Global Journal of Computer Science and Technology
Software & Data Engineering
Volume 13 Issue 13 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

TPA Ensuring Data Integrity in Cloud Environment

By Jaspreet Kaur & Jasmeet Singh
Mandi Gobindgarh/ Punjab Techincal University, India

Abstract- Cloud computing is an internet based computing where virtual shared servers provide software, infrastructure, platform and other resources to customers on a pay-as-you-use basis. In one of the services offered by cloud viz. Storage as a Service, users outsource their data to cloud without having direct possession or control on it. Storage of large data in cloud reduces costs and maintenance. But the customer is unaware of the storage location. Here risk involved is modification of data or tampering of data. In this paper we propose a data correctness scheme in which Third Party can audit the data stored in the cloud and assure the customer that the data is safe. Hence we implemented a scheme for verifying integrity of data. Such verification systems prevent the cloud storage archives (storage) from misrepresenting or modifying the data stored by using frequent checks on the storage archives.

Keywords: *audit, cloud, integrity, station to station protocol, SHA-2, third party auditor, XOR.*

GJCST-C Classification : *C.2.1*

Strictly as per the compliance and regulations of:

TPA Ensuring Data Integrity in Cloud Environment

Jaspreet Kaur[α] & Jasmeet Singh[σ]

Abstract- Cloud computing is an internet based computing where virtual shared servers provide software, infrastructure, platform and other resources to customers on a pay-as-you-use basis. In one of the services offered by cloud viz. Storage as a Service, users outsource their data to cloud without having direct possession or control on it. Storage of large data in cloud reduces costs and maintenance. But the customer is unaware of the storage location. Here risk involved is modification of data or tampering of data. In this paper we propose a data correctness scheme in which Third Party can audit the data stored in the cloud and assure the customer that the data is safe. Hence we implemented a scheme for verifying integrity of data. Such verification systems prevent the cloud storage archives (storage) from misrepresenting or modifying the data stored by using frequent checks on the storage archives.

Keywords: audit, cloud, integrity, station to station protocol, SHA-2, third party auditor, XOR.

I. Introduction

Cloud Computing is emerging as the next evolution of computing for its numerous contribution to the IT enterprise. In contrast to traditional solutions, Cloud Computing has a number of essential characteristics, such as: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service.[3]

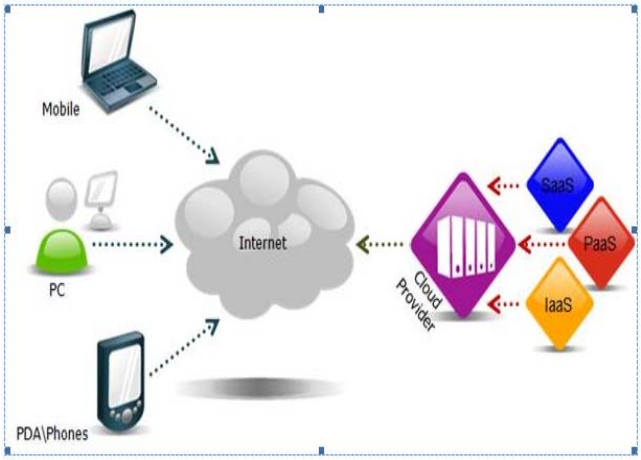

Figure 1 : Cloud Computing

Author α: Jaspreet Kaur Lecturer, Thapar Polytechnic College M.TECH (Computer Science and Engineering) RIMT-IET, Mandi Gobindgarh, Punjab India. e-mail: kkhushi12@yahoo.co.in

Author σ: Jasmeet Singh Asst. Professor(CSE Department) RIMT-IET, Mandi Gobindgarh, Punjab India. e-mail: jasmeetgum@gmail.com

Data outsourcing, one of the fundamental components of Cloud Computing, centralizes users' data to the cloud server (CS). Users including both individuals and enterprises move their data or store their data in cloud storage centers to minimize the costs and enjoy benefits, such as: release the pressure from storage management, universal data access with independent geographical locations.[4]

Despite these distinct advantages outsourcing brings, there are also many security issues.

