Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 8; October, 2014 pp. 91-96
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Approaches for Data Storage Security in Cloud Computing

Md Waseem Akram

Al-Falah University, Faridabad, Haryana, (India)

Abstract: **Cloud computing is now a days an emerging field because of its performance and high availability. The foundation of cloud computing is the delivery of services, software and processing capacity over the Internet, reducing cost, increasing storage, automating systems, decoupling of service delivery from underlying technology, and providing flexibility and mobility of information. It is a new computing paradigm that attracted many computer users, business, and government agencies. It has gained a lot of hype in the current world of I.T. Cloud computing is said to be the next big thing in the computer world after the internet. The 'Cloud' represents the internet. Cloud computing is related to several technologies and the convergence of various technologies has emerged to be called cloud computing. In the cloud many services are provided to the client by cloud. Data store is main future that cloud service provides to the companies to store huge amount of storage capacity. But still many companies are not ready to implement cloud computing technology due to lack of proper security control policy and weakness in protection which lead to many challenge in cloud computing.**

The main objectives of this paper are, 1) To prevent Data access from unauthorized access, it propose a distributed scheme to provide security of the data in cloud .This could be achieved by using homomorphism token with distributed verification of erasure-coded data. 2) Proposed scheme perfectly stores the data and identifies the any tamper at the cloud server. 3) And also performs some of the tasks like data updating, deleting, appending. This paper also provides a process to avoid Collusion attacks of server modification by unauthorized users.

Keywords: **cloud computing, homomorphism token, Collusion attacks, servers, antagonist model, storage, Authentication.**

1. INTRODUCTION

Cloud computing is the most demanding and emerging technology throughout the world. Cloud computing is an Internet based computer technology. Some of the major firms like Amazon, Microsoft and Google have implemented the "CLOUD" and have been using it to speed up their business. The most basic service offered by cloud computing is that we can store any kind of data that we use in our day to day life from simple photographs, favorite songs, or even save movies to huge bulk amounts of data which is confidential. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. At first, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, we require verification of data storage in the cloud. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying accuracy of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The stored data in cloud may be frequently revised by the users, including operations like insertion, deletion, modification, affixing, reordering, etc.

Fig. 1. Results of IDC survey ranking security challenge

From the viewpoint of data security, which has always been an important aspect of quality of service, Cloud Computing unavoidably poses new challenging security threats for number of reasons.

- Unauthenticated person don't attack the authorized file.
- Avoids Collusion attacks.
- Malicious data modification attack.
- Dynamic data operations.
- Identification tamper server.

The benefits of cloud computing are many. One is reduced cost, since you pay as you go. Other benefits are the portability of the application is that users can work from home, work, or at client locations. This increased mobility means employees can access information anywhere they are.

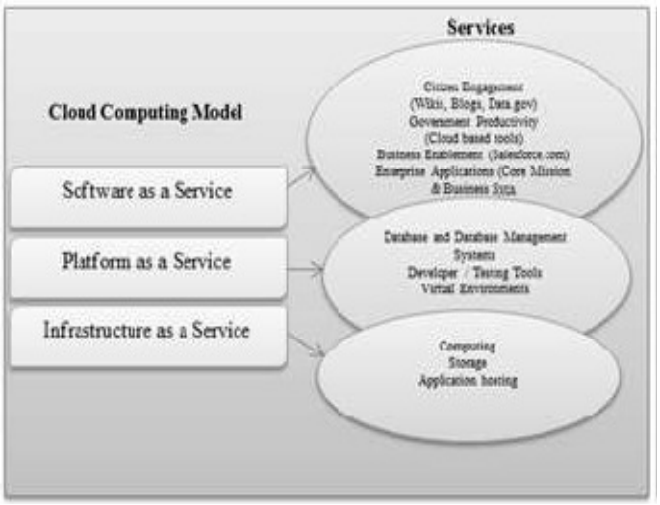
2. BACKGROUND

There are various things that are very important to understand the data storage in cloud computing:-

A. Cloud Computing Models

Cloud computing model provides mainly three types of services.

