substance set in appropriated stockpiling [5].

PROPOSED METHODOLOGY

The proposed work is planned to be carried out in the following manner.

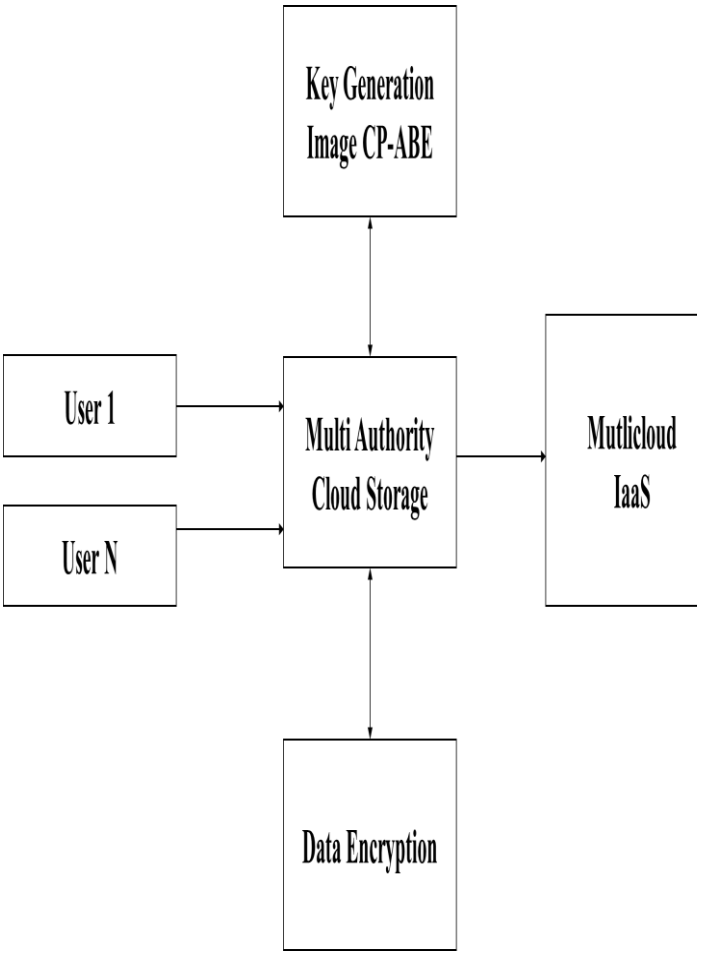


Figure Proposed System Architecture

In proposed system, we present an efficient heterogeneous framework with single CA/multiple AAs to address the problem of single-point performance bottleneck. The novel idea of our proposed scheme is that the complicated and time-consuming user legitimacy verification is executed only once by one selected users. Furthermore, an auditing mechanism is proposed to ensure the traceability of malicious users. Thus our scheme can not only remove the single-point performance bottleneck but also be able to provide a robust, high-efficient, and secure access control for public cloud storage. Also we plan to extend this system from single to multicloud Databases using IaaS.

The cloud that will be used is Google Drive and multiple access will be provided to user based on permission i.e. Read / Write and Delete.

AES Encryption

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable. AES became effective as a federal government standard on May 26, 2002, after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module (see Security of AES,