1. Firstly, although the cloud service provider (CSP) can provide more powerful and reliable infrastructures than users, a huge mass of data storing in the CS makes it more vulnerable to active attack.
2. Secondly, towards the cloud users, the CSP may deliberately distort the status of users' outsourced data for some benefits. For example, the CSP may discard the data that users rarely or never access to save costs, or even hide data loss incidents for the sake of reputation .[4]

So we can see, although data outsourcing can bring advantages and convenience to users, it can not ensure the integrity of data. But integrity monitoring is essential in cloud storage for the same reasons that data integrity is critical for any data center. Data corruption can happen at any level of storage and with any type of media. The truth is that data corruption can happen anywhere within a storage environment. Data can become corrupted simply by migrating it to a different platform, i.e., sending your data to the cloud. Cloud storage systems are still data centers, with hardware and software, and are still vulnerable to data corruption. [13]

Generally speaking, users like to outsource a huge mass of data in the CS, so simply downloading the data to verify the integrity is not a feasible solution. To solve the security problems of data outsourcing mentioned above, researchers proposed auditing protocols to ensure the correctness of the outsourced data. The integrity of data should be guaranteed in a relatively low computation and communication overhead through an efficient auditing protocol.[4]

So he appoints a Third Party Auditor to check the availability of data and its correctness without devotion of their computation resources. [1] TPA checks the correctness of data stored in the cloud and

communicates this with the client. Whenever the client needs the data the cloud returns the data with full guarantee of delivery, availability and correctness. As TPA verifies for its correctness and availability he considers the data is safe.

Figure 2 represents data outsourcing in cloud environment where user delegates task of monitoring integrity to third party auditor(TPA).

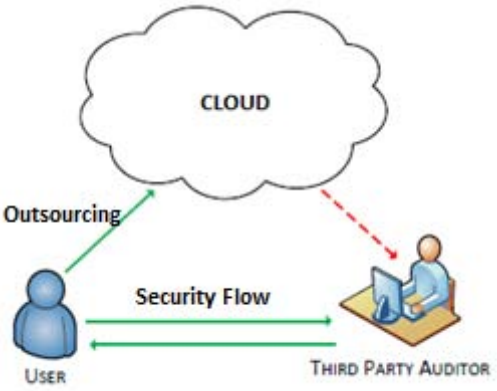

Figure 2 : Data Outsourcing in Cloud

II. Problem Definition

In Cloud Computing, it is difficult to maintain data integrity because the user usually has no control over the security mechanisms that are used to protect his/her data. User cannot trust cloud service provider to handle the data by himself as he himself can modify or delete the original data and integrity may be lost. If any intruder attacks and steals the data and modifies it then in some cases the modification is not even noticed by the cloud server or data loss or corruption is intentionally hidden. So, user can rely on a trusted third party auditor to check for the integrity of his data. To trust third party entity authentication is needed. For auditing (on user's request or at regular intervals), strong and secure cryptographic hash function is required to check for integrity of cloud data and informs the user about data corruptions or loss if any.

III. Methodology

We propose a data correctness scheme which involves verifying integrity of data with the help of third part auditor as shown in figure 3.

For ensuring the integrity of the data we will be using combination of three approaches-

1. Station-to-Station protocol (based on Diffie-Hellman key exchange algorithm) generates mutual key which is known to both user and auditor. It also provides entity authentication to both.
2. Exclusive-OR (XOR) to perform a xor operation between the message and the key generated using Station-to-Station protocol.
3. Secure Hashing Algorithm (SHA-2) to generate a digest by passing the original message to the hash function. This is done by both the user and the auditor and the value obtained from the hash function by both of them is compared and hence the data integrity is verified.

