Secure Data Autolysis of Data Scheme in Cloud Computing

P. Prema[1], R. Geetha[2], R. Padma[3], S. DivyaGanga[4]

[1]Assistant Professor, [2,3,4]UG Scholar
Department of CSE
Dhanalakshmi College of Engineering, Chennai.

***Abstract*— Cloud Storage is a model of data storage, where the logical pools of digital data are stored. Cloud Storage providers are responsible for keeping data available and accessible. If we share data in groups the insider threat would be encountered. Some methodology used to provide secure data sharing in clouds, that provides data confidentiality and integrity, access control, data sharing and insider threat security. In this paper, we propose: 1)One-Time download 2)Share Time Expire 3)Secret Key Management. The data will be shared through virtual cloud to provide more security. A key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a secure data Autolysis of Data scheme in cloud computing is used. In this scheme, The time interval is provided to cipher text while time limit is provided to private key. The cipher text can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the cipher text satisfy the key's access structure.**

***Index terms*--Autolysis, key-policy attribute-based encryption with time-specified attributes (KP-TSABE), virtual cloud, time limit.**

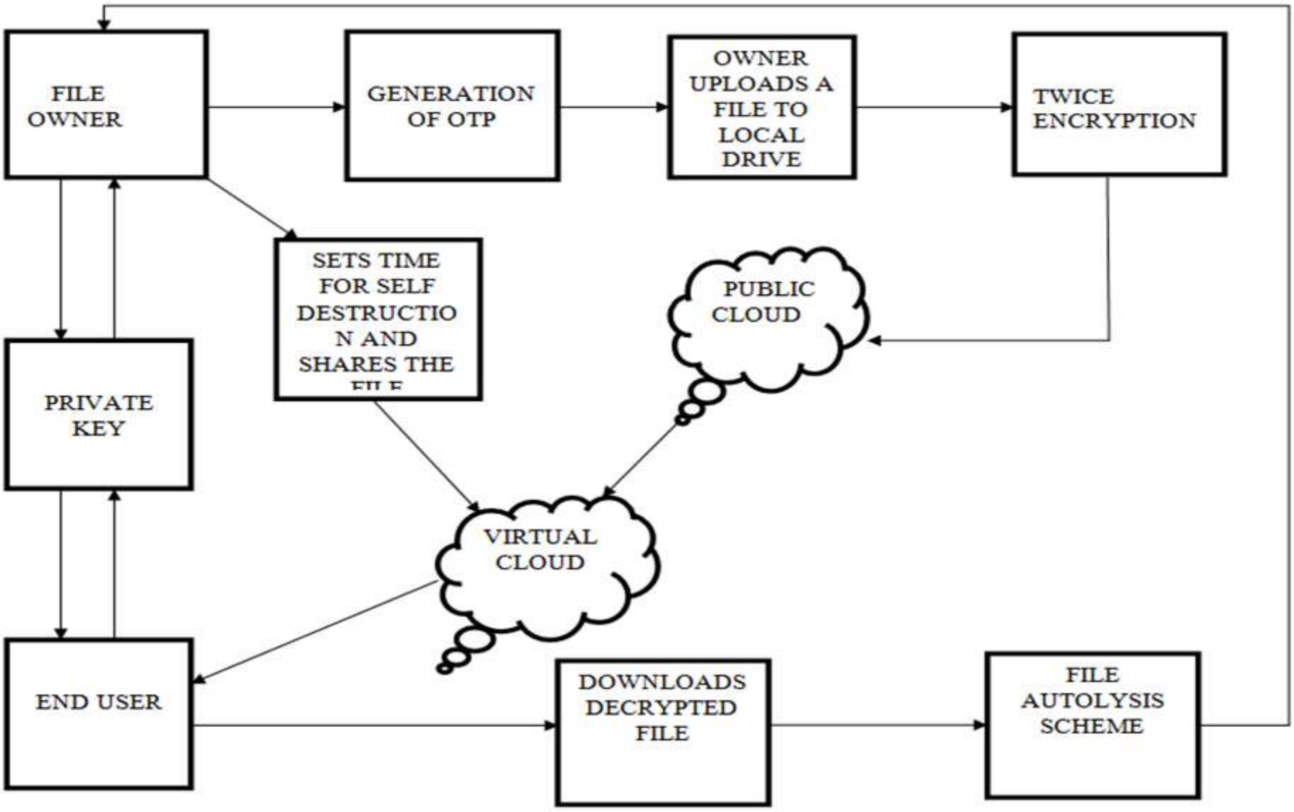
I. INTRODUCTION

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility [1]. High computation and storage services can now be utilized by organizations with low budget without investing heavily in infrastructure and maintenance [2]. The privacy and confidentiality services are provided to the data using cryptographic tools [3]. The files shared to another user may not be secure because the files are shared from the exact location so once the file gets corrupted it cannot be replaced with the same file. The shared file can be downloaded at any number of times using the link [4]. The files shared to another user is more secure because the files are encrypted twice before sharing by using symmetric encryption algorithm- Advanced Encryption Standard(AES). Here, the shared file will be sent to the another users virtual cloud so only the user to whom the file was shared can view the file [5]. Even if the shared file gets corrupted in the virtual cloud the original file will remain safe in the user cloud.