5.5.1 Architecture and Working of AES

 ISSN: 2321-8169
230- 236

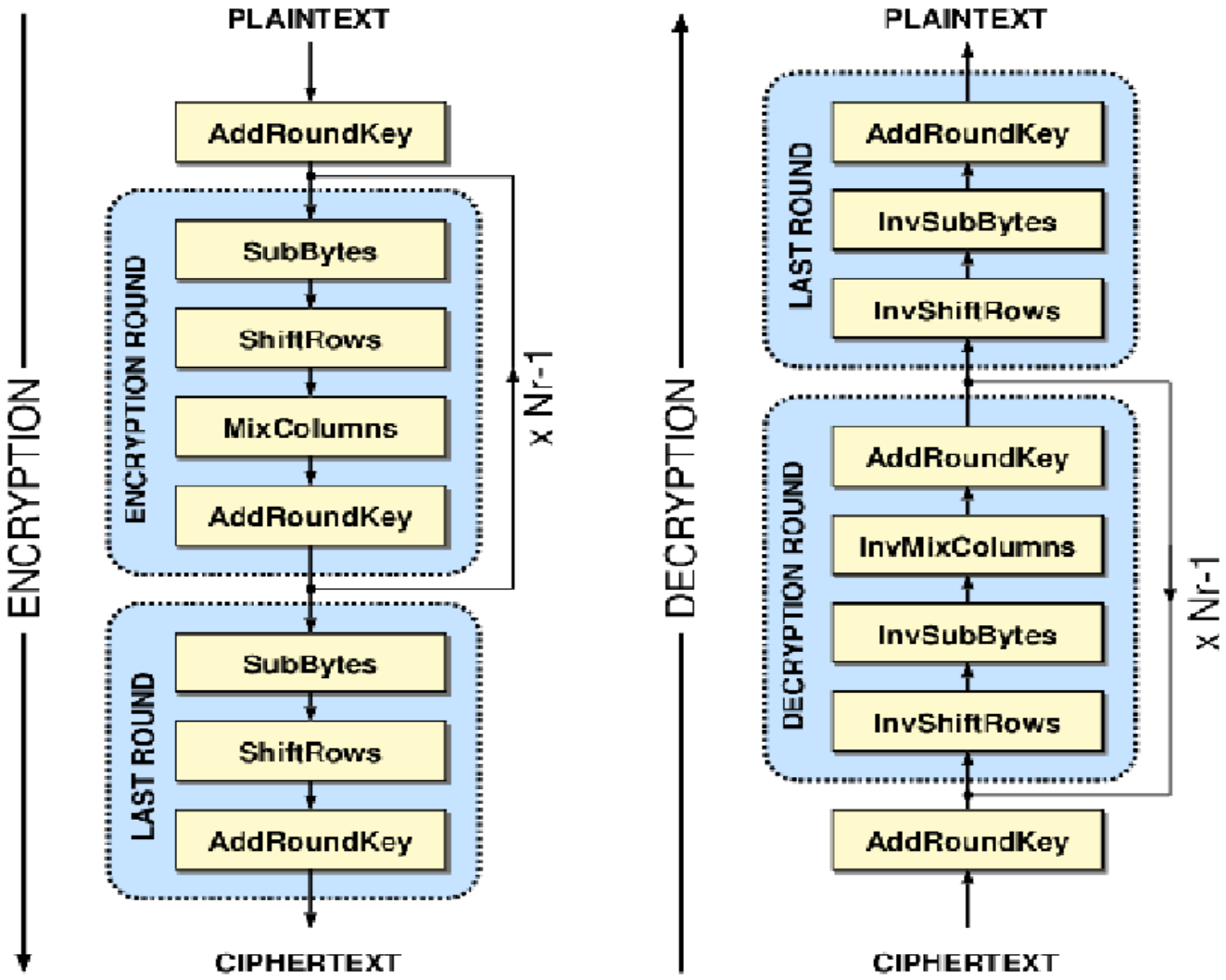


Figure 5.5.1 Working of AES

1. KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. InitialRound
    1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
    1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows

AddRoundKey.

Experimental SNAPSHOTS

New Group Creation:

