ISSN 2229-5518

Cloud Data Security while using Third Party Auditor

Abhishek Mohta and Lalit Kumar Awasthi

Abstract— The Cloud is a plateform where all users not only store their data but also used the software and services provided by Cloud Service Provider (CSP). The service provided by the cloud is very economical. The user pay only for what he used.This is a platform where data owner remotely store their data in the cloud to enjoy the high quality applications and services. The user can access the data, use the data and store the data. In a Corporate world there are large number of client who accessing their data and modifying a data. In Cloud, application software and services are move to the centralized large data center and management of this data and services may not be trustworthy. To manage this data we use third party auditor (TPA).It will check the reliabilty of data but it increases the data integrity risk of data owner. Since TPA not only read the data but also he can modify the data, therefore a mechanism should be provided who solved this problem. We first examine the problem and new potential security scheme used to solve this problem. Our algorithm encrypt the content of file at user level which ensure the data owner and client that there data are intact. Side by side it also preserves the data dynamics and consistency of n number of client and server.

Keywords— Third party Auditor, Integrity, Cloud Service Provider, Cloud Computing.

.

1 INTRODUCTION

CLOUD 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].

- Abhishek Mohta is currently pursuing M.Tech. in Computer Science and Engineering in NIT Hamirpury,India, PH-9736788306.E-mail:abhishek_mohta123@rediffmail.com

- Lalit Kumar Awasthi,a Professor and Head of Department of Computer Center in NIT Hamirpur, India, PH-01972254420. E-mail:lalitdec@yahoo.com

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

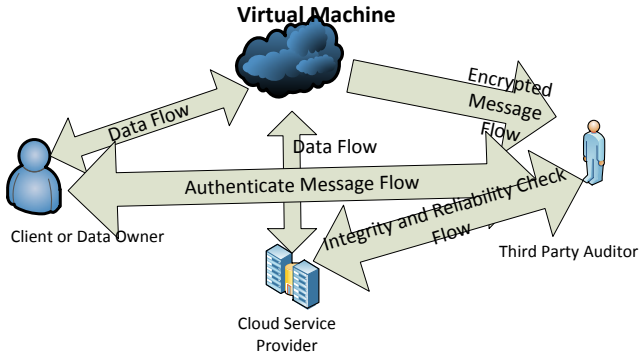
read by second user .So to resolve the data dynamics is become an important task of the data owner. So in my scheme we added the information of insertion, updation and deletion in the message.

2. THE BASIC SCHEME

2.1 Proposed cloud model

In the figure below we prepared a model in which Client, CSP and TPA are shown. The client asks the CSP to provide service where CSP authenticate the client and provide a virtual machine by means of Software as a service. In this Vitual Machine (VM), RSA algorithm are used where client encrypt and decrypt the file. In this VM, SHA-512 algorithms also there which make the message digest and check the integrity of data.

Figure 1: Architecture for Client, Third Party auditor and Cloud Service Provider



2.2 Cryptography at user level

After performing file operation it will send the data to CSP and TPA. This CSP and TPA will keep our data not only safe but also provide integrity but how it doesnot ensure that we will full trust on TPA. He can send data's of data owner to unauthorized user. If we remove the TPA even it will not solve the problem because CSP can also send the data to unauthorized user and also data owner does not get an advantage of TPA. So cryptography is required at user level. In this scheme encryption and decryption is done with the help of RSA algorithm. For supporting data dynamics when data owner got services from CSP than at that time it will generate a two large prime number as a key i.e. P_{uk} and P_{rk} . P_{uk} is the public key of Data owner where all clients will use this key as encryption and P_{rk} is the private key of Data Owner or Client. P_{rk} will be used to decrypt the file. P_{uk} will be same for all users but P_{rk} is different for the entire user. Data owner first generate his public key and private key from (1). His public key will be same for entire user. After generation of keys by data owner or client he will encrypt the file F to F′. This F′ is an encrypted file in (2). This encrypt file will reduce the understanding of message for not only unauthorized user but also for TPA. Decryption will also be done at client side .with the help of his private key P_{rk} he will decrypt the file that what shown in (3).

