Cloud Data Security while using Third Party Auditor

Ashish Bhagat
Department Of Computer Science & Engineering
Lovely Professional University, India

Ravi Kant Sahu
School of Computer Engineering
Lovely Professional University, India

ABSTRACT

In this paper the computing resources in the form of service rather than a utilities and product are provided to users over internet. The corporate world there are huge number of client which is accessing there data and modifying the data. The cloud is a platform where the data owner remotely stores their data in cloud. The goal of cloud computing concept is to secure and protect the data which come under the property of users and security of cloud computing environment is exclusive research area into which requires further development from both academic and research communities. The cloud application and services move to centralized huge data center and services and management of this data may not be trustable into cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. Third-party-auditor not only read but also may be change the data. Hence a mechanism should be provided who solved the problem. 1st the examines the problem contradiction between client CSP new potential securities schemes used to solve problem. the purpose of this paper is attempted to bring greater clarity landscape about cloud computing security and their solution at user level using encryption which ensure the data owner and client that there data are intact using algorithm.

Keywords

Data Integrity, Third party Auditor, Cloud Service Provider.

1. INTRODUCTION

Cloud computing gets name as a metaphor for the Internet. The computer industry is the only industry that is more fashion-driven than women's fashion he told to a group of Oracle analysts. So let's talk about what cloud computing is and tighten up definition and understanding of this implementation. Cloud computing has become most important propaganda issue in since 2007 and many companies used to attempt to use the cloud computing services. Typical cloud computing services are Amazon EC2 and Google app engine, amazons they use the Internet to connect to external users with the gadget, economy, high scalability and other advantages, Pick up any tech magazine or visit almost any IT website or blog and you'll be sure to see talk about cloud computing. Internet is represented in the network diagrams as a cloud, the cloud icon represents "all that other stuff" that is makes the network work. It's kind of like "etc."It also typically means an area of diagram or solution that is somebody else's concern so why diagram it all out? It is probably this notion that is most applicable to the cloud computing concept and Cloud computing promises to cut capital costs and operational more importantly let IT departments focus on strategic projects instead of keeping centralized the data centre running, as in [1].

As in [8] references statistics that suggest one third of breaches due to laptops falling in the wrong hands and about 16% due to stolen items by employees. It is up to the clients to decide the vendors depending on how willing they are to implement secure policies and be subject to 3rd party verifications. Sales force and Amazon, Google are currently providing such services charging clients using an on-demand policy Storing the data in the cloud can prevent these issues altogether. The basic point of view pattern is changing the way it is being focused over cloud. Users view i.e. in addition to this advantage it brings forth exclusive and challenging security threats towards user's outsourced data. Moreover, vendors can update application/OS/middleware security patches faster because of higher availability of staff and resources. Cloud computing change Internet into new computing platform is business model that achieve purchase on-demand and as pay-per-use in network has a broad development prospect. The proposed problem is multi write and problem of TPA if Third-party-auditor not only uses data but also modify the data than how data owner or user will know about in this problem. Here user has two types' keys one of which only the owner knows called private key and another one which is known to anyone called public key.

The third party match both the data it must be same as the sent one on the sender cannot deny that they sent it (non repudiation).Downloading of data for its integrity verification is not feasible task since it's very costly because of the transmission cost across the network.

It is very important to provide public auditing service for cloud data storage. For well organization it is very essential that cloud that allows investigation from a single party audit the outsource data to ensure data security and save the data storage and user's computation. That user trusts an independent third party auditor (TPA). It provides the reasonable way for users to check the validity of data in cloud. Check the integrity of data on cloud on the behalf of users. Public auditing in addition to user provides the external party to verify the correctness of stored data against external attacks it's hard to find. However these schemes, as in [7] don't involve the privacy protection of data and a main disadvantage which affect the security of the protocols in cloud computing. Cloud service provider has significant storage space and computation resource to maintain the user's data. Also it has expertise in building and managing distributed cloud storage servers and ability to own and operate live cloud computing systems. So users who depend on only TPA for their security storage want their data to be protected from external auditors. Users who put their large data files into cloud storage servers can relieve burden of storage and computation and at the same time it is important for users to ensure that their data are being stored correctly and security check. Users should be beautified with certain

security means so that they can make sure their data is safe and Cloud service provider always online & assumed to have abundant storage capacity and computation power. Third party auditor is invariably online too and It makes every data access be in control.