 ISSN: 2321-8169
230- 236

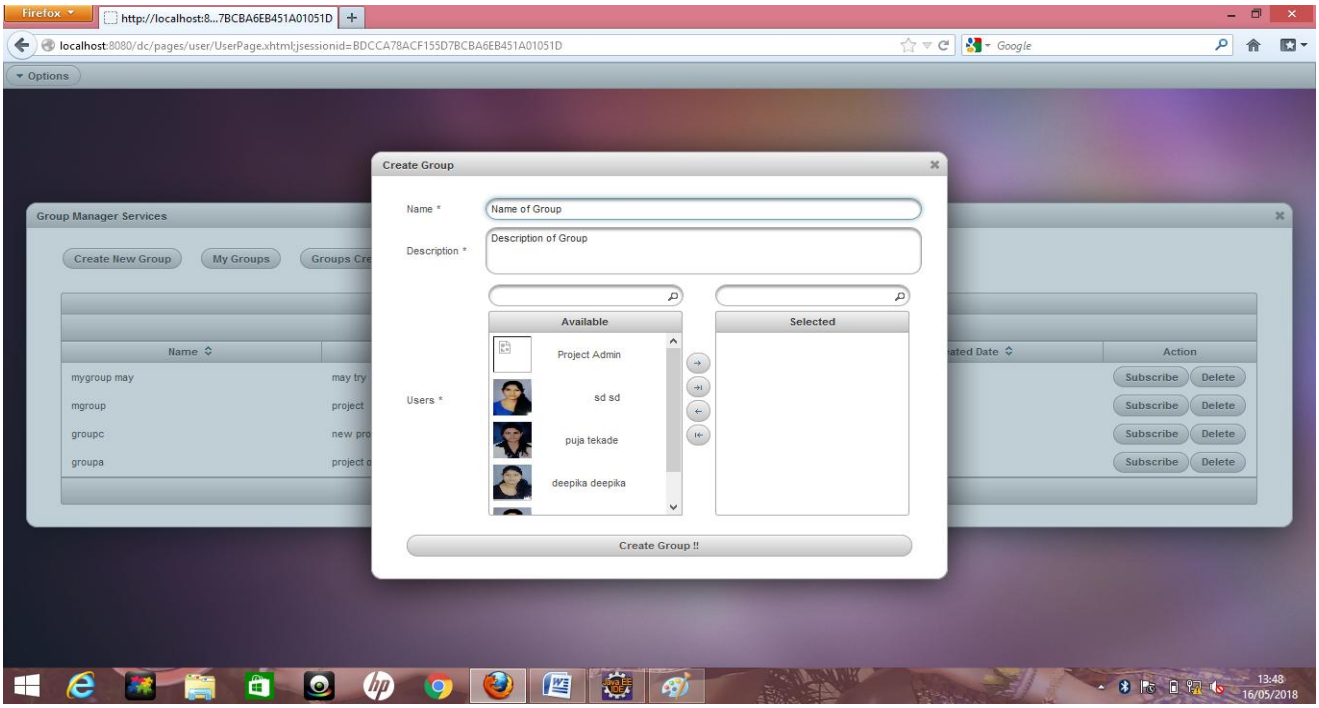


Fig:New Group Window

When user want to create a new group he click on group option then this window opened. There are four option Name, Description, Users, Create Group.

