IJCAT - International Journal of Computing and Technology, Volume 1, Issue 11, December 2014
ISSN : 2348 - 6090
www.IJCAT.org

A Meticulous Description of Applying Watermarking Technique for Secure Cloud Storage

[1] M. Guresh, [2] R. Suresh

[1] M.Tech 2nd Year, Department of CSE, CREC
Tirupati, AP, India

[2] Professor & HOD, Department of CSE, CREC
Tirupati, AP, India

Abstract - The Cloud computing is a latest technology which provides various services through internet. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this paper, we propose a new innovative idea for Privacy Preserving Public Auditing with watermarking for data Storage security in cloud computing. It supports data dynamics where the user can perform various operations on data like insert, update and delete as well as batch auditing where multiple user requests for storage correctness will be handled simultaneously which reduce communication and computing cost.

***Keywords* - Privacy Preserving, Security, Cloud computing, Data storage, Watermarking.**

1. Introduction

CLOUD computing continues to be envisioned as being the next generation information technology (IT) architecture with regard to enterprises, because of its big list of unparalleled advantages within the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and also transference of risk . As being a disruptive technology together with profound implications, cloud computing is actually transforming the particular nature associated with how businesses use information technology. One fundamental part of this paradigm shifting is always that data are now being centralized or even outsourced towards the cloud. From users' perspective, which includes both of these individuals also it enterprises, storing data remotely towards the cloud in a very flexible on-demand manner provides appealing benefits: relief from the burden with regard to storage management, universal data access together with location independence, as well as avoidance associated with capital expenditure upon hardware, software, along with personnel maintenances, etc.,. Even though cloud computing makes them advantages more desirable than ever before, in addition , it brings new as well as challenging security threats toward users' outsourced data. Considering that cloud service providers (CSP) are usually separate administrative entities, data outsourcing is definitely relinquishing user's ultimate control within the fate with their data.

Consequently, the correctness from the data within the cloud has been put at an increased risk because of the following reasons. To begin with, even though infrastructures within the cloud less difficult more efficient and reliable compared to personal computing devices, they may be still facing the particular wide range of both external and internal threats with regard to data integrity . Samples of outages and also security breaches of noteworthy cloud services appear every now and then. Second, there perform exist various motivations for CSP to be able to behave unfaithfully towards the cloud users regarding their particular outsourced data status. As users will no longer physically contain the storage with their data, traditional cryptographic primitives with regards to be able to data security protection cannot be directly adopted. Specifically, simply downloading each of the data because of its integrity verification is just not a practical solution because of the expensiveness in I/O and transmission cost throughout the network. Besides, it is sometimes insufficient to be able to detect the data corruption only if accessing the particular data, mainly because it doesn't give users correctness assurance for all those unaccessed data and could possibly be already happening to get better the data loss or damage. The particular cloud server stores wide range of data which doesn't offer guarantee upon data integrity as well as consistency. This issue is addressed as well as solve by providing public auditing with regard to secure cloud.

To be sure the data security as well as integrity in order to reduce online burden it can be worth focusing on to allow public auditing service with regard to cloud storage, to ensure that user may make use of third-party auditor (TPA) to be able to audit the information. TPA does the particular auditing process on the part of the user. The particular TPA who may have capabilities and also expertise that may periodically look into the integrity from the data saved in cloud. The particular user doesn't have the capabilities which the TPA has. The actual TPA look into the correctness of data kept in cloud with respect to user and look after the particular integrity of data. Which allows public auditing service will have a crucial role for privacy data security & reducing your data risk through hackers. The proposed system supports data dynamics in which user performs update, insert, delete operation. For public auditing process we use the hashing technique in which hash function is applied on the user's data. So during the auditing process TPA would not learn any knowledge or users data.

In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider/ cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud without worrying about storage and maintenance. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done. Security in cloud computing can be addressed in many ways as authentication, integrity, confidentiality. Data integrity or data correctness is another security issue that needs to be considered. The proposed scheme specifies that the data storage correctness can be achieved by using SMDS (Secure Model for cloud Data Storage).

It specifies that the data storage correctness can be achieved in 2 ways as

1) Without trusted third party
2) With trusted third party based on who does the verification.

