International Journal of Distributed and Cloud Computing
6 (2) December 2018, 01-04
http://www.publishingindia.com/ijdcc

Storage of Data on Cloud with Double Check Admission Regulator

P. Shanthi Kumari
Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, Karnataka, India.
Email: shanthikumarip373@gmail.com

Abstract: An admission regulator scheme to cloud services that are based on web is explained here. The proposed method is an admission regulator technique. It is executed having two things such as key from user which is secret and a lightweight device which is secured. This technique will improve security of system. Users cannot have entry to system in the absence of both (secret key and device) things. This method provides security where many users share same access point to use service offered by cloud. This admission regulator technique allows server of cloud to confine the access to users who are having same components. This is to sustain safety. The service provider only recognizes whether user fulfils the ground as per requirement. But it does not have any clue on precise uniqueness of the consumer who uses data on cloud.

Keywords: Admission regulator, Cloud services, Light-weight device, Secret key.

I. Introduction

Cloud computing can be defined as an invisible atmosphere of computing resources. With the help of it organizations can use resources virtually. It provides services based on request. Uses of Cloud computing are plenty which includes sharing of data, storage of data, management of big data etc. Physical existence of resources is immaterial here. A cloud is an Information Technology setting that is designed for providing resources. A collection of nets provides isolated entry to distributed resources. It is a different Information Technology trade section. The representation of a cloud is used to describe the internet in a various description.

Ultimately the end users utilize cloud resources through a mobile application or any other way. The data are stored on servers at remote locations to be available to users.

II. Related Work

J. Lai, R. H. Deng, C. Guan, and J. Weng in their paper [1] give idea about Attribute-Based Encryption (ABE). It is a public-key-based one-to-many encryption system. It allows users to encrypt and decrypt data based on user attributes. One of the main drawback of ABE is decryption involves expensive pairing operations.

J. Hur [2] gives idea about recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks. One of the problems in data sharing systems is the inclusion of access policies and the support of policies updates.

M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou [3] gives idea about Personal Health Record (PHR). Emerging patient-centric model of health information exchange method is used. Privacy is main issue here.

Taeho Jung, Xiang-Yang Li [4] present that Cloud computing is an inventory computing idea. Importance is given to contents privacy and the access control, while less importance is given to the privilege control and the identity privacy. A semi anonymous privilege control scheme is proposed.

Fine-Grained Control of Security Capabilities [5] gives a new approach for fine-grained control over users security privileges. It provides many practical advantages over current revocation techniques. It provides details about both the architecture and implementation of our approach as well as its performance and compatibility with the current infrastructure.

III. Proposed Methodology

An efficient storage of data on cloud with security and double-checked admission regulator for resources of cloud which are based on web with the help of user secret key and a security device which is of light weight is proposed here. Fig. 1 shows the Architecture of the system.

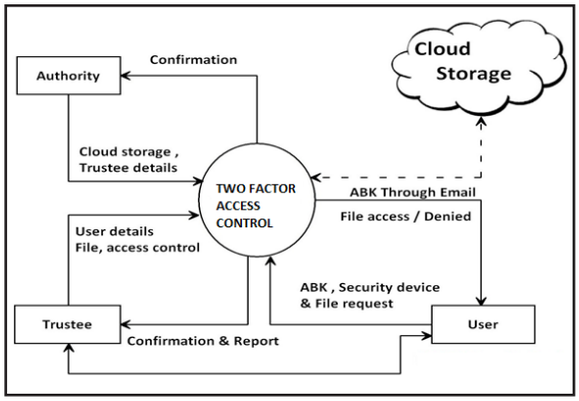

Fig. 1: Architecture of the System

IV. Modules

Modules are the elements in proposed method which include Authority, Trustee and User.

i. Authority is a prime user who is having ability to create the Trustee and User. He manages arrangements of cloud server. He has the ability to manipulate Trustee.

