Implementation of Robust Multiple Authority and Attribute Based Encryption for Access Control in Cloud Computing

Ms. Mona Padole, Prof. NutanDhande
Department of Computer Science and Engineering
ACE NagthanaWardha MH India

Abstract- Data access control is a challenging issue in public cloud storage systems. Cipher text-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 Computing, Access Control

I. 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.

II. LITERATURE SURVEY

A. Auditable ∂-time Outsourced Attribute-based Encryption for Access Control in Cloud Computing [1]

Author: JiantingNing, Zhenfucao, Xiaolei Dong, Hui Ma, Lifei Wei.

IEEE transaction on information forensics and security, 2017, Volume: 13, Issue: 1

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has so far been regarded as one of the most promising techniques for data access control in cloud storage systems. This technology offers users flexible, fine-grained and secures access control of outsourced data. There exist two main long lasting open problem of CP-ABE that may limit it's widely development in commercial application. 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.

B. Cloud Computing Security: From Single to Multi-Clouds [5]

Authors: Mohammed A. AlZain, Eric Pardede,BenSoh, James A. Thom
System Science (HICSS), 2012 45th Hawaii International Conference on, February 2012

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.

C. Reliable Re-Encryption in Unreliable Clouds [6]

Authors:Qin Liu, Chiu C. Tan, Jie Wu, Guojun Wang
Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, 19 January 2012

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.

D. Ensuring Data Integrity and Security in Cloud Storage [7]

Authors: WenjunLuo, GuojingBai
Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, 13 October 2011

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).

E. Key-Aggregate Cryptosystem for Scalable Data Sharing In Cloud Storage [8]

Authors:Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng
IEEE Transactions on Parallel and Distributed Systems, Feb 2014, Volume: 25, Issue: 2

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 keyholder can release a reliable size aggregate key for versatile choices of figure substance set in appropriated stockpiling.

III. PROPOSED SYSTEM

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

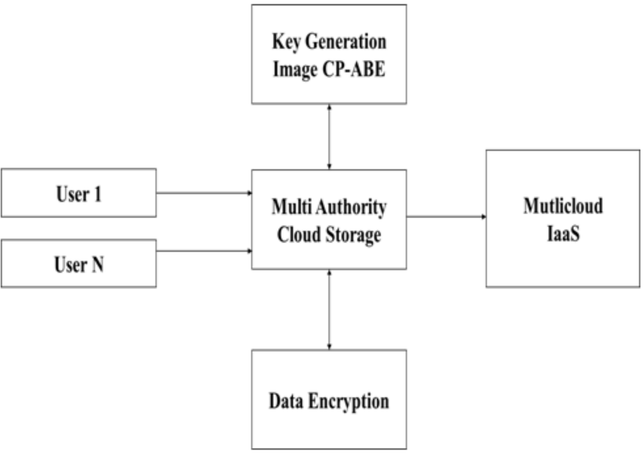


Fig.3:Proposed System Architecture

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.

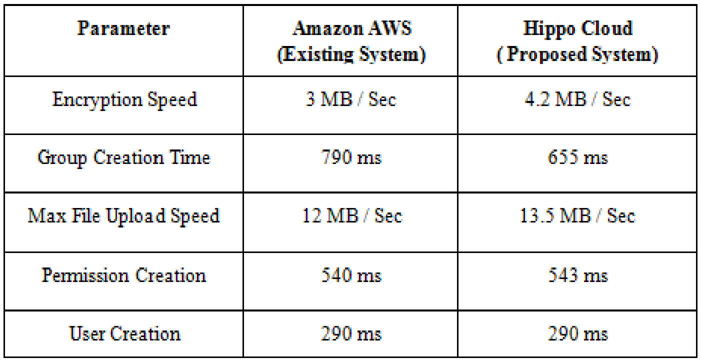
The cloud that will be used is Google Drive and multiple access will be provided to user based on permission i.e. Read / Write and Delete.