TPA eliminates the involvement of client through auditing of whether his data stored in cloud are indeed intact which can important in achieving economies of scale for Cloud Computing 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. Released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for cloud service provider to improve their cloud based service platform, as in [7].This public auditor will help to data owner that his data are safe in cloud with use of TPA management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensures that his data

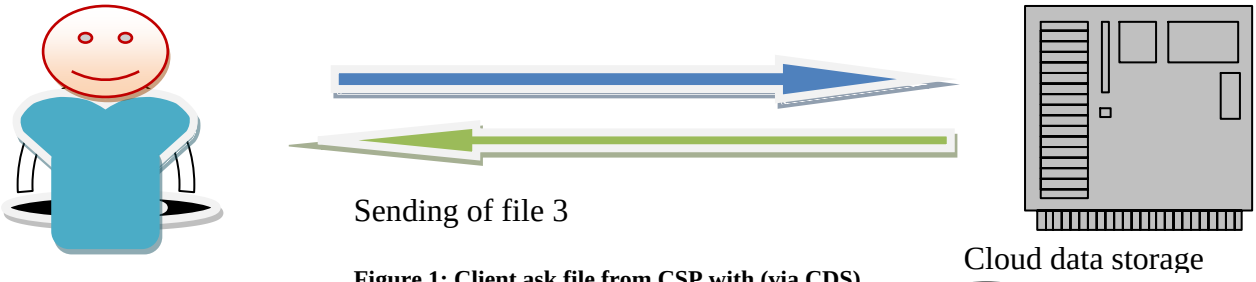


Figure 1: Client ask file from CSP with (via CDS)

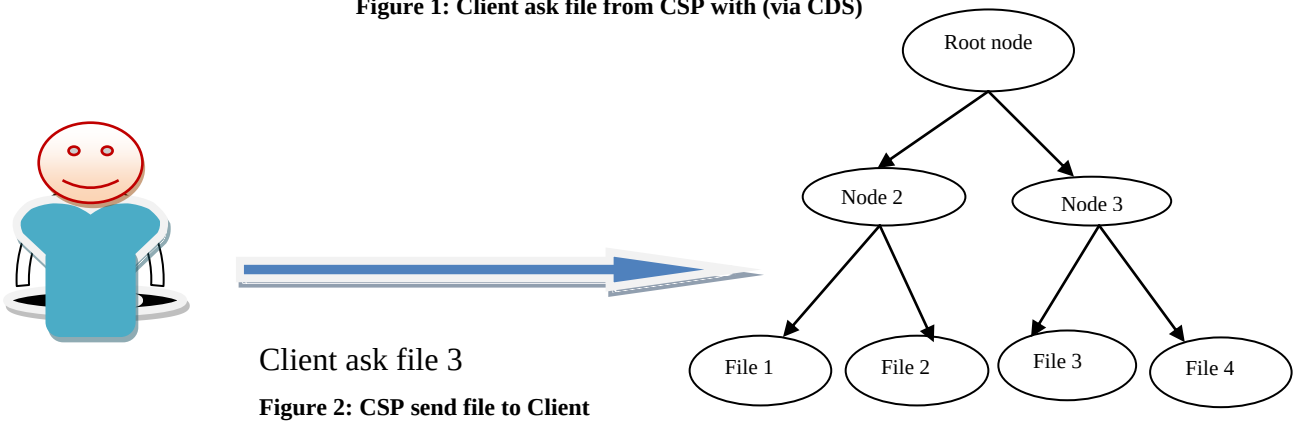


Figure 2: CSP send file to Client

are in a safe hand.
Two or more user is using the data any time than consistency of data is important because any time anyone unwanted person can use data and change or modify the data or delete data. If two user or more is using a data user one is reading a data while another one is writing a data than it may be wrong read by one user. So that resolve data inconsistency becomes an important task of the data owner.

2. REVIEW OF LITERATURE

Using Third Party Auditor as in [6] this 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, as in [2]. If two users or more users are using a data, one is writing a data while one is reading a data than it may be wrong read by 1 user, so to resolve data inconsistency is become an important task of the data owner. Another problem how to trust on TAP is not calculated. If TPA become intruder and pass information of data or deleting a data than how owner know about this problem are not solved Consistency and Integrity. Proposed scheme in this vm, Advanced Encryption Standard (AES) are used where client encrypt and decrypt the file. In this vm, this mechanism solves the problem of unauthorised access of data in this suggested scheme that can be used for integrity and consistency of data.

