International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Secure Cloud Storage of Text and Image Files by Giving Access Control to Users

Madhura Mahajan, S C Dharmadhikari

Abstract: ***Cloud computing is extensively used but it's not completely trustworthy. It can be in terms of protecting or securing the confidential data from malicious attacks as well as from cloud providers. Also once the data is deployed on cloud, the user has no control over it. So rather than deploying the original text file the user encrypts the file and then uploads on the cloud. When this file needs to be shared with other it can be done using Cipher text Policy Attribute Based Encryption (CP-ABE). This gives the central access to the owner and secures the data from external attacks. Besides, the cloud provider serves both as the payee of resource consumption fee, lacking the transparency to data owners. So to reduce these factors a specific encryption strategy is been used and the time for encryption is also taken into account. The files are also encrypted by the priority that are given by the user during the file uploading section. A text file of size 1GB with the CP-ABE encryption strategy requires 174 seconds whereas encryption done using AES is 473 seconds and that of RSA is 330 seconds. Hence, this dissertation work proposes methodology to secure or protect encrypted cloud storage from Economic Denial of Sustainability attacks and give an efficient time constraint approach.***

Keywords: ***Cipher text Policy Attribute Based Encryption, Access control***

I. INTRODUCTION

Cloud computing has emerged exceedingly and wide spread all around the world over last 20 years. Cloud computing involves delivering the hosted services Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service over the globe and internet. A cloud can be firstly private (a data center which hosts services to a limited number of people) or cloud can be public.

Various examples of available cloud service providers are: AWS, Google Cloud, Microsoft Azure, IBM Cloud and many more. The most promising feature of cloud computing is that you pay as you go. We pay for only the services that we use and for the specific amount of time of use. The storage also is flexible and we can always rely on its infrastructure.

Manuscript published on November 30, 2019.
* Correspondence Author
Madhura Mahajan, PG Student, Dept IT, PICT, Pune, India
Dr. S C Dharmadhikari, Associate Professor, Dept IT, PICT, Pune, India

Also due to virtualization and distributed computing high speed internet has boosted. Along with all these AWS is the most favorable cloud provider for the work that we propose and hence it has been selected. It is mainly providing free service for one year after subscription and then the regular charges are been invoked.

The EC2 instance created in the first step of the implementation and Ubuntu 16.04 version of operating system is installed. Further the IP address is obtained and it is used for mapping it to our main website myownwork.info with the help of route 53 protocol.

II. LITERATURE SURVEY

1. Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage

There is an absence of user to cloud controllability and hence cloud providers cannot be totally trusted for host privacy. By the encryption techniques confidentiality of the sensitive data can be ensured. After encryption, in order to share the encrypted files with other users, cipher text policy based encryption (CP-ABE) can be used to give access control to the owners. This demands transparency to data owners with effect of consumption fee by the accountant. The encryption is also possible using Advanced Encryption Standard (AES) and RSA algorithms [1].

2. Cloud Trust - a Security Assessment Model for Infrastructure as a Service Clouds

The data storage at remote points but along with high quality applications and services is possible to achieve through pool of resources. It brings burden on the method of data storage and its maintenance. With this it's also important to maintain the integrity of the data. The man thing to be taken into account is that the users should be able to use cloud storage without thinking about its integrity and confidentiality. Infrastructure as a service is been used from Amazon web services which gives storage space as per requirement [4].

III. ARCHITECTURE

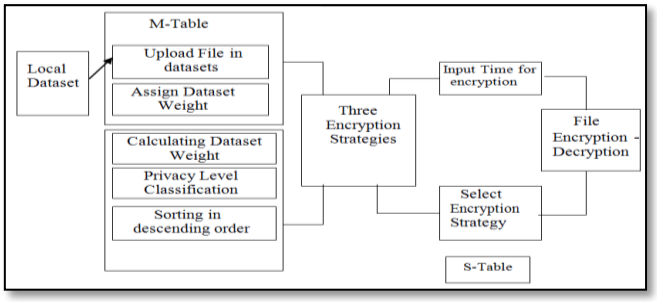


Figure 1 Architecture of the System

Figure 1 shows the detailed architecture of the proposed system and has two main algorithms: M Table and S Table. The local data is uploaded in the respective datasets where the encryption of those files is done accordingly. While uploading the files, also assign the priority number to the file so that it can follow the S Table algorithm where it is arranged and encrypted according to the priority assigned by the user. Also after one of the three encryption strategy is chosen, the time is to be set for encryption. The encryption depends upon the file type, the time given by user for encryption. Also the decryption of the file is done by the same method.

IV. ALGORITHMS

M-TABLE: The priority of each file is given in this table
S-TABLE: Size of the objects and their execution time is obtained here

Ts- Time required for execution overall
Tc- Time for input
Tm- Least time required for execution
P- Encryption Plan.
Di- Data Package type,
Nd- No. of objects like file images in Di,
Td- Execution time of processing file in Di.

