Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Ensuring Data Storage Security in Cloud Using Two Way Integrity Check Algorithm

Garima
Department of Computer Science,
BPIT, GGSIPU, India

Abstract— In this paper, a new scheme has been introduced, "Two Way Integrity Algorithm". The paper presents a way to implement Third Party Auditor (TPA) which not only checks the reliability of Cloud Service Provider (CSP) but also checks the consistency and accountability of data. This paper addresses this challenging open issue of integrity, confidentiality and authentication of data. It provides an efficient data integrity mechanism between the client and the cloud service provider by applying RSA with digital signature on the message digest instead of on the whole data to make the computations faster. It then uses TPA for auditing the data stored in the cloud and finally provides an algorithm to check data integrity between the client and the TPA.

Keywords— Two Way Integrity Check Algorithm, Cloud Service Provider, Third Party Auditor, Message Digest, Message Authentication Code.

I. 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. 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].

II. PROPOSED SCHEME

In our scheme , The client asks the CSP to provide service where CSP authenticate the client. RSA with Digital signature part will be done by the user to provide data authentication, data integrity and non-repudiation. This is done by first encrypting the user's data using symmetric encryption. The secret key involved is also encrypted using RSA algorithm (by receiver's public key).Then the message digest is created using MD5 algorithm and then the message is signed. After that the message and the signature is sent to the cloud service provider. Thereafter the CSP uses the receiver's private key to retrieve the digest. CSP uses the receiver's private key on the signature to retrieve the digest D' and then it applies the hash algorithm on the encrypted data to get the digest D. CSP now compares the two digests. If they are equal the message is accepted otherwise it informs the user that the data has been intrude. Digital signature will be used as a client's or data owner's identity and message digest helps in ensuring integrity of the data[1]. To enable cloud data storage security under the aforementioned model, our protocol design should achieve the following security and performance guarantee:

1. Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users[2].
2. Storage correctness: to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact.
3. Privacy-preserving: to ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process;

Our scheme consist of 3 parts :

1. RSA with Digital signature part will be done by the user.

2. The CS verifies over the user data in the cloud to check over the manipulation or intrusions in the cloud data
3. The TPA verifies over the cloud server part to check if the cloud server was manipulating in the user data or not.

Now, the each entity function in the proposed model is mentioned below:
1. User: User first uses RSA scheme to construct the public and the private keys then he\she will sign the data using the private key to form the digital signature to be uploaded to the cloud. After that the user sends the digital signature and the data to the cloud server and deletes its local copy.
2- CS: CS will compute a hash value from the original data to send it to the TPA, and then takes this hash value along with the data signed in the cloud for verification using the public key. At the end, the CS will inform the user if the data in the cloud intruded or not.
3- TPA: After the cloud server finishes its role, the TPA will be initiated to verify over the cloud server work by taking the hash value from the cloud server. TPA will take the data signed from the cloud and decrypt it with the public key. The decryption will result a hash value that will be compared along with the hash value that the cloud server compute it in his part. After finishing the verification, the TPA will inform the user if the CS was trusted or not.

III. TWO WAY INTEGRITY CHECK ALGORITHM

Our proposed algorithm consists of two algorithms:

A. Integrity Check Mechanism Between Client and CSP

The steps are:

1. The sender first encrypts the data using symmetric encryption using a shared key.
2. The shared key is also encrypted using RSA algorithm (Receiver's public key).
3. Then the message digest is created using md5 algorithm , D=h(M').
4. Then the message is signed , S=D^d mod n.
5. Then the encrypted message and signature is sent to the cloud service provider.
6. Then CSP uses the receiver's private key on the signature to retrieve the digest, D'=S^e modn.
7. Then it applies the hash algorithm on the encrypted data to get the digest D.
8. CSP now compares the 2 digests D and D'. If they are equal, the message is accepted, otherwise it informs the user that the data in the cloud is intruded.