$$Key\_Generation(2^k) \rightarrow (P_{uk}, P_{rk}) \quad (1)$$

$$E(P_{uk}, F) \rightarrow F' \quad (2)$$

Decryption at Client Level

$$D(P_{rk}, F') \rightarrow F \quad (3)$$

2.3 Integrity of data check mechanism

As data owners no longer physically possess the storage of their data, cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the file for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission cost across the network. Also it is not easy to check the data thoroughly and compare with our data. Even the loss of data and recovery of data is also not easy. Considering the large size of the outsourced data and the owner's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. Hence, to fully ensure data security and save data owners' computation resources, we propose to enable publicly auditable cloud storage services, where data owners can resort to an external third party auditor (TPA) to verify the outsourced data when needed. Third party auditing provides a transparent yet cost-effective method for establishing trust between data owner and cloud server. In fact, based on the audit result from a TPA, 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. But it will create a new problem that is data owner and client is totally depending on TPA for security. If data send by the client or data owner are not correct or transmission error or any error then how will found the accountability of data owner or client. To ensure that data reach to a CSP is in correct form and also send by the authenticate user we proposed a new scheme. In this scheme F′ from (2) will be used for message digest M_d in which digital signature of client Φ_c and I i.e. Insert (in case of new file) or U (in case of modification or updating of file) or D (in case of Deletion). This message digest will be made with the help of SHA-512 algorithm. Digital signature will be used as a client's or data owner identity. In case of any failure at client or data owner side digital signature will resolve the problem of accountability. Message Digest will helps in ensuring integrity of data.

After a certain period of time TPA can check the data for integrity and reliability.

$$(F', \Phi_c, IorUorD) \rightarrow M_d \quad (4)$$

$$(F', M_d) \rightarrow T_d \quad (5)$$

From (3) we get message digest M_d. This M_d will be merge with F′ to form T_d i.e. data. This data is send to CSP where first it disintegrate the data from T_d to form F′ and M_d where it SHA-512 algorithm to check F′ with F′ came from Md and also check the identity of the data owner or client. If it find something wrong in file then it will ask the client or data own-

er to send the file again or if it's correct than it update this file according to the instruction is in Message digest i.e. I or U or D as shown in (7).

$$T_d \rightarrow (F', M_d) \quad (6)$$

$$M_d \rightarrow (F', \Phi_c, IorUorD) \quad (7)$$

3 ALGORITHM

It check the integrity of data and also maintaining consistency at cloud data storage for CSP and Client

3.1 For updating records

Client Side	CSP Side
1. Client request to access a file from CSP. $\rightarrow$	2. CSP ask client for authentication just like login page. $\leftarrow$
3. Client authenticates CSP by his password. $\rightarrow$	4. Verify password if correct send a file that he wants to access. Else move to step 2.
5. Client decrypts the file by applying RSA decryption algorithm [12].	
6. If client modify the file he will send file to CSP and TPA with a message like M_d as (F', Φ_c, M) and F' here M denotes for modification, F' for encrypted file, M_d for message digest file [12] and Φ_c for signature. $\rightarrow$	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 and move to step12.
	9. Else ask the client to follow the step 8.
	10. CSP sends a same message $(F', M_d \leftarrow (F', \Phi_s))$ to client after addition of his signature Φ_s. $\leftarrow$
11. If F' file is same as previous one, drop this packet and move to step 1 or step 13.	
12. Else ask CSP to follow step 11 again.	
13. Exit.	

3.2 For insertion of record

The algorithm is for this is similar to updating of record but here after verification of user, the CSP will ask the client for new location of file and clients send the message like (F', Φ_c, I) where I denote insertion of new file.

3.3 For deletion of record

1. Client sends a request to CSP to delete the record.
2. CSP ask client for authentication just like login page.
3. Client send a message like F_n and M_d as (F_n, Φ_c, D) to CSP where D denotes for Deletion and F_n denotes for File name.
4. CSP will delete the file.

From updating of record and insertion of record algorithm, TPA already have encrypted file. So it will check this encrypted file with the encrypted file of CSP. If there is mismatch in file than it send the error report to data owner.

For encryption and Decryption of file we will use RSA algorithm [11, 12].

Table 2: Support of features by existing scheme

	[7]	[8]	[6]	[4]	[9]	Proposed Scheme
Protecting Data Privacy			✓	✓		✓
Dynamic Update		✓	✓			✓
Integrity					✓	✓
Constant Bandwidth Cost	✓	✓	✓	✓	✓	✓

As shown in table 2, this new scheme will provide data privacy to owner or client and any one can update their data dynamically. This scheme solves the problem of integrity. As TPA also checking the data of owner at any time and client can also check his data at the time of submission which will make this scheme as robust in compare to others.

