A Mutual Approach to Reduce Cost and Enhance the Security from Client Side to Cloud Storage Side

Dheeraj Kumar, Parikshit Prasad, Preetish Ranjan, and Abhishek Vaish

***Abstract*—This paper focuses on data leakage problem and its security in cloud storage technology. It has been seen that there are still some vulnerabilities in cloud storage which may results to compromise of C.I.A. This paper brings out, works on two phase of work to avoid data leakage problem, first phase is from client side and second phase is done by cloud provider side.**

The data which is stored by client in cloud storage application have different C.I.A. Some of them are Sensitive Having high confidentiality rating, some of them are least confidential but some of them have no confidentiality issue, which can have public access but require more integrity. In such situation, the data stored in cloud database with equal priority is not feasible. This paper has given a concept to store the data in database after prioritizing and then encrypting from client side itself. Before Uploading on cloud side, the client is required to mention criticality of that data. After Information declaration a matrix is prepared on basis of CIA analysis of data as desired by user which elaborates the criticality of data. Criticality is estimated on the basis of C.I.A. Confidentiality, Integrity and Availability. Based on sensitivity, data will be encrypted and access control list will be defined.. The second phase removes the problem of file access by another user who wants to access, as it is encrypted by client (owner).

The proposed model addresses for reliability in storage systems (where the key component under investigation is to maintain the C.I.A.). Our observations and techniques are instrumental for a wide spectrum of systems, ranging from distributed storage systems for the enterprise to cloud data services.

***Index Terms*—Cloud security, data protection, cost reduction, data storage, C.I.A.**

I. Introduction

A. Motivations and Background

Cloud computing is one of the emerging concept in today's business arena. It certainly may bring revolution in many domains. Cloud computing is known for its flexibility, low cost, client easiness and many more. Cloud computing helps the company to react quickly to market condition. It also allows company to focus on its core business [1]. Another advantage of cloud computing is that both small and medium sized business can instantly obtain the benefits of the large or extended infrastructure without having to implement and administer it directly [2]. Now a day, this technology is used for business continuity planning by permitting accessibility to multiple data centers anywhere on the globe. This means that as the demand of resources may increase, companies can add additional service, without having to pay for additional hardware and software.

1) The model and problem

Still people have lot of confusion about cloud computing. According to survey of CIO respondents [3] 58 percent says cloud computing will cause a radical shift in IT, 54 percent says cloud computing is evolving concept that will take years to mature, 36 percent says that currently on demand offering is not appropriate for my business and 18 percent says that it is passing fade. Why some organization is not relying on cloud computing? Why now companies are binding up there services from cloud computing technologies? This is because of fear of data leakage, they don't want to leak there sensitive data which may be disaster for their company [4]. There is the issue of confidentiality, integrity, availability of their data. There is a huge risk associated with its exposure [5]-[7].

Manuscript received February 5, 2013; revised July 13, 2013.

Dheeraj Kumar, Parikshit Prasad, Preetish Ranjan, and Abhishek Vaish are with the Dept. of Cyber Law Information Security Indian Institute of Information Technology, Allahabad, India (e-mail: {dheerajsrivastava12, chaurasiast, mail.preetishranjan}@gmail.com, abhishek@iiita.ac.in).

II. The Coverage Problem

This paper articulates the client to analyze, prioritize and then encrypt the data before sending for storage. As it is well known that the owner of data will only know how sensitive this data is. So keeping this as important aspect, this paper proposes a formula in first phase at client side. In this phase the client have to give the value of C. I. A. (confidentiality, integrity, availability) on 1 to 10 scales [8]. Now from first phase it is clear that the data send for storage is being encrypted itself, but now there is a problem i.e. how another person access this data if the owner define access control for either read access or write access. For this, either the owner has to give the key to that person, which is not feasible at all or he has to take some extra burden. To tackle this issue this paper proposes another model in second phase which work at cloud end. In this phase the proposed model uses the concept of TTL and TUID. TTL stands for "Time to Live" and TUID stands for "Temporary Unique Id". When user request owner to access the file, the owner immediately put the file from database of cloud to buffer and put TTL, TUID with it. Now owner grant TUID to user who want to access with the help of Zero concept [9] Shamir no key algorithm. After getting TUID the user access the file via server process.

