Improving Cloud Storage security using TPA &Watermarking Technique

D.Jayandhiran, Assistant Professor,Department of Information Tech., Sri Lakshmiammal college of Engg. & Tech.

D.Sumithra, Department of Computer Science, Christ College of Engineering &Tech

Abstract

Cloud computing is the way of providing services to the user in the form of delivery of services over internet. Many users place their data in the cloud storage; however the problem is that users no longer have physical possession of large size of outsourced data. The data integrity protection in could computing is a challenging and potentially formidable task, especially the user data constrained computing resources and capabilities. Cloud computing mechanism transfers the data to third party auditor using private key and public key. The load image from the server provides the security and stored files from the particular cloud server. TPA sends to the public key from the client and connects to the server. They data provide secret key and those data to be stored in the cloud server, and connect TPA and accept private key and request the user viewing the information from authentication persons, as well as them to be changed or modify in the data cloud server. TPA cannot change data cloud computing mechanism, as well as those data should be stored in the private cloud

Keywords: TPA, Data Coloring, Public key, Private Key, Cloud computing mechanism.

I. INTRODUCTION

Cloud computing is foreseen to be the upcoming architecture to be employed in industries, owing to its vast merits in information technology history. Need for self-services, universal network processing of a network location autonomous resources availability, spontaneous resources flexibility, pricing is determined on the level of usage also on the risk of the transfer. Computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware. Through the use of virtualization and resource time-sharing, clouds address with a single set of physical resources a large user base with different needs. Thus, clouds promise to enable for their owners the benefits of an economy of scale and, at the same time, reduce the operating costs for many applications. For example, clouds may become for scientists an alternative to clusters, grids, and parallel production environments [1]. The ever cheaper and more powerful processors, together with the “software as a service” (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high-quality services from data and software that reside solely on remote data centres.

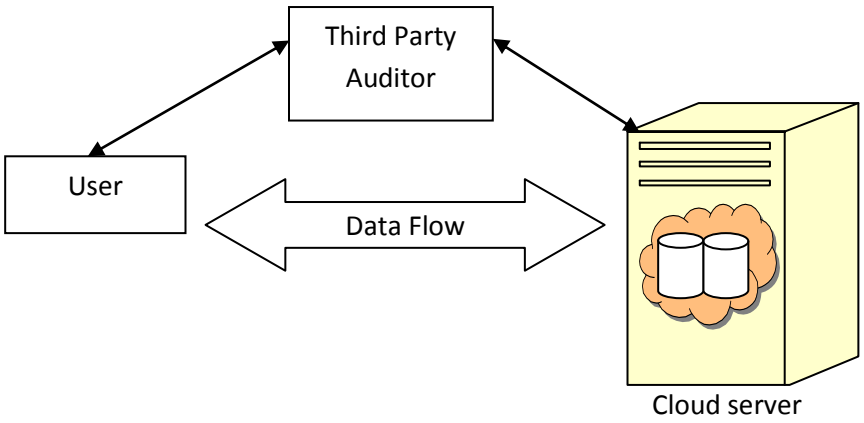
Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible

from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [10]. Although envisioned as a promising service platform for the Internet, this new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns in cloud data storage is data integrity verification at entrusted servers. For example, the storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files [2]. TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform [5].This public auditor will help the data owner that his data are safe in cloud. With the use of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand. When n numbers of user are using the data than consistency of data is quite important because anyone can use the data, modify the data or delete the data. If situation arise where one is writing a data while one is reading than it may be wrong read by second user .So to resolve the data dynamics is become an important task of the data owner. So in my scheme we added the information of insertion, updating and deletion in the message.

II. THIRD PARTY AUDITING

Cloud computing is a model which provides a wide range of applications under different topologies and every topology derives some new specialized protocols. TPA is the third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform. This public auditor will help the data owner that his data are safe in cloud.

With the use of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand. When n numbers of user are using the data than consistency of data is quite important because anyone can use the data, modify the data or delete the data. So to resolve the data dynamics is become an important task of the data owner. So in my scheme we added the information of insertion, updating and deletion in the message.