4.1 M - TABLE GENERATION ALGORITHM:

INPUT : S-Table, M-Table, Tc, Tm.
OUTPUT : P (Encryption strategy plan)
PROCEDURE : Set P<=0;
Ts=[Tc-(Tm+Σ(Di) (N Di * TDi)];
While S≠0
do Get **Di** which has most priority in S-Table
for Di, **i=1** to NDi **do**
if Ts>TDi then
Add one data packet Di to **P** : **Ts= Ts- (TDi)**
else Break **end if end for end while End all**

4.2 S - TABLE GENERATION ALGORITHM(STG):

NEED : M table (Table describing each file size and its execution time.)
INPUT : S table,Tc,Tr.
OUTPUT : Sorted S table (in descending order).
PROCEDURE :
M table, Initialize S table=0,
Initialize **Tr**=0, Enter required time constraint.
for Di in M table
do If Wd = infinity **then Tr=Tr-(Ndi*Tdi) else**
if Wdi>0 **then**
Calculate **Sdi=Wdi/Tdi** Put **SDi** to S table
end if
end if end for
Sort S table by **Sdi** in descending order Return S Table ,**Tr**
End all.

V. EXPERIMENTAL STEPS AND RESULTS

AWS is the best platform available for cloud applications and hence is selected. Elastic Compute Cloud service is useful to install the ubuntu operating system as per our requirement.

After installation the code has been uploaded and the following results are obtained in the graphical manner. These results are showing the CPABE algorithm being used for encryption and decryption along with the M-Table Algorithm.

5.1 CPABE ALONG WITH M-TABLE ALGORITHM:

The CPABE scheme has been implemented practically and the following graph represents the encryption time required by the different files of same size in seconds. These files are nothing but images, text, pdfs, audio and video files. It is obtained that a file of size 10 MB requires 200 ms for encryption while that of size 50 MB requires 600ms.

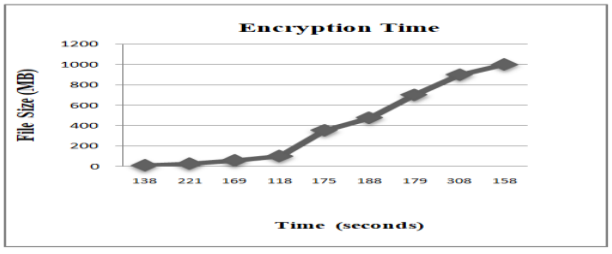


Figure 2 CPABE Encryption

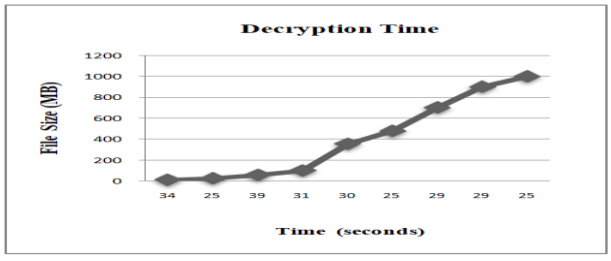


Figure 3 CPABE Decryption

5.2 COMPARISON OF ALL THE THREE ALGORITHMS:

Table 1 Encryption time of all three algorithms

ID	File size(MB)	AES (Secs)	RSA (Secs)	CPABE (Secs)
1	10	115	34	13
2	25	123	50	45
3	58	149	69	59
4	101	154	75	68
5	354	252	90	75
6	478	265	130	88
7	701	335	158	99
8	832	356	170	108
9	923	378	200	158
10	1008	437	330	174

The Figure 4 shows that the best suitable algorithm for all types of files for encryption and decryption is CPABE in comparison to RSA and AES. With the data in table 3, it encrypts and decrypts the larger files in less amount of time than the other two algorithms. It means that a text file of size 1 GB with the CPABE encryption strategy will require less amount of time than the same file encrypted using AES or RSA strategy. Here the experimental work has successfully achieved the encryption of text, images, audio and video files in all three encryption strategies.