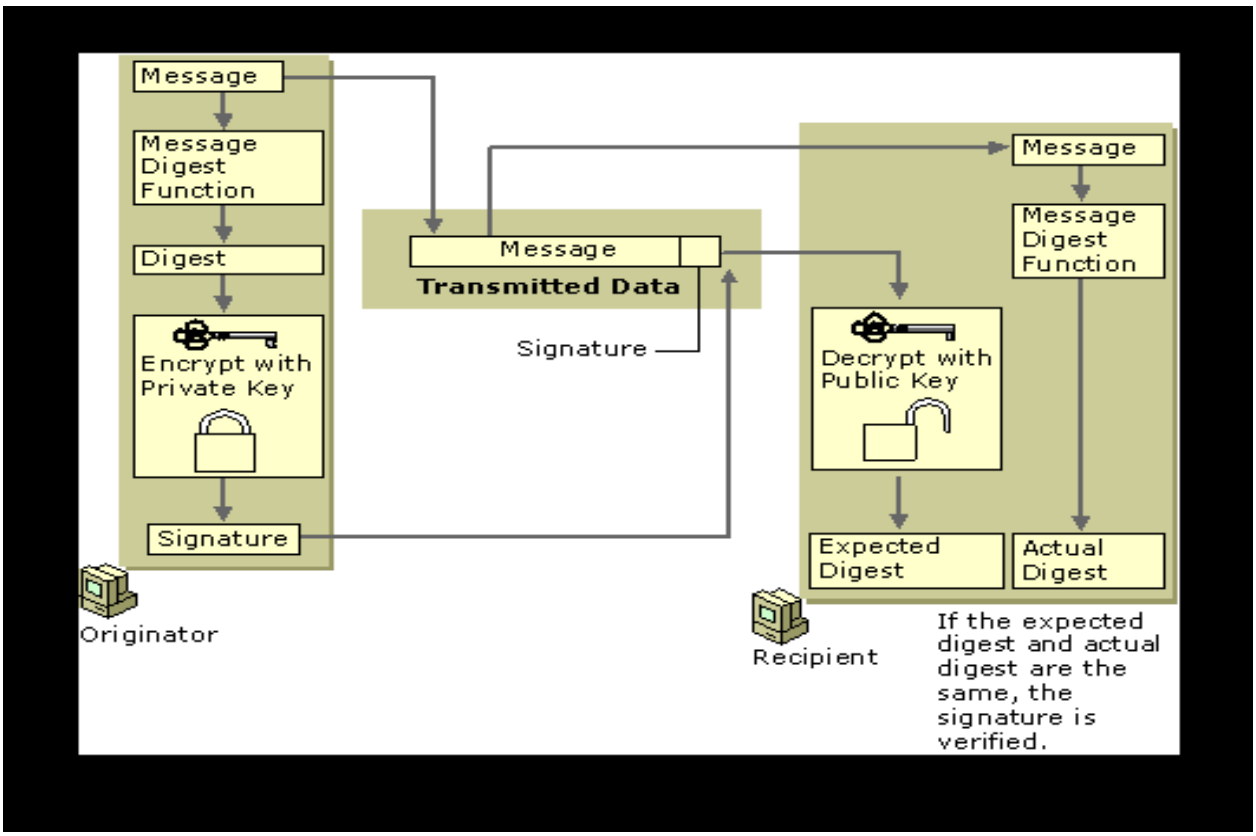

Fig. 1. Integrity check mechanism between client and CSP

B. Integrity Check Mechanism Between Client and Third Party Auditor

The steps are:

1. After the CSP finishes its role, the TPA will be initiated to verify over the cloud server work by taking the hash value(digest) from the CSP (i.e D).
   TPA will take the data signed from the cloud and decrypt it with the public key and finds the Message digest.

2. The decryption will result a hash value that will be compared along with the hash value that the cloud server compute it in his part. After finishing the verification, the TPA will inform the user if the CSP was trusted or not.
3 If D(computed by CSP)=D''(computed by TPA) then it means that the CSP is reliable and the data is secured

IV. MATHEMATICAL MODELING

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof).
KeyGen is a key generation algorithm that is run by the user to setup the scheme.
SigGen is used by the user to generate verification metadata, which may consist of MAC, signatures, or other related

information that will be used for auditing.
GenProof is run by the cloud server to generate a proof of data storage correctness.
VerifyProof is run by the TPA to audit the proof from the cloud server.[3]

Our public auditing system can be constructed from the above auditing scheme in two phases, Setup and Audit:

A. Setup-Phase:

The user initializes the public and secret parameters of the system by executing KeyGen, and preprocesses the data file *F* by using SigGen to generate the verification metadata. The user then stores the data file *F* at the cloud server, deletes its local copy, and publishes the verification metadata to TPA for later audit. As part of pre-processing, the user may alter the data file *F* by expanding it or including additional metadata to be stored at server. The cloud user runs KeyGen to generate the system's public and secret parameters.

