Dynamic Policy Update on Cloud for File Access

Shrikant Malge[1]
[1] M.Tech. Student, Department
of Information Technology, Bharati Vidyapeeth Deemed
University College of Engineering BVUCOEP, Pune, India
[1]spmalge@gmail.com

Prof. Snehal D. Chaudhary[2], Priyanka Paygude[3],
Shrikala Deshmukh[4]
[2,3,4]Assistant Professor, Department of Information
Technology, Bharati Vidyapeeth Deemed University
College of Engineering, Pune, India
[2]sdchaudhary@bvucoep.edu.in, [3]pspaygude@bvucoep.edu.in

***Abstract**:* In today's era of digitalization everyone stores and access data online. Cloud computing has become prominent in data storage and access any where globally, but there is concern by data owners regarding data ownership. It is monotonous to assign access rights and simultaneously provide security in real time is a concern. To resolve this issue of access control in recent times Attribute based encryption method is widely preferred. One of the most popular method to handle access rights is by used is Attribute-based Encryption (ABE) method, the two ways for performing the implementation of ABE are ciphertext-policy and key-policy ABE. One of the widely practiced methods of safe communication is through cryptography. In this work we are proposing a method to handle access rights dynamically on the outlines of Ciphertext-policy attribute-based encryption (CP-ABE) scheme along with this we are using two symmetric encryption algorithm namely AES and Serpent for providing better security to the system. This work implements a new policy update method which helps to manage data access control in the dynamic policy update for data in the cloud storage. In this, same input key is utilized for the both encryption and decryption operation. Here two types of files are handled as an input such as Text file and image file. In experimental result, comparison of both algorithms is shown with the help of graphs with different parameters such as Time, Number of files, file size. And we have also shown the comparison of system having dynamic update policy and system with out in tabular form. We have also shown the comparative analysis of both algorithms that shows SERPENT encryption algorithm gives superior performance in Encryption.

Key words: *Access control, AES, Serpent, cryptography, cloud storage, Attribute-based Encryption.*

*****

I. INTRODUCTION

In traditional communication physical medium was used for connecting distributed computer through networks such as LAN, MAN, WAN. This was sufficient until the need for communication with larger distributed computer network was arrived. At this point internet played a vital role in connecting physical distributed computers, this was widely accepted by business organizations, educational sector and government organizations for daily drudgery. As there is increase in network bandwidth and depletion of latency have achieved attainable remote access.

In the decade of 21st century availability of high- capacity network, high- computational power machine at low cost and large storage devices led to wide spread in growth of cloud computing. Many organizations and for personal use cloud was preferred and adopted as cloud has both computational power and storage [1].

However cloud has failed in privacy concern in public cloud. People dithered placing private and sensitive data in public domain as the assumption of data servers keep data secure and enforce access control policy is no longer true today. People have concern regarding placing their data on cloud as cloud server can't be trusted completely. Since this has become the obstacle in future growth of cloud computing. Attribute based encryption (ABE) technology is a promising scheme to solve this end-to- end communication. ABE allows the date owner to assign attribute and encrypt the data along with attribute so that the user who satisfies the attribute can only access the file. As multiple organizations outsource the data on cloud and change their access control frequently so policy update become a significant issue. This issue is not taken in to consideration in the existing ABE system. As user don't have the copy of the file every time on local machine and only single copy is kept on cloud, so whenever data owner wants to change the access rights of a file then he has to again download the file then decrypt the file and then again upload the file in encrypted form with modified access rights. This increases the computational burden on system and decreases the system performance. So to solve this problem we have propose a method through which user can modify the access right dynamically on cloud without going through the previous monotonous method.

In cloud storage confidentiality and access control is one of the top security concerns. So the solution to this was cryptography. Cryptography is classified in to two major parts that is symmetric and asymmetric ciphers. In symmetric cipher single key is used for both encryption and decryption and in asymmetric cipher two pair of keys are used public and private key that should be with every user. When same data is shared by group of users, key management in symmetric cipher will become a sever issue and in asymmetric cipher multiple different encrypted versions of same document will be there on cloud. This results in inflated cloud storage with heavy redundancy and duplication of data. So there is a need for flexible solution.

Amit sahai et al. proposed a cipher-policy Attribute Based encryption (CP-ABE) [2] scheme. This solved the problem of cloud storage with CP-ABE, cloud storage only needs to keep a single copy of ciphered text for multiple users. A user can only decrypt a file his/her attributes satisfies the access control policy which is set at the time of file upload and encryption. Data owner has the private key which he/she shares with the user whose has access right. In cloud computing key will be generated separately for every file and only ciphered text will be stored on cloud. This resolves the issue of multiple duplicate copies of same data on cloud and complex key management issue is resolved. Without the private key data cannot be decrypted and accessed by cloud service provider [1].