A. Phase-1 General Framework for Data Storage In Cloud

As shown in Fig. 1, the data which is to be sent for storage is first analyzed by client itself by giving the value of different parameters i.e. CIA. After analyzing, the data is prioritized for applying the access controls for storage of

secured data. This encrypted data is then ready for storage in cloud.

The encryption of files is based on their corresponding sensitivity level. Initially the client is required to give information before sending for storage, like what are its confidentiality, integrity and availability? On the basis of rating scale (1 - 10) a matrix is designed and also priority is calculated from proposed formula, which suggest that files are encrypted (which encrypting algorithm) or leaved as it is. And accordingly access control is defined for that file. Proposed formula:

$$Criticality\ Rating = (C+I+ (1/A *10))/3 \quad (1)$$

C: Confidentiality of data (1- 10)
I: Integrity (1 -10)
A: Availability (1-10)

III. Analytical Base of the Framework

Assuming that there are 3 files: Client, Bills, and Company. Before sending these files to cloud storage, 3 attributes of these files should be defined in order to determine their criticality as shown in Table I. Based on these values, criticality rating of these files is calculated using Eq. 1.

Table II, shows the criticality rating of these files.

As shown in Table III, files with high rating value should be encrypted with stronger encryption algorithm and accordingly access controls for those files are to be defined.

A. Analysis of Phase-2

After the file is being encrypted at client end it sends for storage via gateway of cloud storage. This model suggests that nobody directly interact with database of cloud, they have to communicate via server process. This implies that when user logon, automatically a server process either starts or already started server process give response. Suppose the data is stored in cloud database, now if another user wants to access that file, he/she must have to contact to the owner of that file. The owner of that file send a request to the server process and server process with the help of writer process place that file in buffer along with TTL and TUID value

which is given by owner. If the user is legitimate then the owner gives TUID to him with the help of Shamir no key algorithm which uses zero concept (if applicable). Now user gets TUID from owner, he gets easily authenticated from server process by providing credentials as TUID. TTL is used to regulate access of resource of certain limit of time. When TTL expires the data get restored in database. If user has "write access" and he committed the change that he would have done. Then redo log is maintained with the help of log writer process and after certain defined time writer atomically writes to database. Log record is used to maintain for recovery process. There is archiving process to make archive the log to archive destination. With the help of Shamir's no key algorithm [9] owner of file, shares TUID to authenticated user.

Here a TUID is to be shared between owner and user without any information of owner to user or vice-versa. For this, owner uses a secret number *A* (1<*A*< (*P*-1)) where *P* is shared prime number between owner and user. Owner sends a message as shown in first pass to user. In the second pass user applies (message)^{B}Mod *P* (1<*B*<(*P*-1)) and send it back to owner. Owner again applies A^{-1}ModP to the received message and send it back to user (third pass). Finally, user applies B^{-1}ModP to the received message and gets the value of TUID without owner and user knowing the information about B and A respectively.

TABLE I: CIA Computation

Files	Confidentiality	Integrity	Availability
Client	9	9	3
Bills	2	8	7
Company	9	9	5

TABLE II: Criticality Rating

Criticality Rating	
Client	9
Bills	2
Company	9

TABLE III: Comparing Different Encryption Algorithm

Rating	Encryption Algorithm recommendation	Access control Required
10-9	AES 256	No Access Control
8-7	AES 192	READ
7-5	IDEA	READ,WRITE,
4-3	Blowfish	READ, WRITE,READ_ACL
2-1	Not Required	FULL CONTROL

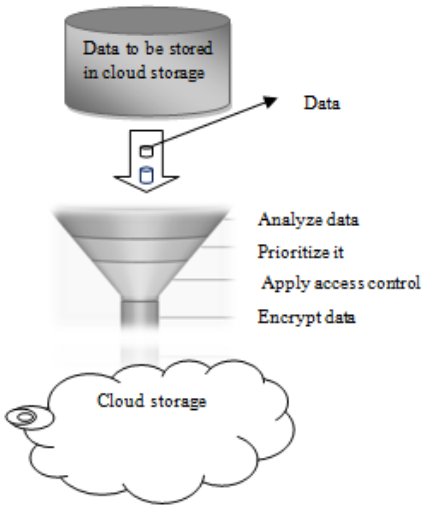

Fig. 1. Basic data flow.