New Permission

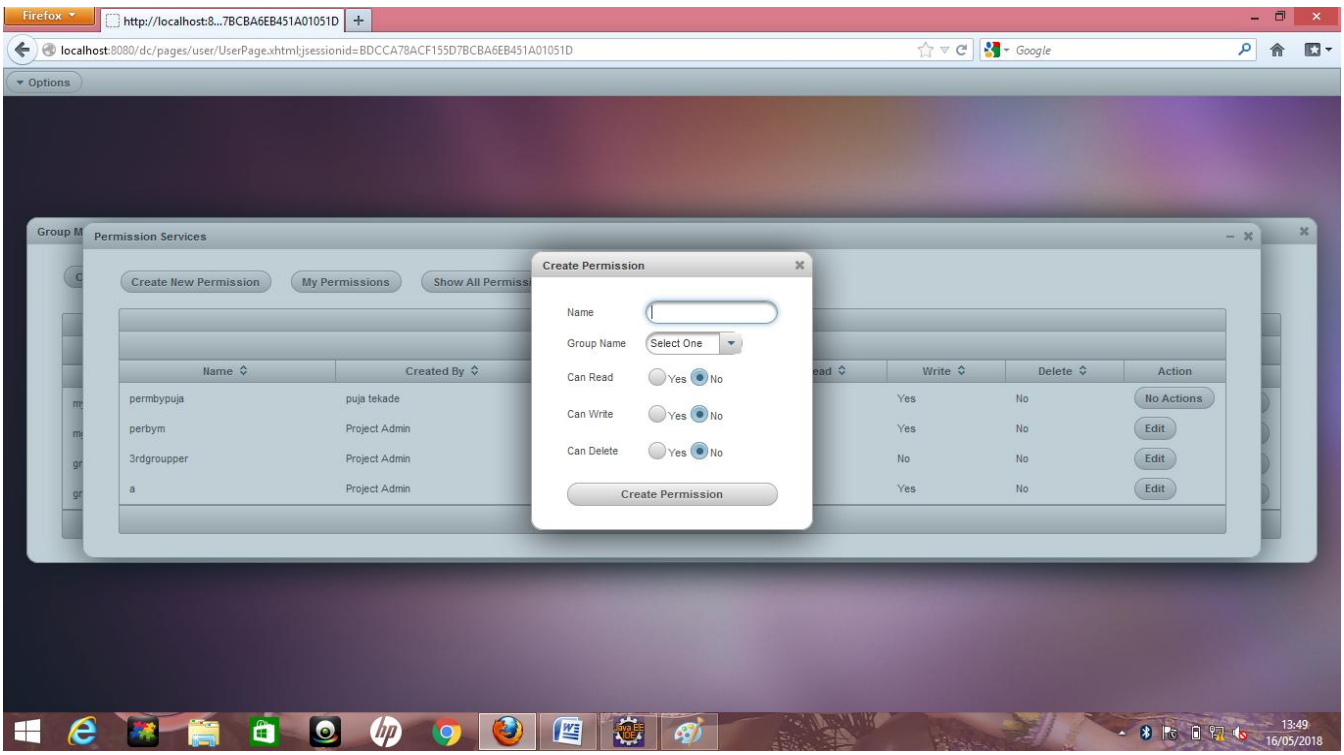


Figure New Permission Window

File Upload

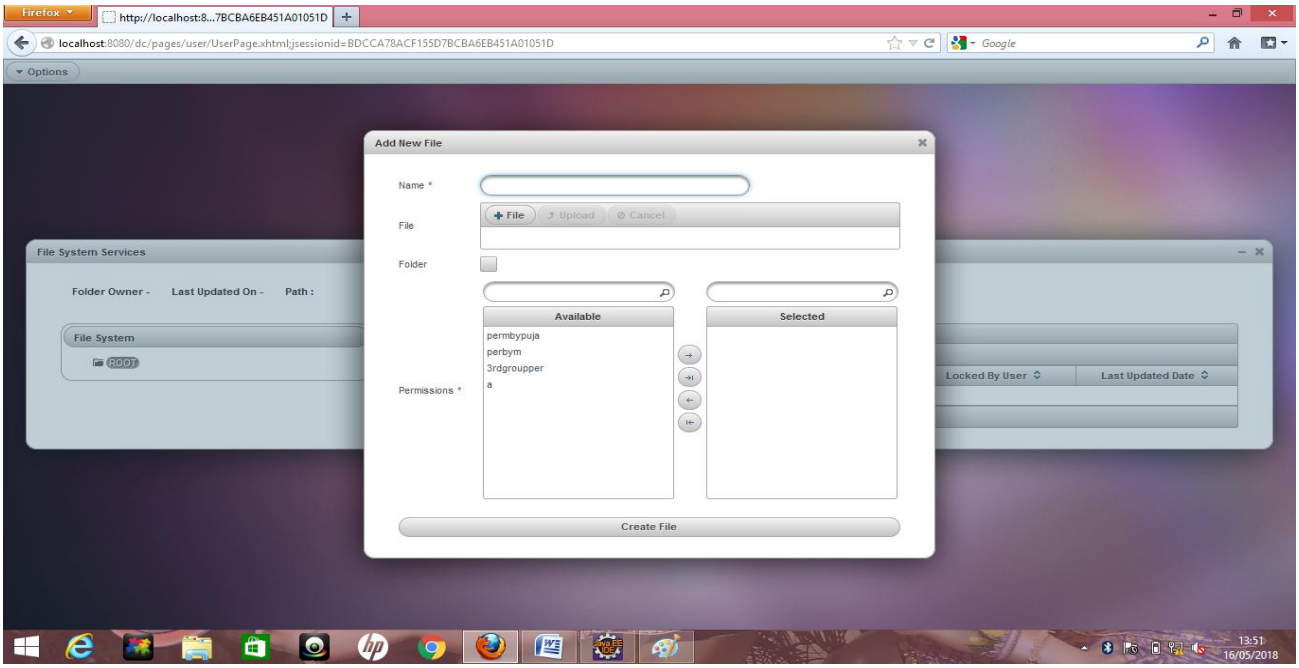
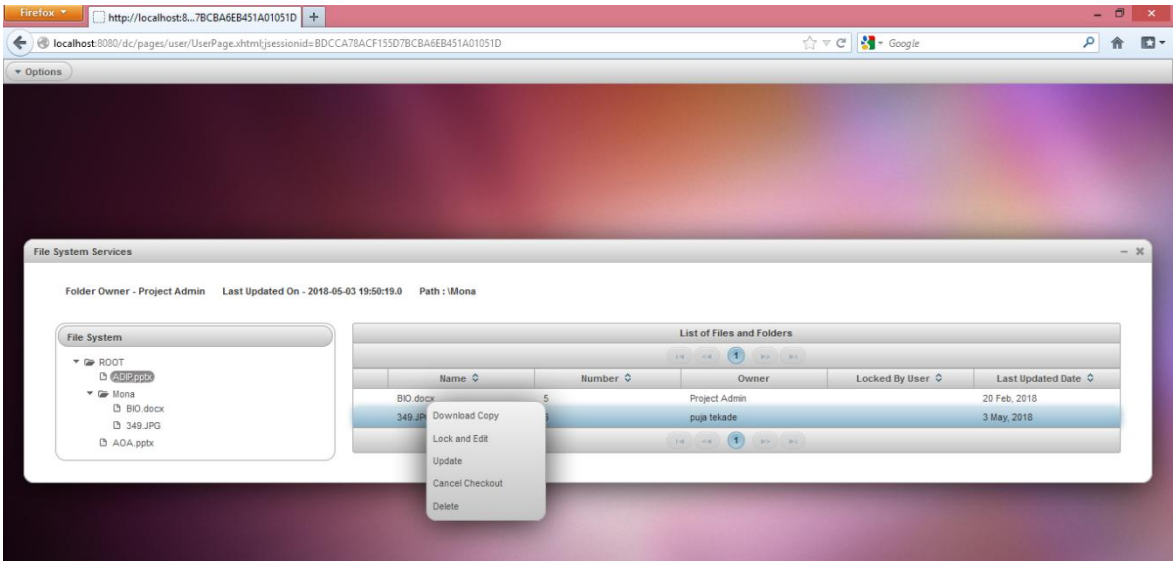


