Storage Space Management and Security by using DCACrypt

Mr.Amit R.Gadekar
Ph.D Scholar ,Dept. Computer Engg
SITRC, Pune, India

Dr. M V.Sarode
Department of Computer Engineering
Government Poly., Yavatmal India

Dr.V M.Thakare
Department of Computer Engineering
SGBAU,Amravati

Abstract — Cloud Computing is a new computing model that distributes the computing missions on a resource pool that includes a large amount of computing resources. More and more companies begin to provide different kinds of cloud computing services for Internet users at the same time these services also bring some security problems. Internet users are able to acquire computing resource, storage space and other kinds of software services according to their needs. In cloud computing, with a large amount of various computing resources, users can easily solve their problems with the resources provided by a cloud. Today most cloud computing system use asymmetric and traditional public key cryptography to provide data security and mutual authentication. This research helps in securing the data without affecting the original data and protecting the data. In this technique the data are segmented into three different levels according to their data importance ranking, set by data owner. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is to store data in a secure and safe way in order to avoid intrusions and attacks. Also, it will reduce the cost and time to store the encrypted data in the Cloud Computing. In this paper conducts a performance analysis by implementing the Advanced Encryption Standard (AES) in all levels in order to check the performance of model.

Index Terms—Cloud Computing, Security, Advanced Encryption Standard.

I. INTRODUCTION

In the current past with the coming of quick systems administration advancements, there has a significant increment in the speed of the Internet and the level of network. Moreover, with the advancement in internet applications, for example, video conferencing, online joint workspaces, a mass talk, multi-client recreations and online interpersonal interaction applications, various potential outcomes for assemble interchanges have been made. Gathering members share basic interests and offer the duty of secure gathering correspondence. In recent decades cloud computing and cloud storage has become popular. Each unit ever-changing the tactic which tend to measure and greatly improve. Now due to limited number of storage resources and need of easy to get and use of storage space,people prefer to store all kinds of knowledge in cloud servers, that's in addition more suitable for corporations and organizations to keep away from overhead of deploying and maintaining instrumentation use when data unit hold on domestically. The cloud

server provides easily accessible storage space. That fitting well with need of person or group of person working together.Public storage facilities are easy to get. Data stored on public cloud may contain some valuable information so it need to protected. A cloud system is also suffer from attacks by every malicious users and cloud service provider. Data

sharing in cloud computing can provide flexible way of information exchange. Also provide greatest level of storage and computational resources to individuals and enterprises. Cloud computing also intimate many security and privacy features, such as data consistency, accuracy, authorized access, trustworthy, continue operating in event of same failure and like so. In is necessary to confirm the safety of the keep information within the cloud. Key agreement protocol is the basic cryptography element, which can provide secure communication among multiple participants in cloud environment. In cryptography, a key agreement protocol is protocol within which 2 or a lot of parties will agree on a key in such the simplest way that each influences the end result. By using the key agreement protocol,the participants of communication will firmly send and receive messages from one another. They agree upon common conference key share between them. Specifically, a secure key agreement protocol is wide utilized in interactive Communication environments with high security needs.

II. MOTIVATION

The recent developments in Cloud Computing allows for orga nizations and usersto use different applications and store their data on a Cloud.Through the study and research in the process of storing the encrypted data within thecloud .

We observed many problems, these are:

1. All types of data are stored using the same encryption algorithms.
2. The cost of storing the data on Cloud is high. Here wi ll need more space for storage.
3. The required time to encrypt and decrypt the data to/f rom the Cloud is long.

All the mentioned problems are because of there is not clear m ethod to split thedata into various classifications or levels to

make each level uses different encryption algorithms depending on the degree of important.

III. PROPOSED WORK

This is proposed that, the data are segmented into three different levels according to their data importance ranking. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is to store data in a secure and safe way in order to avoid intrusions and attacks.