Cipher text with attribute based encryption method has resolved the above mentioned problems with offering elegant retrieval method CP-ABE has turned in to a better cloud storage method, CP-ABE scheme is used to parallelize seaport in to multi processor construction equipment[3]. A limitation of real time deployed of attribute based encryption is that the definiteness of cloud server's alteration can't be confirmed by users. Also an end user might be swindled in accepting erroneous or defamatory transformed data. A protection to this is by providing a conformation key in the outcome of the decrypted file. This does not increase in computational power of cloud or client system the only additional computation is needed for hash computation [4]. To ensure data security in cloud access control is an effective method as it provides additional power in data retrieval. Due to dubious cloud servers data access control is an challenging issue CP-ABE is one of the most suitable technology in cloud computing as it gives data owner undeviating control of access policies [5].

In this paper we have used two symmetric encryption algorithms such as AES and Serpent to manage the data on the cloud storage with secure data access. Also we have proposed a new policy update method which helps to capable data access control in the dynamic policy update for big data in the cloud storage. In this, we have utilized same input key for the both data encryption and data decryption. Here we have handled two types of files as an input such as Text file and image file for encryption and decryption. At the end we have done experimental practice that shows the result of both algorithms with the help of graphs with two different parameters such as Time and Number of files. We have also shown the comparison of both algorithms that shows Serpent encryption algorithm gives enhanced performance than the AES encryption algorithm in encryption.

The special features of this paper are as follows:

- It designs competent data access control method for data on cloud with dynamic access modification.
- It completes dynamic access policies with future secure access and reducing computational cost.
- Implementation of symmetric encryption algorithm for encryption for better security.

II. RELATED WORK

Taeho Jung et.al. has exhibit a semi-anonymous benefit control plot Anony Control to address not just the information protection, additionally the client character security in existing access control plans. Anony Control decentralizes the focal specialist to confine the personality spillage and along these lines accomplishes semi-anonymity. In addition, it additionally sums up the record get to control to the benefit control, by which benefits of all operations on the cloud information can be overseen in a fine-grained way. Along these lines, he displays the Anony Control-F, which completely keeps the personality spillage and accomplishes the full secrecy [6]

Shucheng Yu et.al has addresses this testing open issue by, on one hand, defining and implementing access strategies based on information qualities, and then again permitting the data owner to assign the vast majority of the calculation undertakings required in fine-grained information get to control to un-trusted cloud servers without disclosing the hidden information substance. They accomplished this objective by exploiting and extraordinarily consolidating systems of ABE, intermediary re-encryption, and sluggish re-encryption. There proposed conspire additionally has remarkable properties of client access privilege confidentiality and client mystery key responsibility [7].

Kan Yang and Xiaohua Jia has introduced design of a recover oversee structure for various security plans and furthermore proposed a fit and in addition ensured different security recover oversee conspire for the cloud information storage. At first they have outlined a creative numerous security trademark stands encryption strategy which does not require an overall security likewise they have attempt to keep up any recover structure. They have additionally displayed a novel technique to determine the trademark re-exchange troubles in numerous security qualities stands encryption strategies [8].

Shulan Wang et.al. they have proposed an efficient file hierarchy ABE scheme. They have integrated a single access structure consisting of several layered access structure and the file is encrypted with integrated access structure. The cipher text is shared with similar attribute users. This reduces computational cost of system. There system is secure under standard condition.[9]

Vipul Goyal et.al. have offered a new cryptography algorithm for the elegant allocating of coded information which is known as a input key strategy distinctive that is based on the coded data algorithm [10]. In the data encryption algorithm, coded information are tagged along with the special group of distinctiveness as well as private input keys that are associated amid the access association which helps to manage coded information that which consumer is accomplished to translate the information in uncomplicated layout. They have uttered the suitableness of the offered system framework to giving out the evaluation information along with convey coded information. The offered system framework manages allotment of secret input keys that comprises Hierarchical distinctiveness that is based on the coded information.

Kan Yang, Xiaohua Jia and Kui Ren has proposed a design for access policies on cloud storage system based on CP-ABE. They have proposed a scheme to deal with the dynamic changes of user's access right in large- scale system. In their system data owner has the power of assigning access rights [11].