Those services are described below through a diagram.



a. ***SaaS:*** To use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser.

b. ***PaaS:*** To deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider(java, python, .Net)

c. ***IaaS:*** To provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

B. Layers of Cloud computing model

There are five layers in cloud computing model, the Client Layer, Application Layer, Platform layer, Infrastructure layer and server layer. In order to address the security problems, every level should have security Implementation

a. ***Client Layer:*** In the cloud computing model, the cloud client consist of the computer hardware and the computer software that is totally based on the applications of the cloud services and basically designed in such way that it provides application delivery to the multiple servers at the same time, as some computers making use of the various devices which includes computers, phones, operating systems, browsers and other devices.

b. ***Application layer:*** The Cloud application services deliver software as a service over the internet for eliminating the need to install and run the application on the customer own computers using the simplified maintenance and support for the people which will use the cloud interchangeably for the network based access and management of the network software by controlling the activities which is managed in the central locations by enabling customers to access the applications remotely with respect to Web and application software are also delivered to many model instances that includes the various standards that is price, partnership and management characteristics which provides the updates for the centralize features.

c. ***Platform layer:*** In the cloud computing, the cloud platform services provides the common computing platform and the stack solution which is often referred as the cloud infrastructure and maintaining the cloud applications that deploys the applications without any cost and complexity of the buying and managing the hardware and software layers.

d. ***Infrastructure layer:*** The Cloud Infrastructure services delivers the platform virtualization which shows only the desired features and hides the other ones using the environment in which servers, software or network equipment are fully outsourced as the utility computing which will based on the proper utilization of the resources by using the principle of reusability that includes the virtual private server offerings for the tier 3 data centre and many tie 4 attributes which is finally assembled up to form the hundreds of the virtual machines.

5. ***Server layer:*** The server layer also consist of the computation hardware and software support for the cloud service which is based on the multi-core processors and cloud specific operating systems and coined offerings.

C. Database Management in the Cloud

In recent years, database outsourcing has become an important component of cloud computing. Due to the rapid advancements in a network technology, the cost of transmitting a terabyte of data over long distances has decreased significantly in the past decade. In addition, the total cost of data management is five to ten times higher than the

initial acquisition cost. As a result, there is a growing interest in outsourcing database management tasks to third parties that can provide these tasks for much lower cost due to the economy of scale. This new outsourcing model has the benefits of reducing the cost for running Database Management System (DBMS independently [1].

A Cloud database management system (CDBMS) is a distributed database that delivers computing as a service instead of a product. It is the sharing of resources, software, and information between multiply devices over a network which is mostly the internet. It is expected that this number will grow significantly in the future. An example of this is Software as a Service, or SaaS, which is an application that is delivered through the browser to customers. Cloud applications connect to a database that is being run on the cloud and have varying degrees of efficiency. Some are manually configured, some are preconfigured, and some are native. Native cloud databases are traditionally better equipped and more stable that those that are modified to adapt to the cloud.

Despite the benefits offered by cloud-based DBMS, many people still have apprehensions about them. This is most likely due to the various security issues that have yet to be dealt with. These security issues stem from the fact that cloud DBMS are hard to monitor since they often span across multiple hardware stacks and/or servers. Security becomes a serious issue with cloud DBMS when there's multiple Virtual Machines (which might be accessing databases via any number of applications) that might be able to access a database without being noticed or setting off any alerts. In this type of situation a malicious person could potentially access pertinent data or cause serious harm to the integral structure of a database, putting the entire system in jeopardy.

3. SECURE CLOUD DATA STORAGE MODEL

The cloud storage model considering here is consists of three main components as illustrated in Fig. 2.

1) **Cloud User:** the user, who can be an individual or an organization originally storing their data in cloud and accessing the data.

2) **Cloud Service Provider (CSP):** the CSP, who manages cloud servers (CSs) and provides a paid storage space on its infrastructure to users as a service.

3) **Third Party Auditor (TPA) or Verifier:** the TPA or Verifier, who has expertise and capabilities that users may not have and verifies the integrity of outsourced data in cloud on behalf of users. Based on the audit result, the TPA could release an audit report to user.

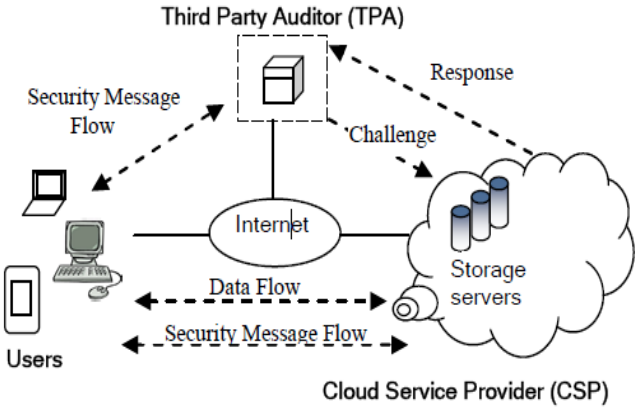


Fig. . 2. Cloud Data storage Model.