III. DIGITAL WATERMARKING

A digital watermark is a pattern of bits inserted into a digital file - image, audio or video. Such messages usually carry copyright information of the file. Digital watermarking takes its name from watermarking of paper or money. But the main difference between them is that digital watermarks are supposed to be invisible or at least not changing the perception of original file, unlike paper watermarks, which are supposed to be somewhat visible.

Watermarking Techniques Water marking is the process of adding the user text at the back of image files. And it's used to shading the text into an image files. And it's mainly used for digital patent administration. Static watermarks are stored in the application complete itself. And have been around for a long time. Markowitz and Cooperman and Davidson and Myhrvold are two techniques of static watermarks. According to Markowitz and Cooperman a static watermark is embedded in an image using one of the many media watermarking algorithms. Whereas according to Davidson and Markowitz static code watermark a fingerprint is encoded in the basic block sequence of a program's control flow graphs.

Dynamic watermarking of PDF content is rules-based. The PDF Watermark Administration screen provided to define rule sets via the Rules tab. If a given request for a PDF document satisfies one of the pre- defined rules, the template associated with that rule is used to watermark a copy of the content before the copy is returned to the requesting user; only the web layout form will be watermarked, the original PDF file unchanged in its vault location.PHP features a wide array of functions for image handling and manipulation. In today's article, we are going to use those functions to create an image watermarking class. This class will operate on two images: a source image and a watermark. As an optional third parameter our class will also accept an alpha value allowing our watermark to contain alpha transparency.

This should be an enjoyable exercise, but hopefully it will also be one that very useful. For example, let us imagine a scenario where you are hired to create a searchable inventory system for a stock photography website. Obviously you will need to protect your client's photographs offering full quality images only to paying customers. To do this, you could create multiple copies of each image, or you could simply implement a watermarking script like the one we are about to create. This script could then add a watermark to any un purchased images, while leaving those that have been purchased unmarked.

IV. PROPOSED ARCHITECTURE

We can use data coloring at unreliable security levels based on the changeable cost function practical. Figure 1 show the details involved in the color-matching process, which aims to relate a colored data object with its owner, whose user classification also colored with the same and recognition individuality. The color- matching process guarantees that color applied to user recognition match the data colors. This can initiate various trust-management events, including verification and authorization. Virtual storage supports color generation, embedding, and extraction. Decoloring process should be executed under decryption process. And it followed by Third Party Auditor because TPA works to checks user as record or not. Generally, Decoloring the process of reconstruct colored image. And it could be processed during decryption process.