III. PROPOSED SYSTEM

In our system we have proposed a new method for access policy on the CP-ABE method which helps in accomplishing dynamic update of user's policies for accessing files on cloud. In our system data owner has full authority of assigning access rights to other users. We have also used two symmetric encryption algorithms such as AES and SERPENT for encryption of files and provide additional security. In our proposed system we are using same key for both encryption file and decryption of file. In our proposed system the users who don't have file access to a particular file can request to the data owner. Here we have handled two types of files as an input such as Text file and image file for encryption and decryption.

4.1 Advanced Encryption Standard Algorithm:

- AES is a symmetric encryption algorithm. Its block size is 128 bit and uses key length 128 bit it has 10 rounds of encryption of file as well as image.

4.2 Serpent Algorithm:

- Serpent is a symmetric encryption algorithm also known as symmetric key block cipher. Its block size is 128 bit and key size is 128 bit it has 32 rounds for encryption of file and image.

IV. SYSTEM ARCHITECTURE

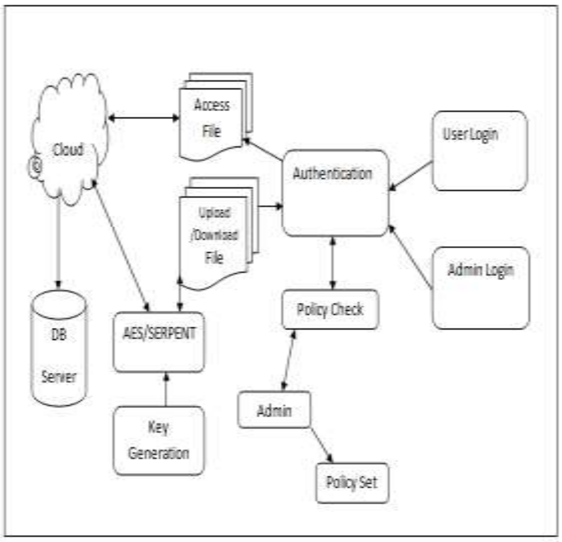

Fig 1: system architecture

The proposed system has following units to manage data storage on cloud as well as managing access policy.

4.1 Authentication:

In this unit every user's authentication is independent and it is responsible for managing the special characteristics and levels which are assigned to user at the time of registration on the outlines of CP-ABE. It generates a secret key which is shared with user via e-mail, user has to enter that secret key to enter the system. The access policy of the users is checked every time the user accesses the system.

4.2 Server:

The server unit function is of storing data from data owner, it also sets the access rights to the file according to data owner speciation. This unit is also responsible for modification in access policies and accordingly provides file access. This unit encrypts and decrypts a file and stores it with access rights for that file and provide access accordingly. For the file which user has access can download and while downloading decryption key will be sent via e-mail by this unit. This unit handles all the file access requests.

4.3 Admin

Admin unit manages all the new user registration in to the system and allocating them there level of access rights along with designation. It also sends request of access policy modification to server unit. This unit also deals with approval or denial of file access request and sending that request to server unit. This unit also deals with modification of user designation.

4.4 User

In user unit it manages the entire user located globally. Through this unit user upload a file and assign access right to the levels accordingly the file will be encrypted with access rights and uploaded on server unit. User which don't have file access cant view the file as it will be in encrypted format and decryption key will not be shared. User unit also handles the file request from same department. Through this unit user can access files and download through server unit depending upon their access rights.

V. EXPERIMENTAL RESULT

In this section we have compared two symmetric algorithms namely AES and Serpent. The parameters which are considered for comparison are time taken for file encryption and number of files as input. We have shown the comparative analysis of both algorithms through graph that shows that Serpent encryption algorithm gives better performance than AES encryption algorithm.