- Encrypt the data to be stored in Cloud according to their importance.
- Reduce the time of data encryption, as well as, decrease the cost of storage and retrieval of data stored in the Cloud.
- The disparity in data encryption which makes data security within the Cloud is varies, therefore, make data security powerful and very difficult against the intrusion and hacker operations.
- Encrypt each file separately by encryption key(s), which aims to increase the protection of privacy and prevent its violation by the hacker, or even by the Cloud Computing service providers themselves.
- Protect the data as much as possible; to make the losses or the penetration of data in case of occurrence is very limited.
- Store the data in different Cloud providers depending on the level of importance

IV. SYSTEM OVERVIEW/SYSTEM ARCHITECTURE

The proposed model architecture consists of three levels, as shown in Figure 1.

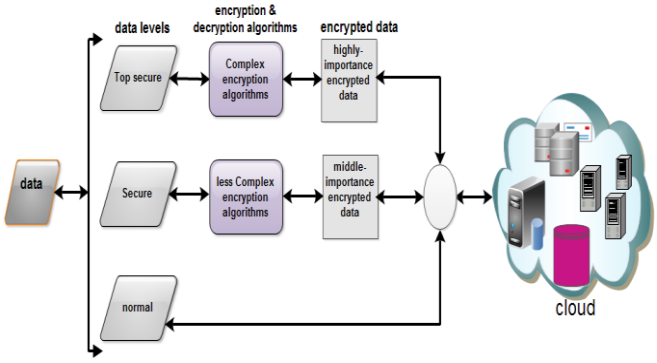


Figure 1: The Architecture of The Proposed Model

In the following subsection we will give a detailed description.

4.2.1 Data Segmentation

This phase takes the data and divides it using the Data-Segmentation Algorithm (as described in details in the next page) into three levels according to its importance , these levels are as follows:

Level 1 : Top Secure-Data

The data in this level is classified by the data owner as the most important and most sensitive data depending on set of specific measures. The data owner is responsible for determine these measures.

Level 2 : Secure-Data

The data in this level is classified by the data owner as middle important depending on set of specific measures. The data owner is responsible for determine these measures.

Level 3 : Classified-Data

The data in this level is classified by the data owner as a regular data that need no encryption at all. Classification of data in this level based on set of specific measures. These measures depend on the data owner point of view.

4.2.2 Data-Segmentation Technique

There are many ways to partition the huge data into set of proper and manageable size, such as horizontal or vertical segmentation, hybrid (horizontal and vertical), and database segmentation into subsets depending on specific criteria. Data varies from one field to another, so the data owner is responsible for data classification to appropriate subsets according to their importance, depending on specific measures, such as the following:

1- The degree of security and protection required for each dataset or group

2 - The required size for each group.

3 - The size of data that generated after encryption.

4 - The time required to store /retrieves each dataset.

Segmentation the data into groups (as shown in Figure 3.2) helps in reduce the storage and encryption costs, also increases the communication speed between the data owner and the cloud's services provider. For the hybrid segmentation (horizontal or vertical) and, also for database segmentation we proposed two methods for grouping data according to their importance level.

Design of DCACrypt

We developed an approach where data is split into block and these blocks store on many cloud storage by randomly show that network observer cannot find which block is sent on which cloud storage. Splitting of data can do on two basis.

1. Fixed size of data block. Block size vary from 1kb to 100kb depends on file type that means number of block will change as size and type of file changed.
2. Fixed number of block depends on file size and type size of block is change as size of file.