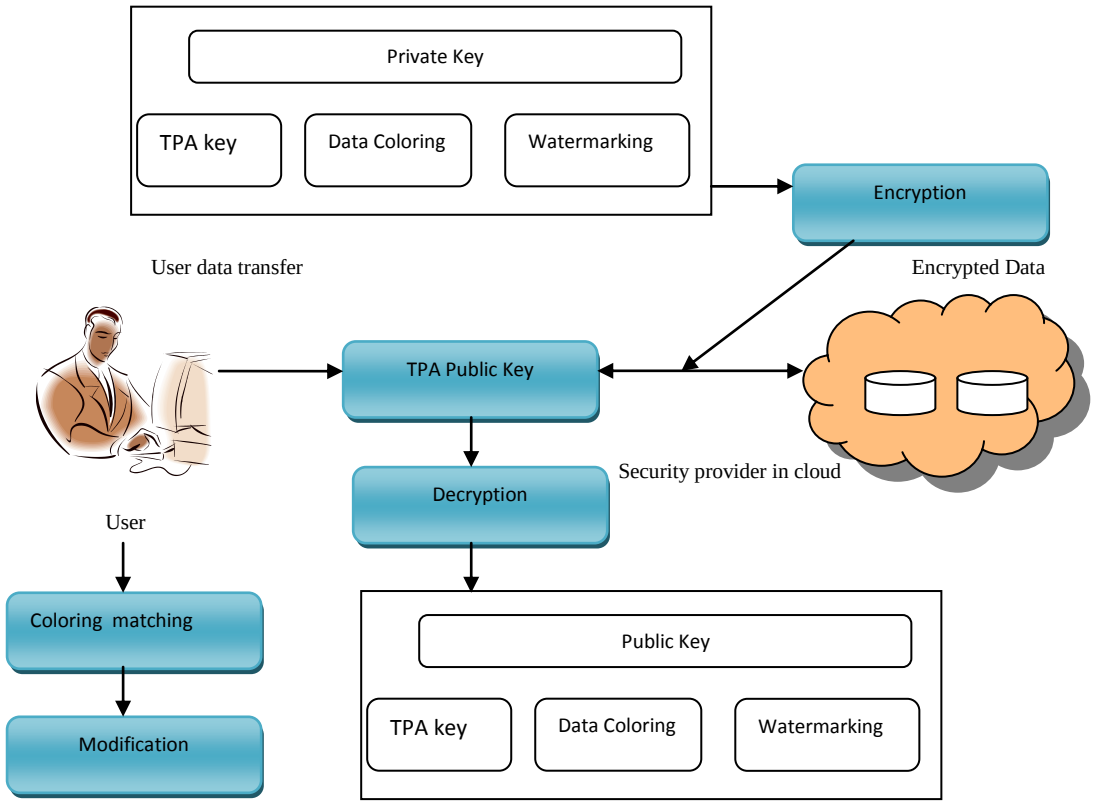


Figure 1 Proposed Architecture

V. CONCLUSION

Data coloring and watermarking techniques used to transfer the data between the user and TPA was presented in this paper. It provides the secret key connects to the cloud server transferred data between the user and cloud server. Data Integrity is maintained very effectively using this cloud server which provides the private key and public key transfer the data from the multi cloud server. The users provide the security key cannot change or modify the TPA the authorized persons only those data should be changed in the cloud computing mechanism.

REFERENCE

[1] G. Divya Zion, D.Kavitha "Remote Sensing Data as a Service in Hybrid Clouds: Security Challenges and Trusted Third Party Auditing Mechanisms" Vol. 1, Issue 7, September 2012.-pg: 1

[2] Sichuan Province Email: wangshaohui@njupt.edu.cn1. -pg:2

[3] Ragib Hasan" Security and Privacy in Cloud Computing" Johns Hopkins Universityen.600.412 Spring 2010.-pg: 2,5

[4] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S" Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud" IJCST Vol. 2, Issue 2, June 2011.-pg: 31,34, 61.

[5] Everaldo Aguiar "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security "University of Notre Dame, Notre Dame, IN, e-mail: eaguiar@nd.edu.-pg: 1, 4,5

[6] Cong Wang, Qian Wang, and Kui Ren "Ensuring Data Storage Security in Cloud Computing" Email: {cwang, qwang, kren}@ece.iit.edu.-pg:2,3

[7] K.S.Sathiyapriya" Integrity And Security Check Through Data Coloring And Water Marking Using Third Party Auditor In Cloud Computing Atmosphere"Vol. 2 Issue 1, 2012,95-99.-pg: 1, 2,6.

[8] Wang Shao-huiP 1, 2 *P , Chang Su-qinP1P, Chen Dan-weiP1P, Wang Zhi-weiP "Public Auditing for Ensuring Cloud Data Storage Security With Zero Knowledge Privacy" 1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing210046, China; pg:1 to 19.

[9] Operations in cloud computing environment "vol. 2 no. 10 October 2012.-pg: 2

[10] Katukam Ganesh" Ensuring and Reliable Storage in Cloud Computing" Vol. 3 (5) , 2012,5157 – 5163.pg: 3, 4

[11] D. Kishore Kumar, G.VenkatewaraRao, G.SrinivasaRao" Cloud Computing: An Analysis of Its Challenges & Security Issues" Issue 5, October 2012.-pg: 1, 2

[12] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan.S "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud" IJCST Vol. 2, Issue 2, June 2011.-pg: 34, 61 and -pg: 31,61