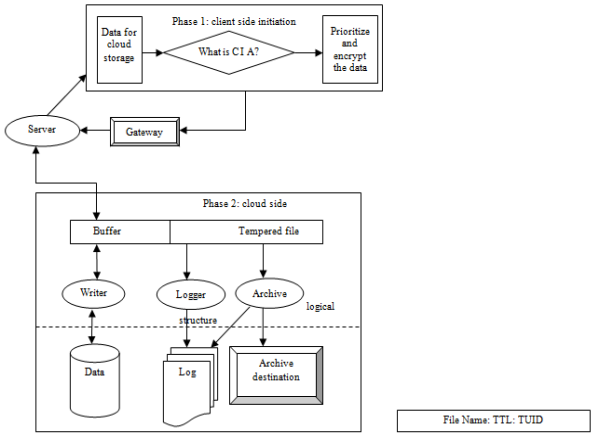

Fig. 2. Proposed model.

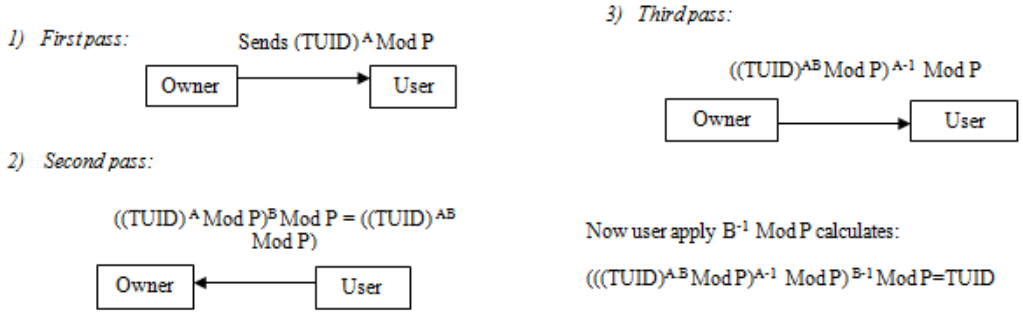

Fig. 3. The three passes.

IV. Result

Times are changing and so are ways of life. Cloud computing is going to create a win win situation for both user and service provider if it is made secure and easy to use. Through this model, the encrypted data is sent from client to cloud storage database. This model uses different parameter to maintain access control. The data stored now become more secure with the use of access control depending on criticality and storage cost is also reduced since the cloud storage is provided at a centralized point with enhanced security measures. Hence, this approach will definitely make cloud storage more reliable.

References

[1] P. Mell and T. Grance. (2010). *Draft Definition of Loud Computing*. [Online]. Available: http://csrc.nist.gov/groups/SNS/cloud-computing/index.
[2] S. S.-M. Chow, Q. Wang, K. Ren, and W. Lou, *Privacy-Preserving Public Auditing forSecure Cloud Storage*.
[3] Cloud computing risks-manageable survey. (2010). Report of C.I.O. survey. [Online]. Available: http://www.cio.in/topstory/cloud-computing-risks-manageable-survey
[4] An SME perspective on cloud computing survey, 2009.
[5] Infoworld. (2008). Gartner: seven cloud-computing security risks [Online]. Available: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1
[6] IBM. (2010). IBM virtualization. [Online]. Available: http://www.ibm.com/virtualization
[7] IBM. [Online]. Available: http://www-03.ibm.com/systems/itsolutions/virtualization/
[8] Taking Account of Privacy when Designing Cloud Computing Services Siani Pearson HP Labs, Bristol, UK HPL-2009-54.
[9] E. Dawson and C. Boyd, "Information security and privacy," presented at Third Australasian Conference, ACISP'98.

Dheeraj Kumar was born in 1986 in Varanasi district (Uttar Pradesh). His phone number is +918939424984 and the e-mail is dheerajsrivastava12@gmail.com. He completed his B.Tech. (Computer Science & Engineering) from Integral University, Lucknow, and then attained his M.S. (Information Security & Cyber Law) from Indian Institute of Information Technology, Allahabad. Dheeraj has published his research work in International Conference on Computing organized by Advanced Computing Research Society (ACRS) at Institute for Defense Studies and Analysis (IDSA), New Delhi. He has more than two years of Industry Experience. Currently he is working with Tata Consultancy Services as an Information Security Consultant. . He is a certified Lead Implementer for ISO27001. His major fields of work areas are ISMS, BCMS, IT Audit, Risk Assessment, Current State Assessment, Artificial Intelligence and Computer Networks.