In cloud data storage model, the user stores his data in cloud through cloud service provider and if he wants to access the data back, sends a request to the CSP and receives the original data. If data is in encrypted form that can be decrypted using his secrete key. However, the data is stored in cloud is vulnerable to malicious attacks; it would bring irretrievable losses to the users, since their data is stored at untrusted storage servers. It doesn't matter that whether data is encrypted or not before storing in cloud and no matter what trust relations the client and the server may have a priori share. The existing security mechanisms need to re-evaluate. Thus, it is always desirable to need an efficient and secure method for users to verify that whether data is intact? If user does not have the time, he assigns this task to third party auditor. The auditor verifies the integrity of data on behalf of users.

B. Antagonist Model

Security intimidation faced by data stored in cloud servers come from two different sources. One hand, a CSP can be self-centered, un-trusted and probably malevolent. Not only it desires to move data that has not been or is rarely accessed to a lower tier of storage than agreed for fiscal reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on.

On the other hand, there may also exist an economically-motivated antagonist, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or erase users' data while remaining undetected by CSPs for a certain period. Specifically, we consider two types of Antagonist with different levels of capability:

a. ***Strong Antagonist*:** This is the worst case scenario, in which we assume that the antagonist can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are

colluding together to hide a data loss or corruption incident.

b. ***Weak Antagonist*:** The antagonist is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an antagonist can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.

4. CLOUD COMPUTING ATTACKS

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include:

a. ***Denial of Service (DoS) attacks:*** Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging.

b. ***Side Channel attacks:*** An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

c. ***Authentication attacks:*** Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

d. ***Man-in-the-middle cryptographic attacks:*** This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

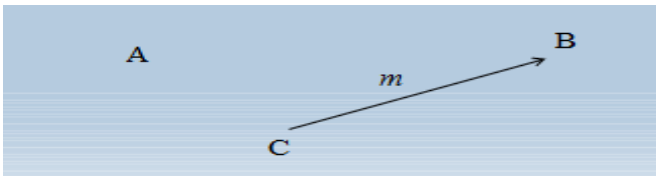
e. ***Inside-job:*** This kind of attack is when the person, employee or staffs who is knowledgeable of how the system runs, from client to server then he can implant malicious codes to destroy everything in the cloud system.

5. SECURITY REQUIREMENTS

In order to have a secured Cloud computing deployment, we must consider the following areas, the cloud computing architecture, Governance, portability and interoperability, traditional security, business continuity and disaster recovery, data centre operations, incident response, notification and remediation, Application Security,

In order to have secure cloud system, the following aspect must be considered:

I. Authentication: ensuring that whoever supplies or accesses sensitive data is an authorized party.

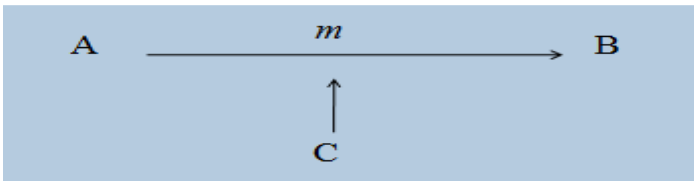


C could send a massage to B pretending to be A. If B cannot verify the source entity of the information then we have

Lack of Authentication

II. Confidentiality: assuring that only authorized parties are able to understand the data.

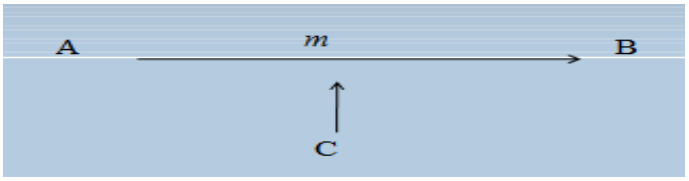
Consider the following security risks that could face two communicating entities in an unprotected environment:



C could view the secret message by eavesdropping on the communication.

Loss of privacy/confidentiality

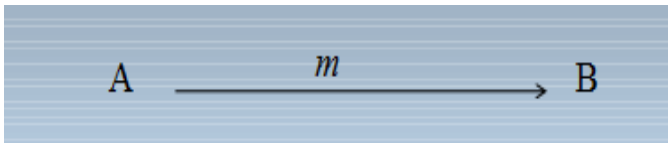
III. Integrity: ensuring that when a message is sent over a network, the message that arrives is the same as the message that was originally sent.



C could alter/corrupt the message, or the message could change while in transit. If B does not detect this, then we have. . .

Loss of Integrity

Nonrepudiation: ensuring that the intended recipient actually received the message & ensuring that the sender actually sent the message.



A might repudiate having sent m to B

6. PROPOSED SYSTEM

The purpose of the intended study is to develop an encryption and decryption algorithm. Algorithms are developed in such a way that they would be easy to understand & implement.