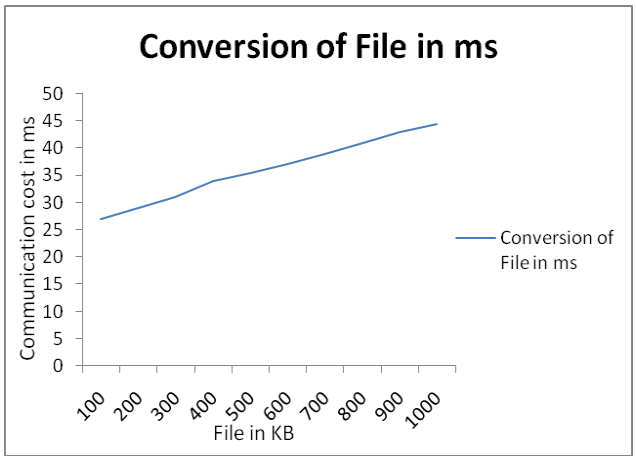
4 SIMULATION AND RESULT

We implemented RSA-based instantiations in Windows 7. Our experiment is conducted using Java on a system with an Intel core i3 processor running at 2.33 GHz, 3GB RAM, and a 7200 RPM Western Digital 320 GB Serial ATA drive with an 8 MB buffer. Algorithms SHA-512 is implemented using CloudSim with Eclipse.

Initially we created one CSP, data owner and TPA. Data owner gave right to change the data to 10 users with keys and identity number. This identity number he sends to CSP and TPA. This user initially generated the file by using algorithm 3.2 then we applied algorithm 3.1 for all 10 user. Now we run algorithm 3.1 step number 7 for TPA. TPA found all 10 files in appropriate form.

To achieve constant bandwidth cost we took a file range from 100 to 1000 KB. All results were obtained after taking of 10 trials. In our observation we find that after getting digital signature of client and encrypted file the message digest takes less time to convert the data as shown in figure 2. The time required to run our scheme can be consider as negligible.After taking negligible time we can enhance the security of data.

Figure 2: Communication cost verses File Conversion



We also find that our scheme detect error probability about 99%.The Data protecting from TPA and CSP is verified by the simulation, as we had converted the file into encrypted form.

5 Conclusion

Cloud Computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware. As market grows the threat on data also grows. To protect the data from unauthorized access and to ensure that our data are intact we proposed a scheme, which solve the problem of integrity, unauthorized access, privacy and consistency. In this article we first present a network in which cloud architecture, users and TPA are shown after that we describe how file is retrieved. We then suggest a scheme for retrieval of file, encryption and decryption of file, how to check the integrity of our data from CSP and how to give control to TPA. Later, we had defined the properties that will be given by our scheme. Further challenging issues for public auditing services that need to be focused on are discussed too. We believe that security in cloud computing is very much needed as data in the cloud storage are not secure and require lots of attention of user.

Acknowledgment

This work was supported in part by Ministry of Human R source Development (MHRD) and the Department of Computer Science and Engineering, N.I.T. Hamirpur (H.P.).

References

[1] Cloud Computing Research, PDS Group, TU Delft http://www.pds.ewi.tudelft.nl/~iosup/research_cloud.html

[2] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li," Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011

[3] Cong Wang and Kui Ren, Wenjing Lou, Jin Li," Toward Publicly Auditable Secure Cloud Data Storage Services" in IEEE Network July/August 2010

[4] G.Ateniese et al., "Provable Data Possession at Untrusted Stores," Proc. ACM CCS '07, Oct. 2007, pp. 598–609.

[5] M. A. Shah et al., "Auditing to keep Online Storage Services Honest," Proc.USENIX HotOS '07, May 2007.

[6] G. Ateniese et al., "Scalable and Efficient Provable Data Possession," Proc. SecureComm '08, Sept. 2008.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Asia- Crypt '08, LNCS, vol. 5350, Dec. 2008, pp. 90–107.

[8] C.Wang et al.,"Ensuring Data Storage Security in Cloud Computing," Proc. IWQoS '09, July 2009, pp. 1–9.

[9] Q. Wang et al., "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS '09, Sept. 2009, pp. 355–70.

[10] Cloud computing making virtual machines cloud ready, www.trendmicro.com/go/enterprise

[11] Xinmiao Zhang, and Keshab K. Parhi, "High-Speed VLSI Architectures for the AES Algorithm" in IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 12, NO. 9, SEPTEMBER 2004.

[12] SECURE HASH STANDARD by Federal Information Processing Standards Publication 180-2 2002 August 1