3. PRESENT WORK

In this paper we know about cloud computing security and find the problem in cloud data security using third party auditor and what is work of TPA and CSP and how can solve the problem when client and csp share the data in network and literature review.

4. PROBLEM FORMULATION

When two or more users are using data any time then consistency of data is more important because unauthorised person can use data and it can change or modify data or delete the data. New data storage paradigm in cloud computing bring about many challenging design issues which has profound influence on the performance and security of overall system. If two or more users are using data, user one is writing a data while other is reading data then it may lead to incompatibility. So resolving data inconsistency becomes an important task of data owner so that TPA can be used as an intermediate party between the user and the Cloud Service Provider. An another problem of TPA not only use data but also modify data than how data owner or user will know about this problem and contradiction between them and another problem is multi-write problem is important issue.

Machine by means of Software as a service this use a new algorithm to improve the security check the integrity of data. The researcher find out the problem which is security issues and third party auditor services and to manage this data using TAP that provides the security and also some key security in cloud computing security is most crucial task. Cloud computing entrusts services with users data, software and computation on a published application programming

interface over a network. Cloud provides a platform for many types of services and it has a considerable overlap with software as a service (SaaS) as in [5] End users access cloud based applications through a web browser or a light weight desktop or a mobile app while the business software and data are stored on servers at a remote location. The Cloud application providers strive to give the same or better service and performance than if the software programs were installed. When we are talk about cloud Security and maintaining data integrity is one of the most important and very hard tasks. When we are talk about cloud users and they are using cloud services, provided by the cloud provider, as in [5] and again, in the case of maintaining integrity of data so user cannot trust the service provider to handle data, as he himself can modify the original data and integrity may be lost and If a smart hacker hacks the cloud server and steals the data and modifies it then in some cases this modification is not even identified by the cloud provider. So, in this case, we take the help of a trusted third party auditor to check for the integrity of data.
This third party auditor takes care of data and makes sure that data integrity is maintained. In the view the procedure of integrity checking as a key's proficiency within software and platform, infrastructure security focuses area of cloud architecture. In the vision for helping assure ongoing system integrity in a virtualised environment includes an evolution of integrity checking competences, as in [5] each phase, in this evolution relies on secure start up enabled and provides an increasing level of assurance and in this evolution begins with one-time integrity checks at systems or hypervisor start up.

5. RESEARCH METHODOLOGY

The use methodology to getting results and shows the work of client, CSP and TPA.

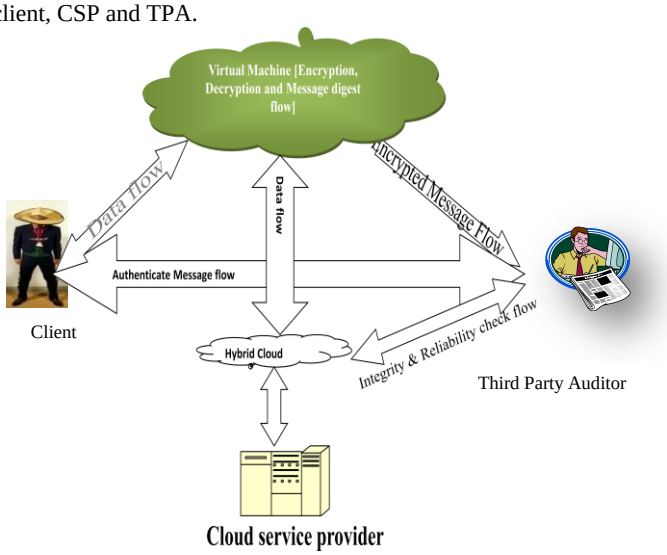


Figure 3: Architecture for Client TPA and Service provider

6. ALGORITHM

It checks the integrity of data and maintaining consistency at cloud data storage for Client and CSP.

For records updating algorithm (1a)

Client Side	CSP Side
1) Client request to access a file from CSP. ⇒	
	2) CSP ask client for authentication like login page.⇐
3) Client authentication CSP by his password. ⇒	
	4) Verify password if correct than send a file that he want to access. Else move to step 2.
5) Client decrypts the file by applying RSA decryption algorithm.	
6) If client modify the file than he will send file to TPA and CSP with a message like $\mathbf{M_d}$ as **(C'Ψ_s M)** and **C' here C'** for encrypted file Ψ_s for ElGamal Digital Signature and **M** denotes for modification. ⇒	
	7) CSP check the signature for authenticity and compute the message digest to find encrypted file which is compare with encrypted file of another message.
	8) If correct it will change previous file with this one end

	move to step 11.
	9) Else ask the client to follow the step 6
	10) CSP sends a same message **(C', M_d ← (C',Ψ))** to client after addition of his signature **Ψs** and TPA. ⇐
11) If **C'** file is same as previous one, drop this packet and move to step 1 or step 12. Else ask CSP to follow.	
12) Exit.	