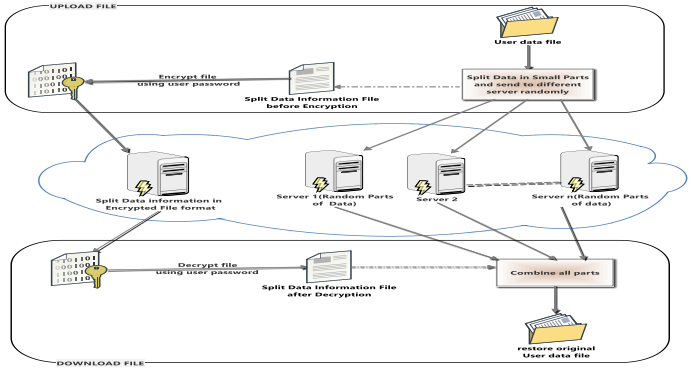


Figure 0.1Proposed DCACrypt Assumption

DCACrypt makes the following security assumptions

1. Communication between client and cloud storage is encrypted (SSL, etc.)
2. Cloud storage provider automatically backup each block to backup server.
3. There are enough simultaneous users to make anonymity feasible.
4. We have lightweight authentication mechanism using pool of session key.
5. Client machine is free from malware.
6. Provider will not able to link two different blocks of the same dataset.
7. Integrity of data block does not harm by cloud provide.

ALGORITHMS

1.Generation of a (v,k+1,1) design

To support a group data sharing scheme for Multiple participants apply an SBIBD. Our system design an algorithms to construct the (v,k+1,1) design to establish the group data sharing model for v participants can perform the key agreements protocol.in this v denote number of participants and number of block.Every block consist of k+1 participants and every participants appears k+1 time in these block.

Algorithm:
For i = 0; i <= k; i + +do (1)
For j = 0; j <= k; j + +do (2)
if j == 0 then (3)
B(i; j) = 0; else (4)
B(i; j) = ik + j; (5)
endif (6)
endfor (7)
endfor (8)
fori = k + 1; i <= (k2) + k; i + +do (9)
forj = 0; j <= k; j + +do (10)
if j == 0then (11)
B(i; j) = [(i □ 1)=k] (12)
Else (13)
B(i; j) = jk+1+MODk((i□j +(j □1)[(i□1)=k]) (14)
Endif (15)
Endfor (16)
Endfor (17)

The Reconstruction of Block:

The structure B of the (v; k + 1; 1)- design is constructed for v participants,should have the property that each block Bi embraces participant i.Here, Bi is the ith block of the structure of the (v; k + 1; 1)-design, and the order of the appearance of these v blocks is represented by i. If the structure B constructed by above algorithm does not have the required property then some transformations of the structure of B are needed. Reconstruction algorithm can be employed to accomplish the re-construction of B to E after the structure of B is created by Generation of(v, k+1, 1)design.

Algorithm:
E(0) = B(0); (18)
Fort = 1; t <= k; t + +do (19)
E(t) = B(tk + 1) (20)
B(tk + 1)[Flag] = 1; (21)
E(Et; 1) = B([Et; t □ 1=k]) (22)
B(tk + 1)[flag] = 1 (23)
Endfor (24)
Fori = k + 1; i <= k2 + k; i + +do (25)
IfB(i)[Flag]! = 1then (26)
E((Bi); [i + 1=K]) = Bi (27)
Endif (28)
EndFor (29)

V. RESULTS

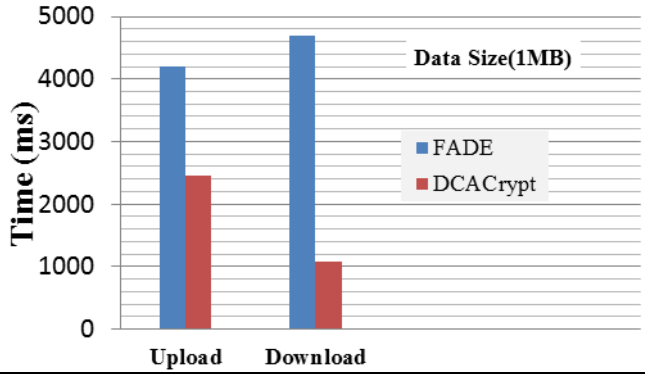
In this section we describe our work to simulate the proposed method. We implement our proposed method on java language. Java is very flexible and cross platform language. We use Java Enterprise Edition (JavaEE7) on Netbeans IDE. We use CloudBees as cloud service provider for storing data in cloud network For light weight file upload client we use Awake-library and for AES we used AESCrypt module. Table 2 show the simulation environment and default value