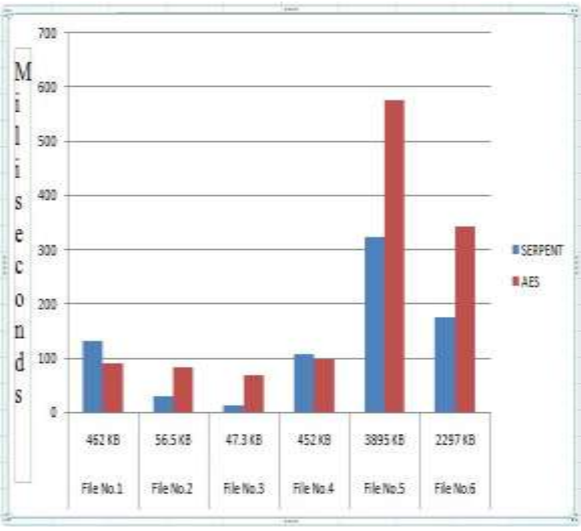

Fig 2: combined graph of AES and Serpent

COMPARISONS BETWEEN SYSTEM WITH DYNAMIC ACCESS POLICIES UPDATE AND SYSTEM WITHOUT DYNAMIC POLICY UPDATE

Sr. no.	Description	System without dynamic access policy	System with dynamic access policy
1.	Data owner has owner ship over data	No	Yes
2.	Control on who will access data	No	Yes
3.	Change in access right	No	Yes
4.	Access to files	Faster	Slower
5.	Sharing of data	Slower as have to share file individually	Faster as we can share data in bulk.
6.	Data management	Not so optimized	Optimized
7.	Change and modify access rights remotely	Not possible	Possible
8.	Data security and reliability	If the service provider's server is breached then our data will also be compromised.	Data is more secure as extra layer of security is provided above the service provider.
9.	Managing users	Less efficient	Efficient
10.	Internal data sharing between users	Not so securely and privately.	More securely and privately.
11.	Application	Used for personal purposes and where security is not a concern.	Used for organizational purposes. And used where security of data is of high concern

VI. CONCLUSION AND FUTURE WORK

In this paper we have developed an effective method of outsource the policy updating on cloud server, which can satisfy the entire requirement of user. New policies update method that assists to capable data access control in the active policy update of data in the cloud computing. In our system data owner has power of assigning file access rights. We have used two different algorithms namely AES and Serpent symmetric encryption algorithms to have secure encryption of file and file access. Same input key is used for both encryption and decryption of data. Here we have handled two types of files as an input such as Text file and image for encryption and decryption. In the Experimental result we have compared the result of both algorithms with the help of graphs with different parameters such as Time, number of files, file size and system with dynamic access policies and without access policies. We have also shown the comparative analysis of both algorithms that shows serpent algorithm provides speedy file encryption.

In future work we can ensure the fast processing by using parallel processing, and computational burden on one server is reduced by creating multiple replicas of server so that multiple request can be handed simultaneously, and for load balancing use multi threading.

References

[1] Lifeng Li, Xiaowan Chen, Hai Jiang, "*P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for Clouds*", 2016 IEEE SNPD 2016, May 30-June 1, 2016, Shanghai, China

[2] A. Sahai, J. Bettencourt and B.Waters, "*Ciphertext-policy attribute based encryption*", IEEE Symposium on Security and Privacy, page 321V334, 2007

[3] Lifeng Li, Xiaowan Chen, Hai Jiang, Zhongwen Li, Kuan-Ching Li, "*P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for Clouds*", 978-1-5090-2239-7/16/ copyright 2016 IEEE SNPD 2016, May 30-June 1, 2016, Shanghai, China

[4] Baodong Qin, Robert h. Deng, Shengli liu, and Siqi ma, "*Attribute-based encryption with efficient verifiable outsourced decryption*", ieee transactions on information forensics and security, 10.1109/tifs.2015.2410137

[5] kan yang, student member, ieee, and xiaohua jia, fellow, "*Expressive, efficient, and revocable data access control for multi-authority cloud storage* ", ieee transactions on parallel and distributed systems, vol. 25, no. 7, july 2014.

[6] Taeho jung, Xiang-yang li, senior member ieee, Zhiguo wan, and Meng wan, "*Control cloud data access privilege and Anonymity with fully anonymous Attribute-based encryption*", ieee transactions on information forensics and security, vol. 10, no. 1, january 2015.

[7] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, *"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing",* Technical Program at IEEE INFOCOM 2010. 978-1-4244-5837-0/10/ ©2010 IEEE

[8] Kan Yang, Xiaohua Jia, "*Attributed-based Access Control for Multi-Authority Systems in Cloud Storage*", 2012 32nd IEEE International Conference on Distributed Computing Systems, 1063-6927/12 © 2012 IEEE.

[9] Shulan Wang, Junwei Zhou, *Member, IEEE,* Joseph K. Liu, *Member, IEEE,* Jianping Yu, Jianyong Chen, Weixin Xie, "*An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing*", 10.1109/TIFS.2016.2523941, IEEE Transactions on Information Forensics and Security.

[10] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "*Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*", *CCS'06,* October 30–November 3, 2006, Alexandria, Virginia, USA. Copyright 2006 ACM 1-59593-518.

[11] Kan Yang, Xiaohua Jia, Kui Ren, "*Attribute-based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems*", ASIA CCS'13, May 8–10, 2013, Hangzhou, China.