Figure: File Upload



File Operation

Figure: File Operation

CONCLUSION AND FUTURE SCOPE

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. In this paper we propose a system that improves the approach of CP-ABE from text based asymmetric to Image based symmetric approach for faster encryption as well as access to data. We also propose a multiple access policy generation for single user where we will be able to implement one to many and many to many methodology.

Future Enhancements

- Higher Security enhancement using dual encryption mechanisms.
- Data Uploading Limit Restriction Policy.
- Compression policy for cloud for better storage efficiency.
- Integrating CP-ABE within proposed approach to improve flexibility.

- Implementing Key Aggregate mechanism for higher key security.
- Evolving from single cloud to multi cloud.
- Strengthening policy for differential roles.

REFERENCES

[1] KaipingXue, YingjieXue, Jianan Hong," RAAC: Robust and Auditable Access Control with MultipleAttribute Authorities for Public Cloud Storage" IEEE ACCESS 2017

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[5] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[6] J. Hur, "Improving security and efficiency in attributebased data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282, 2013.

[7] J. Hur and 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.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on timesensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[9] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011, pp. 568–588

[11] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proceedings of 2013 IEEE Conference on Computer Communications (INFOCOM 2013). IEEE, 2013, pp. 2895–2903.

[12] J. Chen and H. Ma, "Efficient decentralized attribute based access control for cloud storage with user revocation," in Proceedings of 2014 IEEE International Conference on Communications (ICC 2014). IEEE, 2014, pp. 3782–3787.

[13] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and Communications Security (CCS 2009). ACM, 2009, pp. 121–130.

[14] M. Lippert, E. G. Karatsiolis, A. Wiesmaier, and J. A. Buchmann, "Directory based registration in public key infrastructures." in Proceedings of the 4th International Workshop for Applied PKI (IWAP 2005), 2005, pp. 17– 32.

[15] W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484– 1496, 2016.

[16] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet x.509 public key infrastructure certificate policy and certification practices framework," IETF RFC, RFC3647, 2003.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributebased encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006). ACM, 2006, pp. 89–98.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy (S&P 2007). IEEE, 2007, pp. 321–334.

[19] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Automata, languages and programming. Springer, 2008, pp. 579–591.

[20] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007). ACM, 2007, pp. 456–465