1. KeyGen
   RSA : Firstly, we describe the parameters involved in a standard RSA signature scheme.
   Each sender has a public key $pk = (e,n)$ and private key $= (d, n)$ where n is a k -bit modulus generated as the product of two random $k / 2$ –bit primes p and q and n= p*q where, p,q ∈ discrete prime numbers.
   $e,d \in Z^*$ and satisfying : $ed \equiv 1 \bmod \varphi(n)$ where $\varphi(n) = (p-1)(q-1)$.
   The security of the RSA cryptosystem is believed to be based on the intractability of the integer factorization problem.
   $H(\cdot)$, $h(\cdot)$: map-to-point hash functions, defined as: $\{0,1\}^* \rightarrow G$, where G is a group.
   $E(K,\cdot)$: An encryption function, with K as the encryption key. $E : \{0,1\}K \times \{0,1\}^* \rightarrow \{0,1\}^*$
2. SigGen :
   First of all, the message digest is formed using the SHA-512 algorithm.
   D = H(M), Where M is the user's message , H() is the applied hash algorithm SHA-512 and D is the message Digest involved. Then, the digital signature is obtained by encrypting the message digest using the private key (d,n).
   INPUT : Private Key (d ; n) for the sender, Public key (e; n) for the receiver , and message to be signed, M.
   OUTPUT: S, signature of M
   1) D = h(M) ;
   2) S =D^d mod n;
   3) Return (s)

B. Audit-Phase:

It consists of GenProof and VerifyProof.

1. GenProf:
   The server runs GenProof to generate a response proof of data storage correctness.
   INPUT: public key of sender(e,n),message M, Signature S
   OUTPUT: D,D'.
   D'=S^e mod(n)
   D=h(M)
   IF D=D' the received data is correct else it informs user that the data is intruded.
2. VerifyProof:
   With the response from the server, the TPA runs VerifyProof to validate the response
   Run by TPA to check whether the CSP is reliable or not.
   INPUT: Signature S, public key of sender(e,n)
   OUTPUT:
   D''=S^e mod(n);
   D=h(M) (from the CSP)
   If D=D'' the CSP is reliable else it is not reliable.

The decryption will result a hash value that will be compared along with the hash value that the cloud server compute it in his part. After finishing the verification, the TPA will inform the user if the CS was trusted or not.

V. CONCLUSION AND FUTURE WORK

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.[12] 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 paper, first a system showing cloud architecture, users and TPA and how TPA helps in interacting with the cloud service provider on behalf of the client in order to check the data security at the cloud and the reliability of the server is presented[13]. Then, an efficient scheme for checking the data integrity between the client and the server is introduced. Also an algorithm is proposed to check for the reliability of the CSP i.e a mechanism checking data integrity between the client and the TPA. Later we had defined the algorithms and the model given by our scheme. 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. Further the proposed algorithm was implemented and the performance was evaluated. The future work includes the implementation of the algorithm that includes data integrity check mechanism between the third party auditor and the cloud service provider. This algorithm will further help in detecting the leakage of data or intrusions done by the cloud service provider itself.

REFERENCES

[1] Abhishek Mohta ,Ravi Kant Sahu, Lalit Kumar Awasthi , " Robust Data Security for Cloud while using Third Party Auditor," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 2, February 2012**.**

[2] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou ," Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE TRANSACTIONS ON COMPUTERS.

[3] Bo Chen, Reza Curtmola ," Robust Dynamic Provable Data Possession,"in 32nd International Conference on Distributed Computing Systems Workshops, 2012.

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

[5] Shucheng Yu, Cong Wang, Kui Ren , and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," presented as part of the main Technical Program at IEEE INFOCOM 2010.

[6] M.Sudha , M.Monica," Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography,"presented at Advances in Computer Science and its Applications, Vol. 1, No. 1, March 2012.

[7**]** Cong Wang and Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services,"presented at IEEE Network ,July/August 2010.

[8] M. Sudha Dr.Bandaru Rama Krishna Rao,M. Monica," A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment," International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[9] Akhil Behl," Emerging Security Challenges in Cloud Computing,"presented at World Congress on Information and Communication Technologies,2011.

[10] Wang Junxiang, Liu Shengli," Dynamic Provable Data Possession with Batch-Update Verifiability,".

[11] Sandeep K. Sood "A combined approach to ensure data security in cloud computing "in Journal of Network and Computer Applications , ELSEVIER, 3 July 2012.

[12] Kan Yang · Xiaohua Jia "Data storage auditing service in cloud computing: challenges, methods and opportunities" in Springer Science+Business Media, LLC 2011.

[13] S. Subashini , V.Kavitha "A survey on security issues in service delivery models of cloud computing" , in Journal of Network and Computer Applications , ELSEVIER, 11 July 2010.

[14] C.Wang, Q.Wang, K. Ren, andW. Lou,"Ensuring data storage security in cloudcomputing," in Proc. of IWQoS'09, July2009.

[15] G.Ateniese et al. ,"Provable Data Possession at Untrusted Stores,"‖ Proc. ACM CCS, Oct. 2007.