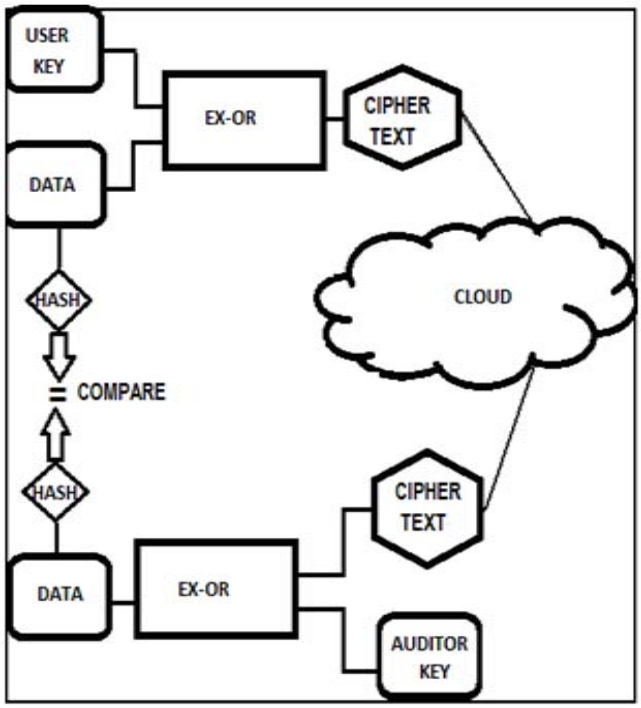

Figure 3 : Methodology

IV. Implementation

Using java netbeans IDE and XAMPP, we have implemented methodology in which TPA ensures integrity of data outsourced by user in the cloud storage and thus reduces overhead of user.

We have created three pages(forms)-

1. client side(figure 4)
2. cloud server (figure 5)
3. auditor side(figure 6)