A. Algorithm/procedure used

```
GroupCreation(User users[])
Step 1: Fetch List of All Users into String array[]
Step 2: For Each User:users[] do
            Insertdata(user,groupname,owner)
            End For
Step 3: Return
Insertdata(User user,Stringgroupname, User owner)
Step 1: Generate Database Connection
Step 2: For Each user:users[] do
            Insert row as groupname,owner,user
            End For
Step 3: Return
PermissionCreation(User users[])
Step 1: Fetch List of All Permission into String array[]
Step 2: Fetch Group Details in User[] Array
            Insertpermission(User[],Permission)
            End For
Step 3: Return
Insertpermission(Userusers[], permission)
Step 1: Generate Database Connection
Step 2: For Each user:users[] do
            Insert row as groupname,permission,user
            End For
Step 3: Return
FileUpload(User owner,File file)
Step 1: Fetch filepath into variable f
Step 2: Read file into byte[] buffer
Step 3: Insert file into cloud location
Step 4: Return
FileDownload(User owner,File file)
Step 1: Fetch filepath into variable f
Step 2: Read permission into object p
Step 3: if(p.value equals requested permission)
            Fetch file path and download
            Else
            Show Error ”You are not allowed to perform
operation”
Step 4: Return
```

IV. RESULT AND DISCUSSION

Table of comparison on AWS and Hippo Cloud



Parameter	Amazon AWS (Existing System)	Hippo Cloud (Proposed System)
Encryption Speed	3 MB / Sec	4.2 MB / Sec
Group Creation Time	790 ms	655 ms
Max File Upload Speed	12 MB / Sec	13.5 MB / Sec
Permission Creation	540 ms	543 ms
User Creation	290 ms	290 ms

A. Results on AWS(Existing System) and Hippo Cloud(Proposed System)

4.2.1 Group Search Timing in Second

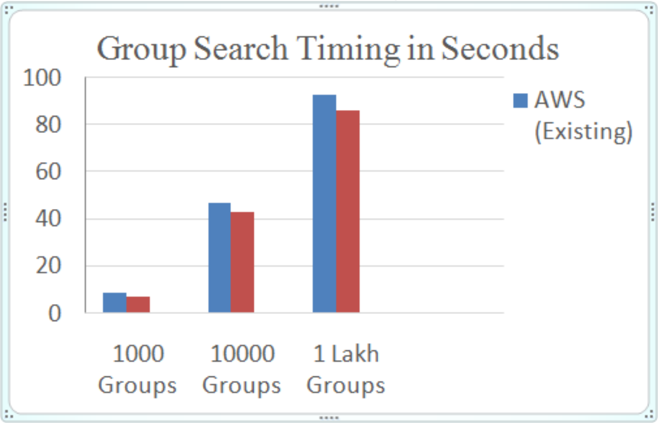


Fig:Comparisons on Group Search Time on AWS and Hippo Cloud

Above graph shows the implementation results of proposed system deployed on AWS and Hippo Cloud systems. Parameters are calculated based on number of groups that were generated randomly on cloud. The time provided is in seconds.

4.2.2 File Search Timing in Seconds

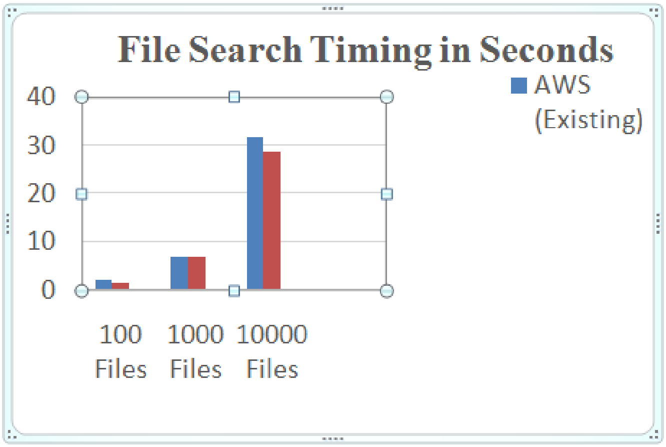


Fig: File Search Time in Seconds

Above graph shows the implementation results of proposed system deployed on AWS and Hippo Cloud systems. Parameters are calculated based on number of files uploaded randomly on cloud. The time provided is in seconds.