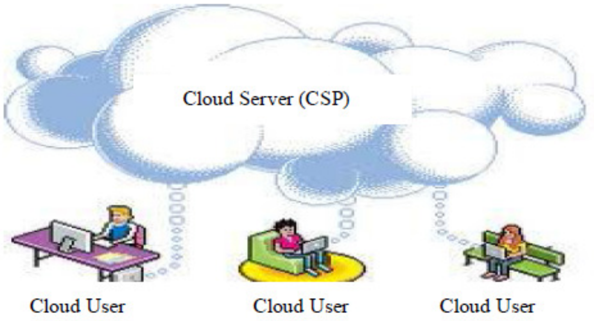

Figure 1: Cloud Architecture

It provides data confidentiality in two stages as

1) Data at rest
2) Data in transmission.

1) Data at rest: Symmetric key encryption technique (i.e. AES, TDES, and DES) are recommended which are secure but more time consuming.

2) Data in transmission: Secure Socket Layer (SSL) protocol is used for integrity verification. It uses a two different hash function such as Secure Hash Algorithm (SHA1) for digital signature and Message Digest (MD5) is a cryptographic hash function which is used to check the data integrity.

2. Literature Survey

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server / cloud service provider. Cloud user is a person who stores large amount of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data. The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data.
Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. It checks the

integrity of the data, storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance.

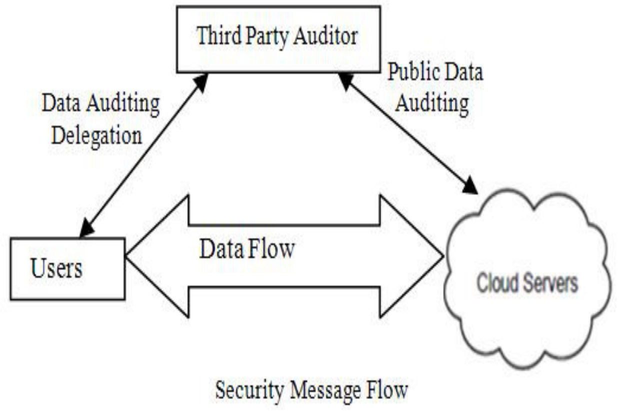

Figure 2: Architecture of Cloud storage service

In cloud, data is stored in a centralized form and managing this data and providing security is a difficult task. TPA can read the contents of data owner hence can modify. The reliability is increased as data is handled by TPA but data integrity is not achieved. It uses encryption technique to encrypt the contents of the file.

TPA checks the integrity of the data stored on a cloud but if the TPA itself leaks the user's data. Hence the new concept comes as auditing with zero knowledge privacy where TPA will audit the users' data without seeing the contents. It uses public key based homomorphic linear authentication (HLA) which allows TPA to perform auditing without requesting for user data. It reduces communication & computation overhead. In this, HLA with random masking protocol is used which does not allow TPA to learn data content.

2.1 Goals

- It allows TPA to audit users' data without knowing data Content
- It supports batch auditing where multiple user requests for data auditing will be handled simultaneously.
- It provides security and increases performance through this system.

2.2 Design Goals

1) *Public audit ability:* Allows third party auditor to check data correctness without accessing local data.
2) *Storage Correctness:* The data stored on a cloud is as it. No data modification is done.
3) *Privacy preserving:* TPA can't read the users' data during the auditing phase.
4) *Batch Auditing:* Multiple users auditing request is handled simultaneously.
5) *Light Weight:* Less communication and computation overhead during the auditing phase.

2.3 Batch Auditing

It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster.

2.4 Data Dynamics

It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Proposed scheme which support simultaneous public audability and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It uses MHT for block tag authentication.

Privacy Preserving Public Auditing Proposed by Cong Wang

Public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting for local copy of the data. Through this scheme, TPA can audit the data and cloud data privacy is maintained. It contains 4 algorithms as

1) *Keygen:* It is a key generation algorithm used by the user to setup the scheme.
2) *Singen:* It is used by the user to generate verification metadata which may include digital signature.
3) *GenProof:* It is used by CS to generate a proof of data storage correctness.

4) *Verifyproof:* Used by TPA to audit the proofs it is divided into two parts as setup phase and audit phase.