The process of encryption is kept simple:

- For given plain text characters, numbers starting from zero (0) onwards get assigned for Position representation.
- Once Position based encryption Algorithm gets applied, plain text characters get replaced with cipher text by using Table-I & Table-II mentioned below.
- The algorithm takes care of replacing same plain Text characters, with different cipher characters as a part of conversion which builds required complexity.
- We need to refer Rows in tables as position of characters whereas column represents character itself.
- The cipher text letter is derived as an intersection of the row & column for the chosen character in consideration.
- If original character is „blank space", the counter for position is reset to 0.

7. ENCRYPT TEXT DATA FOR STORAGE

Consider original text as: *'methods can be used to encrypt data'*. Let's take first two words of above word for example purpose.

Positions will be represented as below

- m e t h o d s
- 0 1 2 3 4 5 6

Encryption: methods

1. Char[x] = [0+25-12] %26 = 13 = "n"
2. Char[x] = [1+25-4] %26 = 22 = "w"
3. Char[x] = [2+25-19] %26 = 8 = "i"
4. Char[x] = [3+25-7] %26 = 21 = "v"
5. Char[x] = [4+25-14] %26 = 15 = "p"
6. Char[x] = [5+25-3] %26 = 1 = "b"
7. Char[x] = [6+25-18] %26 = 13 = "n"

Decryption: Cipher text : nwivpbn:

1. Char[x] = [0+25-13] %26 = 12 = "m"
2. Char[x] = [1+25-22] %26 = 4 = "e"
3. Char[x] = [2+25-8] %26 = 19 ="t"
4. Char[x] = [3+25-21] %26 = 7 = "h"
5. Char[x] = [4+25-15] %26 = 14 = "o"
6. Char[x] = [5+25-1] %26 = 3 ="d"
7. Char[x] = [6+25-13] %26 = 18 ="s"

8. TABLE USED

	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
1	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b
2	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c
3	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d
4	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e
5	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f
6	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g
7	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h
8	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i
9	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j
10	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k
11	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l
12	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m
13	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n
14	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o
15	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p
16	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q
17	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r
18	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s
19	s	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t
20	t	s	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v	u
21	u	t	s	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w	v
22	v	u	t	s	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x	w
23	w	v	u	t	s	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y	x
24	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	I	h	g	f	e	d	c	b	a	z	y
25	z	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

9. CONCLUSION

The purpose of this study is to provide a secured & computation efficient solution to encrypt text data for the security purpose. That data are now more secure to store on cloud server or anywhere for communication. The implementation of the developed algorithms is simpler as system requirements (both hardware and software) are not significant. Numbers and Picture files are not in scope of this work. If the user requirement is specifically for Key based algorithm, above algorithm would needs to be suitably modified.

REFERENCES

[1] Masayuki Okuhara et al, "Security Architecture for Cloud Computing", FUJITSU Sci. Tech. J., Vol. 46, No. 4, pp. 397-402 (October 2010)

[2] Sun Microsystems, Inc., "Introduction to Cloud Computing Architecture", White Paper, 1st Edition, June 2009.

[3] Gerald Kaefer, "Cloud Computing Architecture", Corporate Research and Technologies, Munich, Germany, Siemens AG 2010, Corporate Technology

[4] Peter Tseronis, "Cloud Computing Overview: A Federal Government and Agency Perspective", ArchitecturePlus Seminar -Cloud Computing, Web 2.0 and Beyond: A Vision of Future Government Operations, August 13, 2009

[5] Kangchan Lee, "Cloud Computing", Vice Chairman of ITU-T FG Cloud Chairman of Mobile Cloud WG in CCF in Korea, ETRI.

[6] VeriSign, "Digital ID, A Brief Overview", A VeriSign White Paper, 2004 VeriSign,

[7] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, Security", CRC Press 2009 by Taylor and Francis Group, LLC.

[8] Information Security Management Handbook by Harold F.Tipton, Micki Krause

[9] S J Shepherd. Public Key Stream Ciphers Published in Security and Cryptography Applications to Radio Systems, IEE Colloquium on Date of Conference: 1994 Page(s): 10/1 - 10/7.

[10] www.schneier.com/blog/archives/2012/11/encryption_in_c.html.

[11] Mandeep Kaur, Manish Mahajan Using encryption Algorithms to enhance the Data Security in Cloud Computing Volume 01 – No.12, Issue: 03 Page 56-59 International Journal of Communication and Computer Technologies

[12] Uma Somani, Kanika Lakhani, Manish Mundra Implementing digital signature with RSA Encryption Algorithm to enhance the data security of cloud in Cloud Computing, 2010.