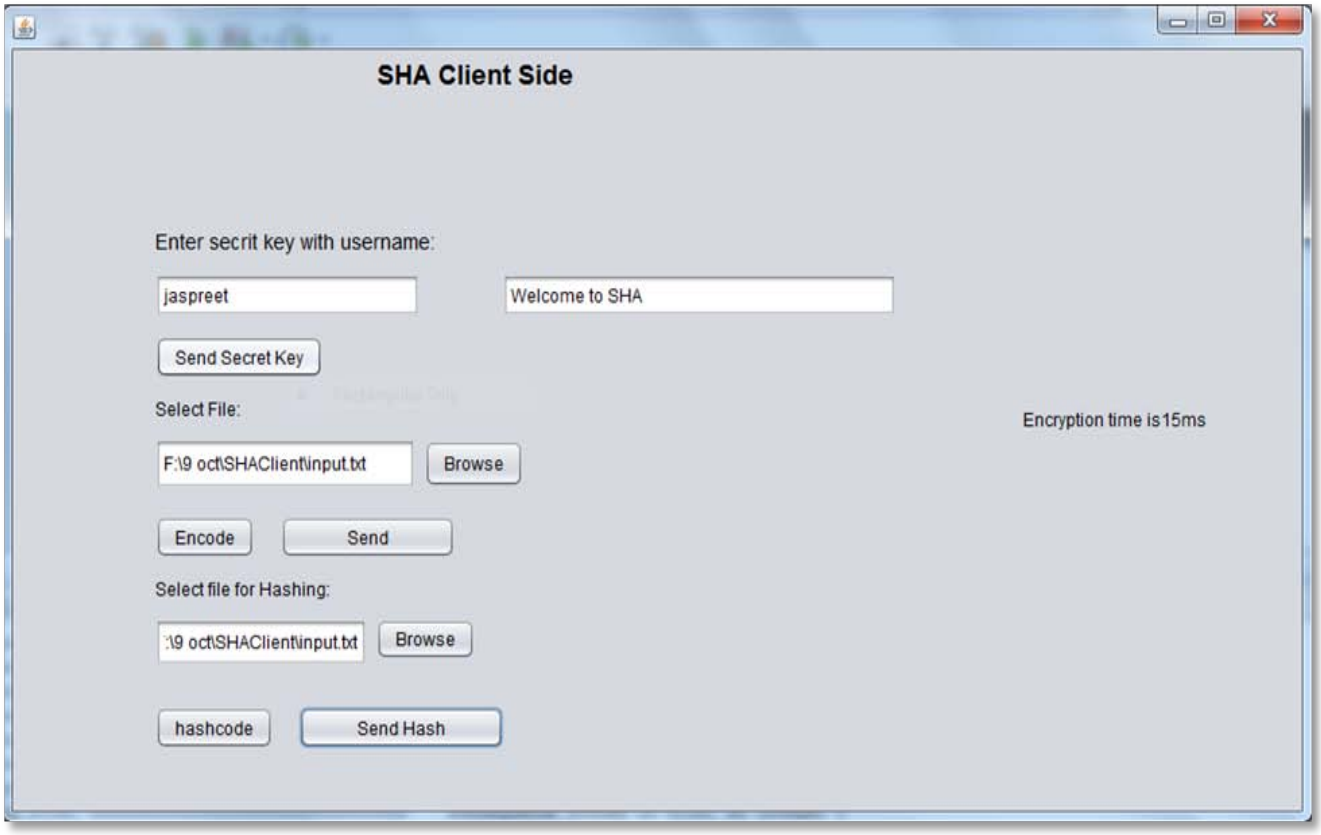

Figure 4 : Client page

Figure 5 : Cloud page

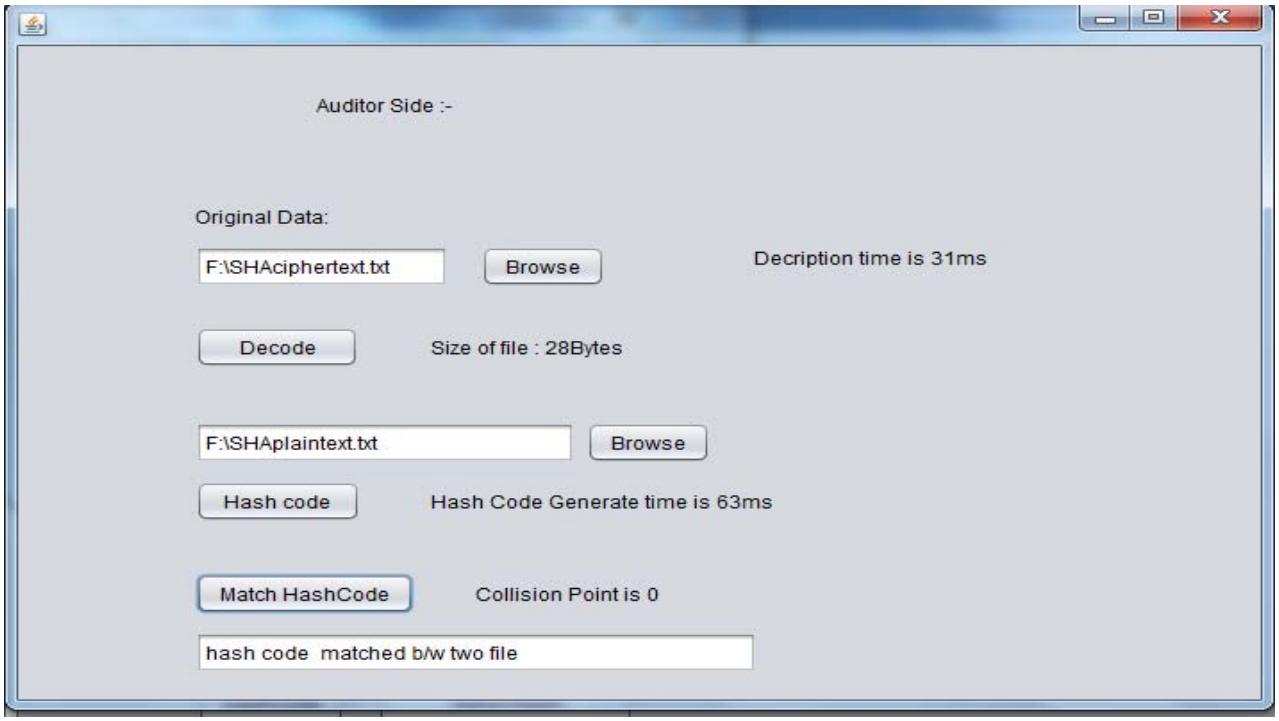

Figure 6 : Auditor Page

The steps of implementation are as follows-

1. A secret key generated using STS protocol (that is known to both user and auditor. Also, mutual authentication is done using this protocol.
2. XOR operation is done between the data and the key generated to create cipher text which is stored in cloud.
3. Separately the data is passed in a hash function (using SHA-2) and the hash value is obtained by the user.
4. Auditor gets the cipher text from the cloud and performs an XOR operation with the secret key generated by the station to station protocol and gets a plain text.
5. Auditor passes this plain text to the same hash function (using SHA2) and obtains a hash value.
6. He then compares this hash value with the hash value received from the user .If both the values are identical then the data integrity is maintained else data is tampered.

V. Results

The results of the above mentioned system are shown in Table 1 and Figure 7.