1) *Setup Phase:* Public and secret parameters are initialized by using keygen and data files f are preprocesses by using singen to generate verification metadata at CS & delete its local copy. In preprocessing user can alter data files F.

2) *Audit Phase:* TPA issues an audit message to CS. The CS will derive a response message by executing Gen proof. TPA verifies the response using F and its verification metadata.

TPA is stateless i.e. no need to maintain or update the state information of audit phase. Public key based homomorphic linear authentication with random masking technique is used to achieve privacy preserving public auditing. TPA checks the integrity of the outsourced data stored on a cloud without accessing actual contents. Existing research work of proof of retrievability (PoR) or Proofs of Data Possession (PDP) technique doesn't consider data privacy problem. PDP scheme first proposed by Ateniese et al. used to detect large amount corruption in outsourced data. It uses RSA based Homomorphic authentication for auditing the cloud data and randomly sampling a few blocks of files. A Second technique proposed by Juels as Proofs of retrievability (PoR) allows user to retrieve files without any data loss or corruptions. It uses spot checking & error correcting codes are used to ensure both "Possession" and "Retrievability". To achieve Zero knowledge privacy, researcher proposed Aggregatable Signature Based Broadcast (ASBB). It provides completeness, privacy and soundness. It uses 3 algorithms as Keygen, Gentag and Audit.

3. Proposed Scheme

The data on the cloud has a minimum concern about sensitive information such as social security number, medical records, bank transaction and shipping manifests for hazardous material. We provide additional security such as watermark technique at specific time interval. These techniques enable single sign-on in the cloud and access control for sensitive data in both public and private clouds. In the Proposed system we used water marking process, to store the data or images in the cloud server by assigning the public key, and this key and watermarking images are sent to third party and third party have complete authority to check the key and sent it to the server, and there Third Party Auditor must have a public key whenever the data to be retrieved. In the watermarking process, the security level is very high so the data or images cannot be identified by the attackers in the cloud. We also use Compression technique for watermark image to reduce communication overhead

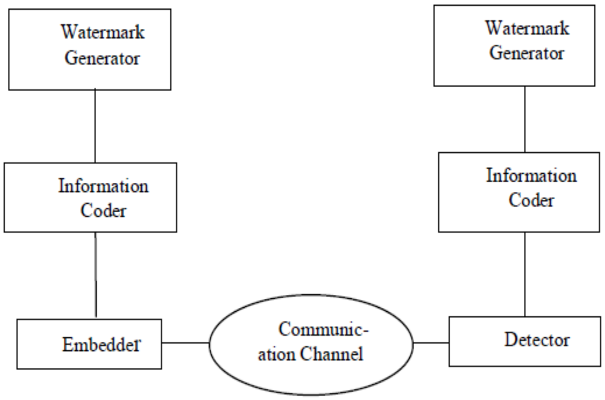

Figure 3: Watermarking Technique

Notations

n	number of attributes in the relations
m	number of tuples in the relations
Ci, m	Compressed Data
M	Signatured attributes
WM	Watermark Calculated
K	random choosing number
i	Watermarking value of tuple
j	Watermarking value of attribute

Watermark Generator Algorithm:

```
➢ Step 1: for i=1:n do
➢ Step2 : for j=1:m-2 do
➢ Step 3: WM=F(Celli,j );
➢ Step 4: M(i, j)=ADS(Celli,j );
➢ Step 5: end for
➢ Step 6: Ci,m−1=WM;
➢ Step 7: Ci,m=ACA(M(i));
➢ Step 8: Lock(Ci,m−1&Ci,m,K);
➢ Step 9: end for
```

The main elements in watermarking process: an embedded, a communication channel and a detector and is shown in Figure2. Watermark information is embedded into original image itself, and it is performed in the encryption process for making security on original information. Embedded is similar to encryption process which is used to change content into another format with the help of the secret key. Detector process is also similar to decryption process which is used to perform reverse process of encryption. The watermark information is embedded within the original image before the watermarked image is transmitted over the communication channel, so that the watermark image can be detected at the receiving end.