As the file is already encrypted twice, so it is not necessary for the user to re-encrypt file [6]. The function of the concept is to secure the user from downloading the file which was affected by threats. Returning back to the previous page is not allowed [7]. Once the user is forwarded to another page they cannot return back to the previous page which enhances security. User can download the shared file only once. They cannot access the same file more than once [9]. The shared file can be accessed only within the specific time limit which is set by the user. The file cannot be accessed beyond the time limit. The shared file can be downloaded by using the secret key which was sent to the user's registered mail id. The key is valid only for specified number of times. If we try to download the file by using wrong keys for more than a specified number of times, the file will be deleted automatically from the cloud using file autolysis scheme.

II. SYSTEM ARCHITECTURE

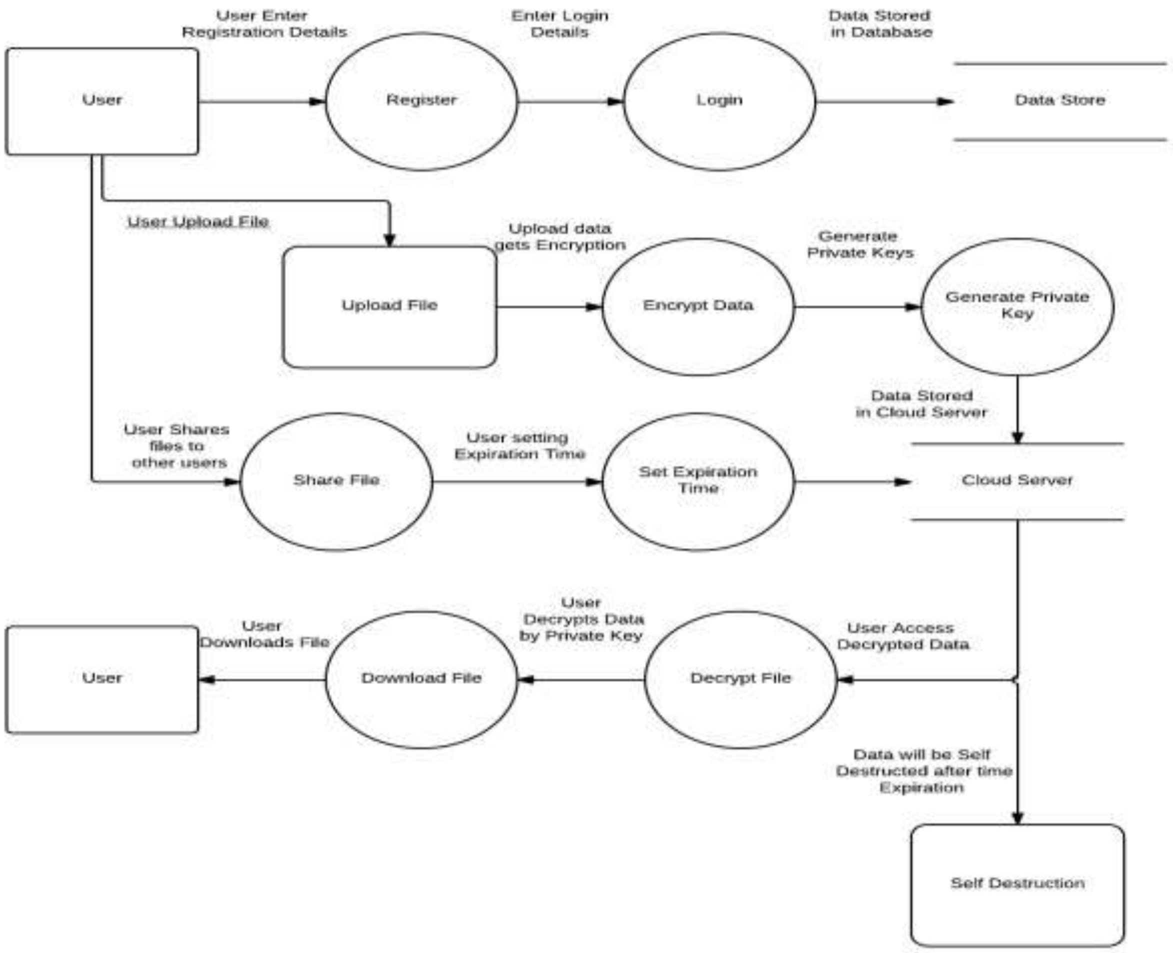
The user uploads the file to the cloud. Once uploaded, the data gets encrypted using the AES(Advanced Encryption Standard) which is converted into 256bits. The Encrypted file is stored in the form of binary data to which a key is attached, is stored in public cloud. At the same time user sets the time for self-destruction such that once the time limit is expired it gets automatically deleted even if the file is not accessed or downloaded. Also the motive of this setting of time is to provide the time limit to share the uploaded file by the user to the friends who needed it. Once when the shared file is accessed by the friend he will be provided with the private key to his mail. Once when the private key is entered the encrypted file gets automatically decrypted and it can be accessed and downloaded by the one who is going to access the file.