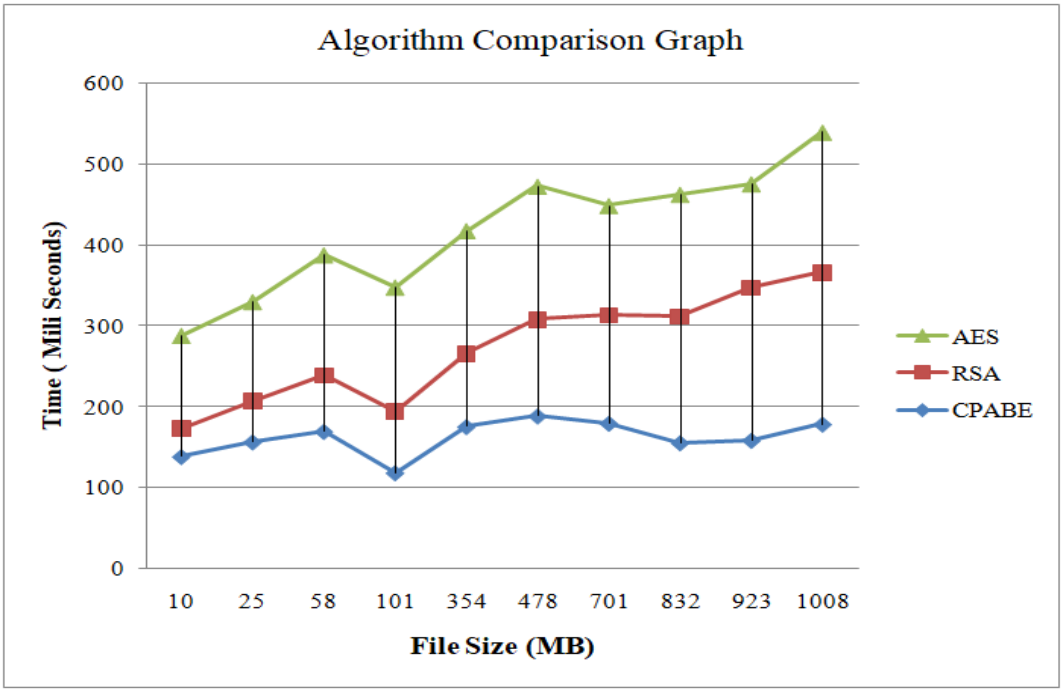


Figure 4 Comparison of AES, RSA, CPABE

It can be summarized that the file of size 100 MB needs 350 seconds for AES encryption while it needs 201 seconds for RSA encryption and only 110 seconds for CPABE encryption. If the file size increases to 1000 MB it is seen that AES strategy need huge amount of time up to 800 seconds for encryption RSA encryption needs 350 seconds while CPABE needs on 170 seconds.

Creating AWS EC2 instance by following steps below:

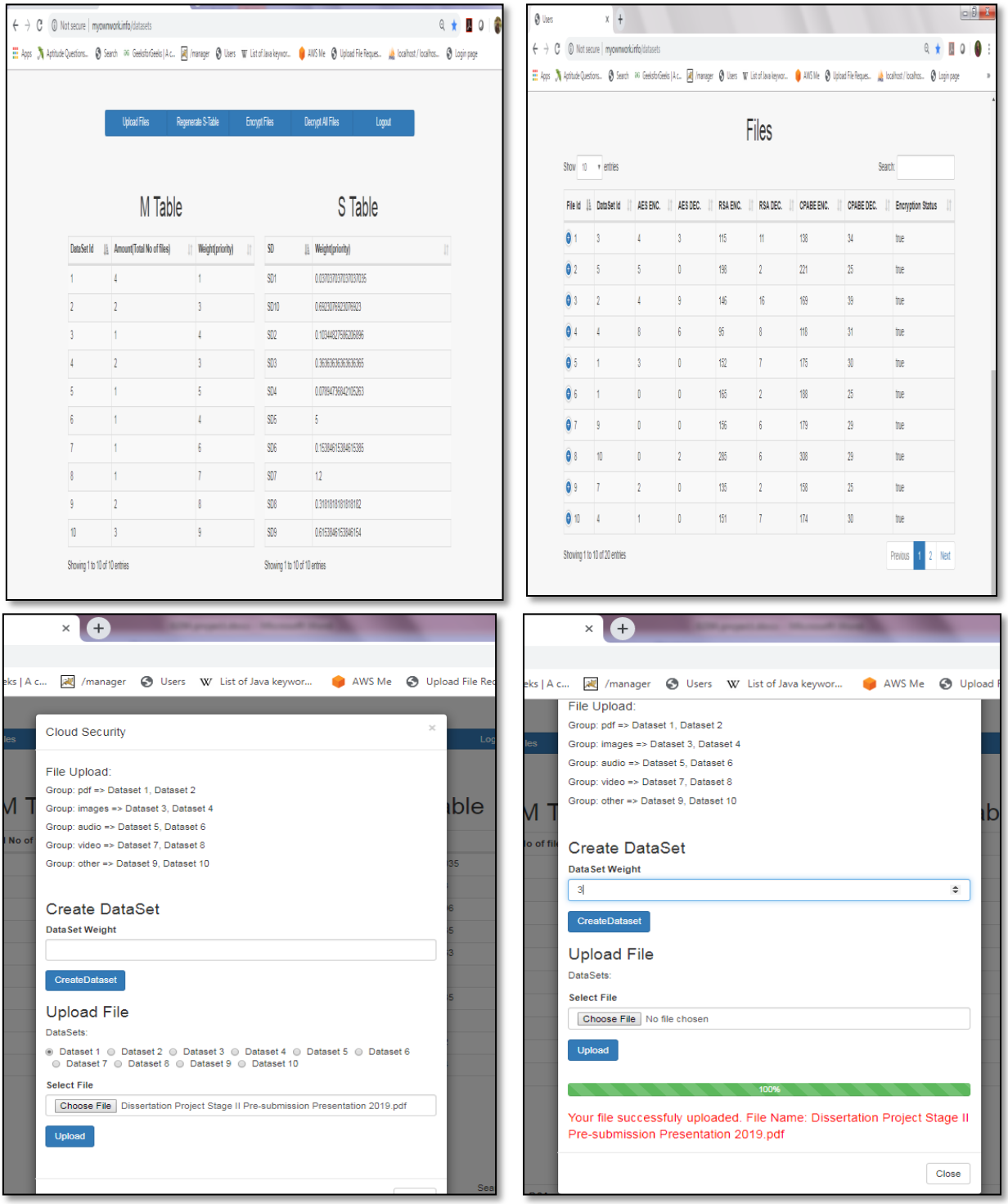
After creating EC2 ubuntu instance,
Login to our domain:

http://myownwork.info/login
http://myownwork.info/datasets

Now after login: go to next page where dataset file specifications are present
http://myownwork.info/datasets

Follow the steps:

1. Upload a file with its respective type in the correct dataset from 1 to 10.
2. Select the time for any of the three and Encrypt the file.
3. The files encrypted will appear at the below section and the user will be able to download the files.



Then click on Encrypt files select one of the encryption strategies and insert the sample time and click on Encrypt all dialog box.

VI. CONCLUSION

In this dissertation work, cloud provider side and data owner side access control in an environment with encrypted cloud storage is implemented, and the architecture follows CP-ABE scheme. The construction is secure against malicious data users and a covert cloud provider.

A user will perform decryption of the encoded text if that user's credentials pass through Encryption algorithm. AES was intended to augment the proficiency of security assurances. AES and RSA algorithms provide fast encryption when the file size is less than 100 MB. Whereas CPABE gives fast encryption of larger file size.

REFERENCES:

1. Kaiping Xue, Senior Member, IEEE, Wei Li, J. Hong, and P. Hong, "Combining Data Owner Side and Cloud Side Access Control for Encrypted cloud Storage", IEEE Transactions On Information Forensics And Security, Vol. 13, No. 8, August 2018.
2. G Zhuo, Qi Jia, L. Guo, Ming Li , and Pan Li, "Privacy-preserving Verifiable Set Operation in Big Data for Cloud assisted Mobile Crowd sourcing", IEEE IOT Journal

3. Zeidler Depa, M. Rizwan Asghar, "Cloud EFS- Efficient and Secure File System for cloud Storage Clemens", 10.1109/PST.2016.7906969, IEEE 2016.
4. D. Gonzales, IEEE, J. Kaplan, E. Saltzman, Z. Winkelman, D. Woods, "Cloud Trust: a Security Assessment Model for IaaS Clouds", IEEE Transactions on Cloud Computing.
5. Charan, K D Kumar, D Arun Kumar Reddy, "Concrete Attribute Based Encryption Scheme with Verifiable Outsourced Decryption", (IJETT) – Volume 12 Number 9.
6. J. H. Mun, J. Lee, and Hyesook Lim, "A New Bloom Filter Structure for Identifying True Positiveness of a Bloom Filter", DOI: 978-1-5090-6008-5/17/$31.00 2017 IEEE
7. Dr. (Mrs.) Ananthi Sheshasaayee, Mrs. B.Anandapriya, " Digital Signature Security Using Cryptography for Industrial Applications", International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017)
8. Roshni Singh, Ataussamad,Dr. Shiva Prakash, " Privacy Preserving in TPA for Secure Cloud by using Encryption Technique", ICIIECS 2017
9. Yong Yu, Giuseppe Ateniese, Xinyi Huang, Y. Dai, and G. Min, "Identity Remote Data Integrity Checking with perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on IFS, Vol. 12, No. 4, April 2017.
10. Y. Li, W. Dai, Z. Ming, and M. Qiu., "Privacy protection for preventing data over collection in smart city," IEEE Transactions on Computers

AUTHORS

Dr. S. C. Dharmadhikari, PhD in Computer Engineering, Associate Professor, PICT, Pune. Contact: scdharmadhikari@pict.edu

Madhura Mahajan, ME in Information Technology, PICT, Pune. Contact: madhurarmahajan@gmail.com