Table 1 Simulation settings

Platform	Java EE 7
Cloud Provider	CloudBees.com
No. of Server	2
Servers	JBoss 7 Tomcat 6
No of blocks per file	64
Type of data file	Image(JPG)
Cloud Resource Allocation	128MB RAM/ Instance

Experimental Results and analysis

This section provides result and analysis of our experiment. We test different size of data file for both uploading and downloading may times. Than calculate average valve of each size of data file. Table 3 show the result of our experiment It is clearly visible that as size of file increase computation time is increase. But most of the data file for normal user or small business users is limited to 5 MB. We compare our DCACrypt with FADE[52] in which pure AES is used. We get that our approach work very well with 1MB of data file



Data (MB)	Upload(ms)	Download (ms)
1	2446	1089
1.2	2456	1200
2.4	2566	1312
6.5	4438	1859

Figure 0.1 DCACrypt V/S FADE

VI. CONCLUSIONS

In this paper, we saw various solutions on how to ensure that data stored in the cloud is not maligned or corrupted by the service providers or other attack agents using various types of challenge response schemes in order to occasionally test the service provider for quality of data provided and ensuring data is correct. Another solution provides a technique to enforce security on the service providers by using provenance labels so that the clients or consumers are assured that they get the correct service they are paying for and thus ensuring maximum security for their data.

Securing a cloud service and providing privacy protection to customer and his data can be quite a daunting task, it would require a substantial effort on behalf of the cloud service provider and the industry in general to implement some of the techniques that have been explained here. To a large extent some of the onus lies with the service providers to live up to their reputation by implementing various features to ensure security and privacy in the services they provide.

We propose a cloud storage system based on DCACrypt which aim to provide confidentiality. We present a formal model of our approach and implement a prototype of DCACrypt to demonstrate it practically. Our experimental result provides that our approach is acceptable. And this may be used by Home and small business user.

VII. REFERENCES

[1]. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," *NIST Spec. Publ. 800-145*, pp. 1–7, 2011.

[2]. H. Takabi, J. B. D. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Secur. Priv. Mag.*, vol. 8, no. 6, pp. 24–31, Nov. 2010.

[3]. Y. Chen, V. Paxson, and R. H. Katz, "What's New About Cloud Computing Security?," *Electr. Eng. Comput. Sci. Univ. Calif. Berkeley*, no. UCB/EECS-2010–5, Jan. 2010.

[4]. V. A. Oleshchuk and G. M. Koien, "Security and privacy in the cloud a long-term view," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, 2011, pp. 1–5.

[5]. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot : Cloud storage with minimal trust Why untrusted storage ?," in *9th USENIX Symposium on Operating System Design and Implementation*, 2010.

[6]. R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling Security in Cloud Storage SLAs with CloudProof," *Proc. 2011 USENIX Annu. Tech. Conf.*, pp. 355–368, 2011.

[7]. "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification." [Online]. Available: http://www.w3.org/TR/P3P11/. [Accessed: 05-Sep-2013].

[8]. L. SWEENEY, "k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY," *Int. J. Uncertainty, Fuzziness Knowledge-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 200

[9]. Atul B.Kathole , Yogadhar Pande "Survey Of Topology Based Reactive Routing Protocols In VANET" International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 39 ISSN 2229-5518

[10]. A Wei Wei, Fengyuan Xu, Chiu C. Tan†, Qun Li (2013) "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks". 1045-9219/13/$31.00 © 2013 IEEE.

[11]. JIA YOU, ZHANGDUI ZHONG, GONGPU WANG, AND BO AI," Security and Reliability Performance Analysis for Cloud Radio Access Networks with Channel Estimation Errors" 2169-3536 2014 IEEE.