III. BLOCK DIAGRAM

The User have to register first to access the data base. Then, the user can login to the site. The authorization and authentication process facilitates the system to protect itself and besides it protects the whole mechanism from unauthorized usage. The Registration involves in getting the details of the users who wants to use this application. User Upload the files which he wants to share. Then the user upload the file to the real Cloud Storage. The file got encrypted by using AES (Advanced Encryption Standard) Algorithm and generates Private Key. The Encrypted Data is converted as Binary Data for Data security and Stored in Cloud. The uploaded files are shared to the users. The Data Owner set the time to expire the data in Cloud. The Private Key of the Shared Data will be send through Email.

The user should give corresponding Private Keys to decrypt the data. The data will be deleted if the user enter the Wrong Private Key for Three times. The Downloaded Data will be stored in Local drive. The Data will be automatically deleted if the User does not downloaded the file successfully with in the time. If the user download the data, then the File Autolysis will be disabled. If the File got deleted by File Autolysis scheme, the intimation Email will be sent to Data Owner. If data owner attach any malicious in our shared file then will intimate to shared user.


User Enter Registration Details
Enter Login Details
Data Stored in Database
User
Register
Login
Data Store
User Upload File
Upload data gets Encryption
Generate Private Keys
Upload File
Encrypt Data
Generate Private Key
Data Stored in Cloud Server
User Shares files to other users
Share File
User setting Expiration Time
Set Expiration Time
Cloud Server
User Decrypts Data by Private Key
User Downloads File
User Access Decrypted Data
User
Download File
Decrypt File
Data will be Self Destructed after time Expiration
Self Destruction

IV. CONCLUSION AND FUTURE SCOPE

Moreover, the Autolysis methodology provides assured deletion by deleting the parameters required to decrypt a file. To employ mobile cloud computing due to the fact that compute-intensive tasks are performed at the CS. This will further enhance the system to cope with insider threats. The response of the methodology with varying key sizes can be evaluated. In the future, the proposed methodology can be extended by limiting the trust level in the CS. In Future, the data can be shared by sending the different private keys to group members by restricting with user constraints.

V. REFERENCES

[1]A. Abbas and S. U. Khan, "A review on the State-of-the-art privacy pre-serving approaches in e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 1431–1441, Jul. 2014
.

[2]K. Alhamazani *et al.*, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," *Computing*, DOI: 10.1007/s00607-014-0398-5, 2014, to be published.

[3]A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," *Future Gen. Comput. Syst.*, vol. 29, no. 5, pp. 1278–1299, Jul. 2013.

[4]Cloud security Alliance, “Security guidelines for critical areas of focus in cloud computing v3.0,” 2011.

[5]D. Chen *et al.*, “Fast and scalable multi-way analysis of massive neural data,” *IEEE Trans. Comput.*, DOI: 10.1109/TC.2013.2295806, 2014, to be published.