4.2.3 File Encryption timing in Seconds

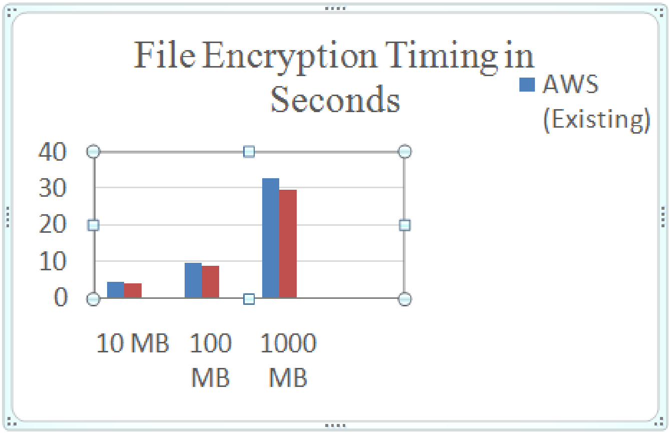


Fig: File Encryption timing in AWS and Hippo Cloud Systems

Above graph shows the implementation results of proposed system deployed on AWS and Hippo Cloud systems. Parameters are calculated based on file encryption time taken by system on different clouds. The time provided is in seconds. We have limited the max file size upload to 1GB based on time requirement in simulation.

V. 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 I 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. I also propose a multiple access policy generation for single user where I will be able to implement one to many and many toomany methodology.

VI. 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.

VII. REFERENCES

[1]. JiantingNing, Zhenfucao, Xiaolei Dong, Hui Ma, Lifei Wei, "Auditable ∂-time outsourced attribute-based encryption for access control in cloud computing"IEEE transaction on information forensics and security, volume PP, issue: 99, 2017

[2]. Mona S. Padole, Prof. N.M. Dhande, "Data Security and Access Control Mechanisms in Cloud: A Review" International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 3 Issue: 12, December 2017

[3]. Mona S. Padole, Prof. N.M. Dhande, "Designing Robust Multiple Authority Control Access for Cloud Storage" International Journal of Research, Volume 05 Issue: 12, April 2018

[4]. Mona S. Padole, Prof. N.M. Dhande, "Robust Multiple Authority and ABE for Access Control in Cloud Computing" International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 6 Issue: 3, March 2018

[5]. Mohammed A. AlZain, Eric Pardede,BenSoh, James A. Thom, **"**Cloud Computing Security: From Single to Multi-Clouds" System Science (HICSS), 2012 45th Hawaii International Conference on, February 2012

[6]. Qin Liu, Chiu C. Tan, Jie Wu, Guojun Wang, **"**Reliable Re-Encryption in Unreliable Clouds" Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, 19 January 2012

[7]. WenjunLuo, GuojingBai, "Ensuring Data Integrity and Security in Cloud Storage" Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on, 13 October 2011

[8]. Cheng-Kang Chu, Sherman S. M. Chow, Wen- GueyTzeng, Jianying Zhou, and Robert H. Deng**, "**Key-Aggregate Cryptosystem for Scalable Data Sharing In Cloud Storage" IEEE Transactions on Parallel and Distributed Systems, Feb 2014

[9]. Anil Somayaji, "Trusting the Cloud & Security in the Cloud"Cloud Technologies and Applications (CloudTech), 2015 International Conference

[10]. Mei Hui, Dawei Jiang, Guoliang Li, Yuan Zhou, **"**Supporting Database Applications as a Service" Data Engineering, 2009 ICDE 09. IEEE 25th International Conference on, 10 April 2009

[11]. Gehana Booth, Andrew Soknacki, and Anil Somayaji, **"**Cloud Security: Attacks and Current Defenses" 8 th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (asia'13), june 4-5, 2013

[12]. Cong Wang, Qian Wang, KuiRen, Wenjing Lou,"Ensuring Data Storage Security in Cloud Computing" Quality of Service, 2009 IWQoS 17th International Workshop on, 18 August 2009

[13]. jaydipsen,"Security and Privacy Issues in Cloud Computing Proceedings"IEEE Conference on Cloud Computing 2013

[14]. 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.

[15]. 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.

[16]. 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.

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

[18]. 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.

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

[20]. 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.

[21]. 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.

[22]. 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.