4. Results

Through the cloud computing server we are able to use are usually of sharing the particular files as well as data's or even any kind of images which can be in the form of privacy security within the existing system. Therefore it was tough to secure the particular data within the cloud, through the hackers. As well as from the existing system which usually most of us used the data coloring model to be able to secure, however the security level is actually low. However in the particular proposed system we make use of the method watermarking generation algorithm in order to secure the data within the cloud server that has been the data need to be secured within the cloud itself, to defend this through hackers. Therefore generally, we now have the particular attacks such as hackers, unauthorization attacks etc, which usually it had been essential within cloud systems.

This kind of cloud platforms which usually cause several difficulties with regard to business platforms that they can loss their particular a lot of the money this kind of insecurity cloud platforms. Therefore within these platforms by itself, we introduce the technique of watermarking as well as data color model to secure the information within the cloud server, which it must be in high security.

Within Figure 4 (0, 0.001, 0.002, 0.003, 0.004 as well as 0.005) signifies the amount of transactions which can be provided in the particular comparison scale with the existing system through the proposed system. Within the proposed we demonstrates the particular comparison through the figure which usually it can be seen which the proposed security process through the security as well as performance is greater than the data coloring process through an existing system. The actual results which might be indicate how the proposed technique will be extendable through the data coloring, which results in watermarking process as shown in the figure. Utilized Data coloring procedure that has been not so efficient, considering that the data security is just not safe. As well as by evaluating the particular performance from the data coloring together with water marking, the particular performance is extremely less within existing and proposed system. The particular water marking availability is actually high in the cloud computing. We are able to utilize this water marking procedure from different security levels from business intelligence, as well as economics and as well with regard to various market places computing.

Table 1. Performance evaluation of Datacoloring & watermarking Generating

	Datacoloring	**Watermarking Generating**
Security	0.0024	0.0041
Performance	0.0025	0.0044
Availability	0.0019	0.0033
Hard to Integrate	0.0046	0.0028

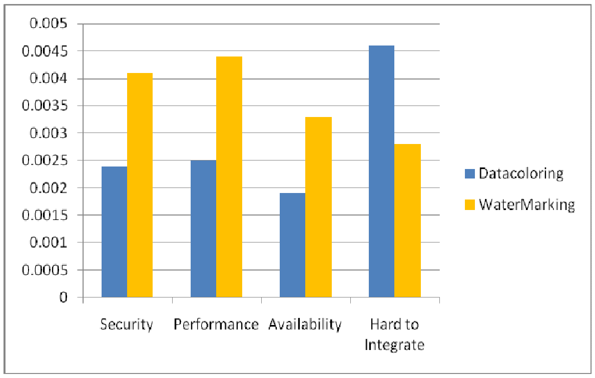

Figure 4: Performance evaluation of Datacoloring & watermarking Generating

5. Conclusion

In this paper, we proposed watermarking technique for Privacy Preserving Public Auditing for cloud data storage security. Cloud computing security is a major issue that needs to be considered**.** Using TPA, We can verify the correctness and integrity of data stored on a cloud. It uses public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preserving data security. We achieved zero knowledge privacy through random masking technique. It supports batch auditing where TPA will handle multiple users request at the same time which reduces communication and computation overhead. It uses bilinear signature to achieve batch auditing. We are introducing Privacy

Preserving Public Auditing with watermark process for secure cloud Storage**.**

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

[2] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

[4] Yunhong Gu , Robert L. Grossman, "UDT: UDP-based data transfer for high-speed wide area networks " National Center for Data Mining, University of Illinois at Chicago, 851 S Morgan St, M/C 249, Chicago, IL 60607, United States

[5] Yunhong Gu and Robert L. Grossman, "Supporting Configurable Congestion Control in Data Transport Services",Proceedings of the 2005 ACM/IEEE SC|05 Conference (SC'05).

Authors

M. Guresh completed my B Tech in Narayana Engineering College ,pursuing M Tech in Chadalawada Ramanamma Engineering College. His areas of interests includes Image Processing, software engineering , Object Oriented systems and Data Mining & Image Mining

Prof. R.Suresh received B.E.degree from SVNIT(REC) in 1996 and M.Tech., degree from JNTU Hyderabad in 2001 and pursuing the Ph.D degree from JNTUA, Anantapuramu. From 1998 to Till date he is with the JNTUA, Anantapur working at different levels. His areas of interests includes Image Processing, software engineering , Object Oriented systems and Data Mining & Image Mining. His Current interests include Texture model approach to Mammograms' classification and Detection.