In this way TPA verify encrypted file with message received from CSP.

For example of RSA with ElGamal digital signature algorithm.

1) Choose the two large prime number p and q.
Like **p=7 and q=17.**

2) Calculate N= (p*q). N=7*17 N= 119.

3) Select the public key $\phi(n) = (p-1)*(q-1)$ such that it is not a factor of this.

$\phi(n) = (7-1)*(17-1)$

$\phi(n) = 6*16$

$\phi(n) = 96$

Researcher have to choose **E** such that none of the factor of **E** is 2 and 3

(Can't choose E= 4, 15, 6….etc) let us choose E **= 5.**

4) (D*E) mod ((p-1)*(q-1)) = 1 **calculate D using this way 96*X+1 =?**

(D*5) mod ((7-1)*(17-1)) = 1

96*1+1=97

(D*5) mod (6*16) = 1

96*2+1=193

(D*5) mod 96 = 1

96*3+1=289

D = 3855/5

96*4+1=385

D = 77.

5). Suppose PT = 10, E=5.

$CT=10^5 \bmod 119$.

CT= 40. **For Encrypt.**

6). $PT = 40^{77} \bmod 119$

PT = 10. **For Decrypt.**

Example of ElGamal Digital Signature Algorithm:

GF (19) that is q=19.

Primitive roots (2, 3, 10, 13, 14, 15) we choose $\alpha=10$.

1) $X_A = 16$ Generate random integer (1<XA<q-1)

2) $Y_A = \alpha^{XA} \bmod q$

$Y_A = \alpha^{16} \bmod 19$

$Y_A = 10^{16} \bmod 19$

$Y_A = 4$.

3) Alice $X_A = 16$. Alice public key is $\{q, \alpha, Y_A\} = \{19,10,4\}$

Message with has value m=14. First computes the hash m=H (m).

i. Alice choose K=5, which is relative prime to [q-1 =18].

ii. $\delta_{1=} \alpha^k \bmod q$

$= 10^5 \bmod 19$

= 3.

iii. $K^{-1} \bmod (q-1)$

$5^{-1} \bmod (19-1)$

$5^{-1} \bmod 18$

=11

iv. $\delta_2 = k^{-1}(m-X_A \delta_1) \bmod (q-1)$

$=11(14 - (16)(3)) \bmod (19-1)$

$=11(14 - 48) \bmod 18$

$=11(-34) \bmod 18$

$=-374 \bmod 18$

=4

Signature consists of the pair $(\delta_1 \delta_2)$

v. Verify the signature

$V_1 = V_2$

$V_1 = \alpha^m \bmod q$.

$10^{14} \bmod 19 =$ **16**

$V_2 = (Y_A)^{\delta 1} (\delta_1)^{\delta 2} \bmod q. (4^3)(3^4) \bmod 19$

$64 * 81 \bmod 19$

$5184 \bmod 19 =$ **16**

7. SIMULATION AND RESULTS

The implemented RSA-with Elgamal Digital Signature based instantiations in windows 7. And an experiment is Conducted using Java on a System with an Intel core i5-2410M processor running at CPU @ 2.30GHz, installed memory(RAM) 4.00GB, System type: 64-bit OS, Intel® Mobile Express Chipset SATA AHCI Controller, Device type IDE ATA/ATAPI controller, 596.17 GB drive. Algorithms Elgamal Digital Signature is implemented using CloudSim and CloudAnalyst with Eclipse.

Initially researcher created one CSP, data owner and TPA. Data owner gave right to change data to 10 users with identity number and keys. In this identity number he sends to CSP and TPA. This user initially gave the file by using algorithm 1a then applied for all 10 users. Now run algorithms 1a step number 7 for TPA. TPA found all 10 files in appropriate form. Show on figure 4. Work Simulation. Give the overall response time and Response Time by Region; User Base Hourly Response Times, Data Center Hourly Loading and also find that scheme detect error probability about 99%. The data protecting from CSP and TPA is verified by the simulation as we had converted the file into encrypted form and show the analysis of response time and data center processing time and also show response time by region as show on table 1, 2. And data center request servicing time as show on table 3.