Capabilities of Authority:

- Updating storage details of cloud.
- Adding, editing and deleting the trustee.
- Viewing and updating key.
- Viewing department details.
- Viewing designation details.
- Changing password.

ii. Trustee is a person having permission to store data onto cloud. These files are used by authorized Users. Assume Trustee as a Liberian in a college. File to be stored will be encrypted by using key of Trustee. Trustee will highlight the Access scheme for all files. Trustee creates the Consumer or User. Trustee must give key to user. This key is Trustee's key and consumer attribution collection.

Functionalities of Trustee:

Creating users

- Filling details of users.
- Selecting key from database.
- Produce key from database and Dept. & Design of consumer.
- Encrypt the key with DNA procedure.
- Send key to the user through mail.
- Generate the Pseudonym Key from ABK using Hashing Technique (MD5).
- Copy Pseudonym Key to lightweight security device & send to respective consumer.

Viewing and deleting user information

Uploading data

- Folder Selection.
- Encrypt it using Private key.
- Fetch Storage Configuration Details.
- Send the Encrypted data to cloud Storage.

Viewing and deleting the data information

Access Control Set of folder

Viewing and deleting folder access control details

Operation Details

Changing Password

iii. Users are those who uses data on cloud. For example, If Trustee is a Liberian then users are like students. Users get key from trustee through email and device which is lightweight and secured. From this key, they can download data from cloud. Access is controlled by trustee or owner. Procedure for downloading uploaded data or file is:

- Selecting folder from collection of folders.
- System will demand access key (got via mail).
- System will demand for pseudonym key (got via device).
- These keys should be matched with keys stored in local database.
- On success, folders can be downloaded or else request will be denied.

Functionalities of User:

Viewing details of folder

Downloading data of folder

- Selecting folder from list.
- Select key folder from the local system and Pseudonym key from device which is secured.
- Decrypt the key using DNA algorithm.
- Generate the Pseudonym (1) Key from key.
- Get Pseudonym (2) from security device.
- Compare Pseudonym (1) & Pseudonym (2) if result is Fail deny the access.
- Get values from decrypted key.
- Check admission limit with Attribute.
- If result is Pass then folder will be download or else access is denied.
- Fill transaction details in the log.
- Decrypting folder
- Choose the folder to be downloaded.
- Retrieve the key from ABK.

- Decrypt the folder.
- Download the folder to user system.

Operation

- View the operations carried out by user.

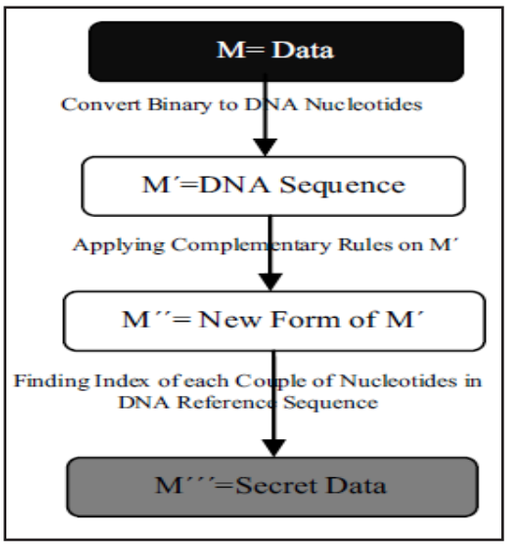

Fig. 2: Encryption Process

Fig. 2 shows the Encryption process of data. It includes two levels of encryption for providing more security for the data to be stored on cloud. Fig. 3 shows the Decryption process of data.