Table 1 : Result Analysis

	File Size(in Bytes)			
	28	99	124	205
Encryption Time	16	94	141	211
Decryption Time	31	141	187	265
Hash Time	63	78	93	108
Collision Point	0	0	0	0

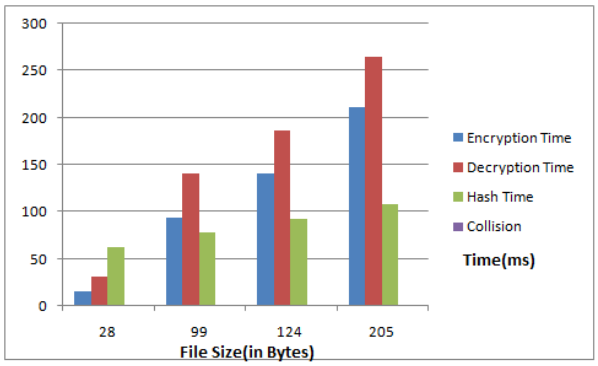

Figure 7 : Graph Showing Results of Encryption, Decryption, Hash Time and Collision

If hash of both files matches, collision point is 0.
If hash of both files do not match , collision point is 1.

VI. Conclusion and Future Work

This paper focuses on auditing mechanisms (using hash function) to ensure data integrity where users can safely delegate the integrity checking tasks to Third Party Auditors and be worry-free to use the cloud storage services. This scheme reduces the computational and storage overhead of the client as well as the computational overhead of the cloud storage server.. We are trying to improve the scheme for auditing multiple files from multiple clients simultaneously as with the increasing development of Cloud Computing technologies, it is believed that more and more users will prefer to store their data in the cloud.

References Références Referencias

1. Malathi, Murugesan, "A Scheme for Checking Data Correctness in the Cloud", International Conference on Information and Network Technology (ICINT 2012).
2. Miss. M.Sowparnika1, Prof. R. Dheenadayalu2, "Improving data integrity on cloud storage services", International Journal of Engineering Science Invention(ISSN), Volume 2, Issue 2 ,February. 2013.
3. N.Madhuri, T.V.Suneetha, A.Haritha, P.V.S.Lakshmi, "A Protocol for Ensuring Data Integrity in Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.
4. XU Chun-xiang, HE Xiao-hu, Daniel Abraha, "Cryptanalysis of auditing protocol proposed by Wang et al. for data storage security in Cloud Computing", School of Computer Science and Engineering, University of Electronics Science and Technology of China, 2006.
5. K.Govinda, E.Sathiyamoorthy, "Data Auditing in Cloud Environment using Message Authentication Code", International Conference on Emerging Trends on Advanced Engineering Research (ICETT), 2012.
6. K.Govinda, V.Gurunathprasad, H.Sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud through Digital Signature using RSA", International Journal of Advanced Scientific and Technical Research, Vol. 4, Issue 2, August 2012.
7. Abhishek Mohta, Lalit Kumar Awasthi, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific and Engineering Research, Vol. 3, Issue 6, June-2012.
8. Akkala Saibabu, T.Satyanarayana Murthy, "Security Provision in Publicly Auditable Secure Cloud Data Storage Services using SHA-1 Algorithm", International Journal of Computer Science and Information Technologies (IJCSIT) Vol. 3(3), 2012.
9. Reenu Sara Georeg, Sabitha S," Survey on Data Integrity in Cloud Computing", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 2, Issue 1, January 2013.
10. Hiren Patel and Dhiren Patel,"Achieving Secure Cloud Data Storage without using a Trusted Third Party Auditor- A Review", International Journal of Computer Applications,Nov.2012.
11. S.Jeyadevan, Dr.S.Basavarij Patel, "A DATA INTEGRITY VERIFICATION IN CLOUD COMPUTING", International Conference on Computing and Control Engineering(ICCCE 2012),12 & 13 April,2012.
12. [7]Dalia Attas, Omar Batrafi," Efficient integrity checking technique for securing client data in cloud computing", International Journal of Electrical & Computer Sciences (IJECS-IJENS), Vol: 11, No: 05.
13. http://www.wwpi.com/index.php?option=com_content&id=12800:data-integrity-in-the-cloud&Itemid=2701018
14. http://en.wikipedia.org/wiki/Cloud_computing.

This page is intentionally left blank