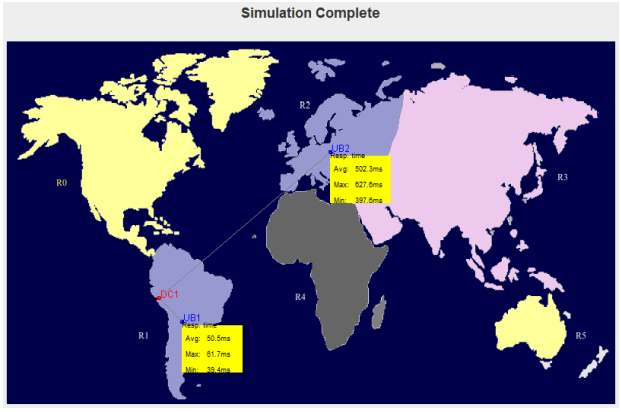


Figure 4: Show Simulation Work

Table 1 Overall Response Time Summary

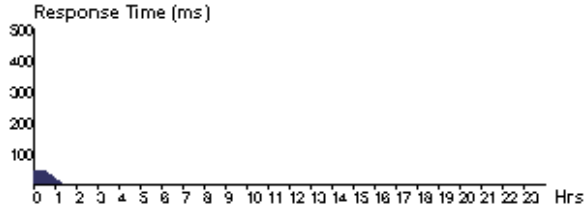
	Avg (ms)	Min (ms)	Max (ms)
Overall response time:	203.24	39.36	627.61
Data Center processing time:	0.51	0.02	1.10

Table 2 Response Time by Region

User base	Avg (ms)	Min (ms)	Max (ms)
UB1	50.53	39.36	61.71
UB2	502.30	397.61	627.61

User Base Hourly Response Times

UB1



UB2

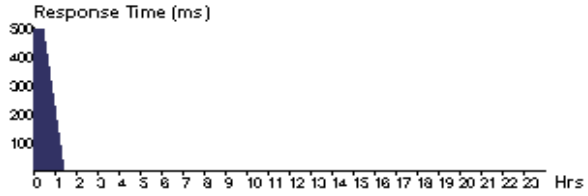
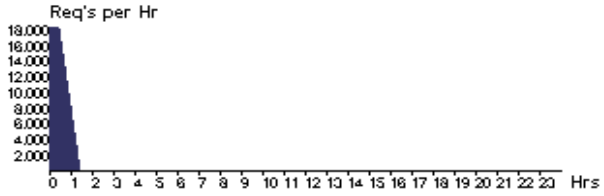


Table 3 Data Center Request Servicing Times

Data Center	Avg (ms)	Min (ms)	Max (ms)
DC1	0.51	0.02	1.10

Data Center Hourly Loading

DC1



8. CONCLUSION

Conclude that secure auditing protocol to store data and verify it and make algorithm with example. Use the RSA algorithm with ElGamal Digital Signature and for the process of encryption and decryption and which is solve the problem of integrity, unauthorized access, privacy and consistency. And in this article first present a network in which cloud Architecture work and which methodology used, user and TPA shown after that how file is retrieved. Encryption and decryption of file how to check the integrity of data from csp and client and how give the control to TAP.

9. REFERENCES

[1] Elsenpeter Robert ,Anthony T.Velte and Toby J.Velte, 2010. Cloud Computing A Practical Approach.

[2] Qian Wang and Cong Wang and Kui Ren, Wenjing Lou, Jin Li 2011. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing in IEEE transactions on parallel and distributed systems volume 22, no. 5.

[3] Cong Wang and Kui Ren and Wenjing Lou and Jin Li, 2010. To ward Publicly Auditable Secure Cloud Data Storage Services in IEEE.

[4] M.Ashah and R. Swaminathan and M. Baker, 2011. Privacy-Preserving Audit And Extraction of Digital Contents".

[5] H. Shacham and B. Waters, 2008. Compact Proofs of Retrivability in proc. of asiascrypt.

[6] Ravi Kant Sahu and Abhishek Mohta, L.K. Awasthi 2012. Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services, conf. IJARCSSE, Vol 2, Issue 2,ISSN: 2277 128X.

[7] P. Mell and t. Grance 2009. Draft Nist Working Definition of Cloud Computing, referred.

[8] Elinor Mills,2009. Cloud Computing Security Forecast: Clear Skies"