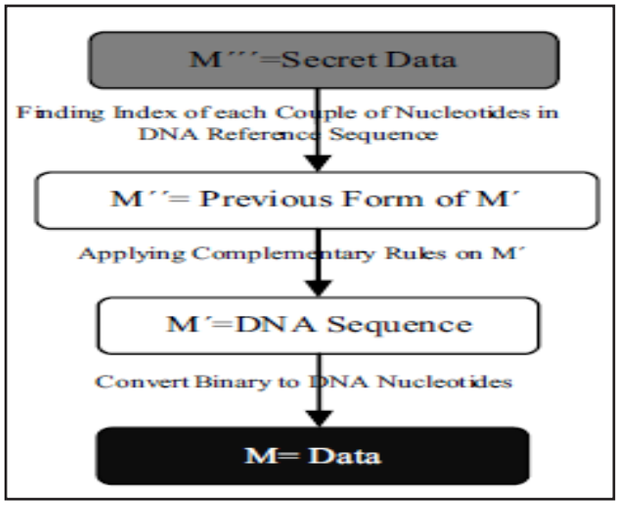

Fig. 3: Decryption Process

V. Result

These graphs show the performance of our system with various internet speed connections and the result shows it requires very nominal time to download the file.

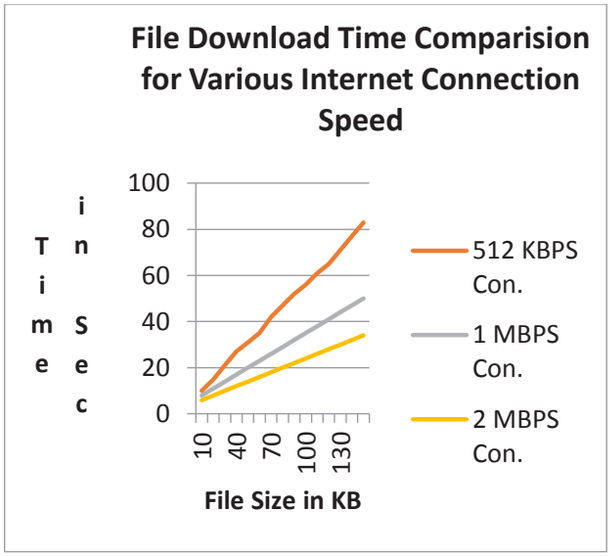

Fig. 4: Time Comparison for Various Internet Connection Speed

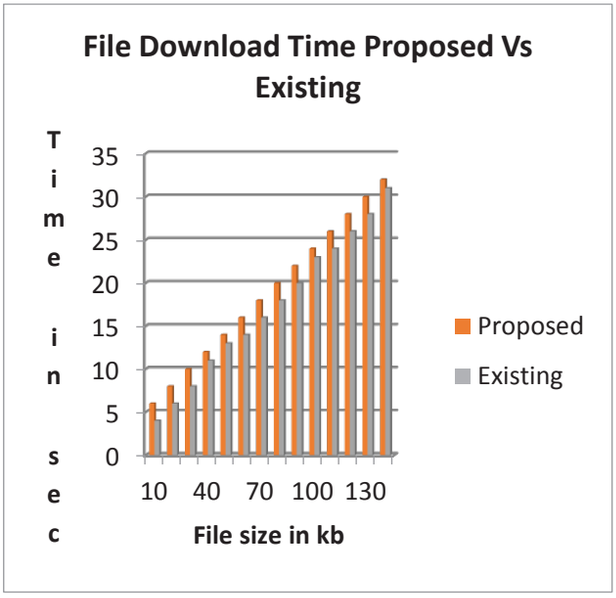

Fig. 5: Time Comparison with Existing System

VI. Conclusion

In this paper, an efficient cloud data storage with double checking admission regulator method is presented. The proposed system restricts unauthorized users. It will preserve users' confidentiality. Results section present that the proposed system can achieve the good result. Security is established in an enhanced manner. Encryption and decryption are carried out to provide more security to users' data to be stored on cloud. The

construction of the system is simple and easy to analyze. Future work can enhance the efficiency along with current properties of proposed system.

References

[1] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343-1354, August 2013.

[2] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271-2282, October 2013.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143, January 2013.

[4] T. Jung, X. Y. Li, Z. Wan, and M. Wen, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 190-199, January 2015.

[5] D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security capabilities," *ACM Trans. Internet Technol.*, vol. 4, no. 1, pp. 60-82, 2004.