International Journal of Engineering Research & Management Technology ISSN: 2348-4039
January-2016 Volume 3, Issue-1
Email: editor@ijermt.org www.ijermt.org

Data Security in Cloud Computing with Third Party Auditor

Mansi Lamba, Poornima Kapoor
Department of Information Technology
SRM University
Delhi- NCR Campus
Ghaziabad

Rahul Punyani
Department of Computer Science & Engineering
SRM University
Delhi- NCR Campus
Ghaziabad

ABSTRACT:
The practice of using a network of remote servers hosted only on the internet to store, manage, and process data, rather than a local server or a personal computer is known as Cloud Computing. Security is thus a top level concern while dealing with cloud computing, majorly due to its dynamic resources and flexible nature. In order to ensure its security, that is maintaining data integrity at every level, third party auditors (TPA) are used. This paper briefly outlines a Third Party Auditing service in which a third party entity ensures a reliable connection between Cloud Service Provider and Client. However, a highly distributed and non-transparent cloud service may hinder the auditing process. Our objective revolves around surpassing these issues and presenting a mechanism to audit cloud platform and maintain integrity in order to ensure users' data safety and satisfaction.

KEYWORDS: Third Party Auditor (TPA), Cloud Service Provider (CSP), Advance Encryption Technique, Data Integrity, Digital Signature Algorithm (DSA)

1. INTRODUCTION:

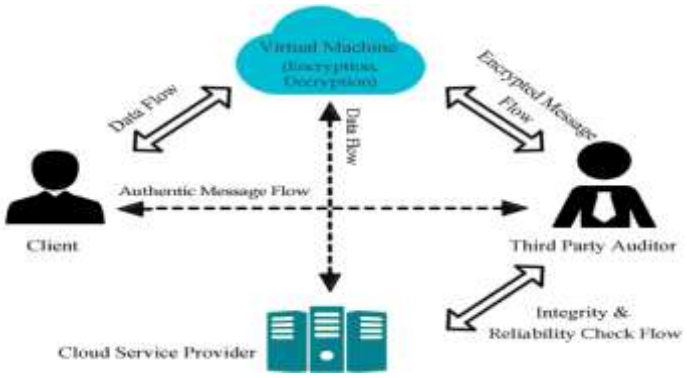
The fact that essentiality of assuring data integrity is a mandatory aspect of Cloud Computing it requires the CSP to take all actions in approach to maintain the same. A Third Party Auditing Service is in the form of extra hardware or cryptographic coprocessor. TPA eliminates need for local data storage, maintenance and security. TPA keeps a check for integrity of data on cloud on behalf of a user. It validates data and ensures nonrepudiation i.e. in a communication one cannot deny the authenticity of sending a message that they originated. TPA has two categories namely Private Auditability which can achieve higher scheme efficiency and Public Auditability which allows anyone (including and other than the data owner) to challenge the cloud for correctness of data. One problem, however, remains unsolved: TPA can modify or delete crucial data. TPA may become intrusive and pass important information to an abuser.

2. TPA SECURITY SCHEME:

2.1 CLOUD MODEL:

Whenever a client requests CSP to provide a service it authenticates user and provides a Virtual Machine by means of Software as a Service. Point to Point Communication channels are established between each cloud server and the user. Virtual Machine uses algorithms for encryption and decryption of files while a Third Party Auditor maintains integrity and reliability and checks flow of data.

Fig. 1 Architecture of a Cloud System with TPA



2.2 ADVANCED ENCRYPTION TECHNIQUES:

Cloud Service Providers strive to provide better service and performance to their client. Unfortunately, like TPA CSP may also leak information or tend to modify it. Thus there is a requirement for cryptographic approach at user level. Every user has two types of keys- one of which is only know to user himself called Private Key and the other known to anyone called a Public Key. These pair of keys is used for encoding and decipherment using algorithms (in this case we have used modified RSA with Digital Signature Algorithm).

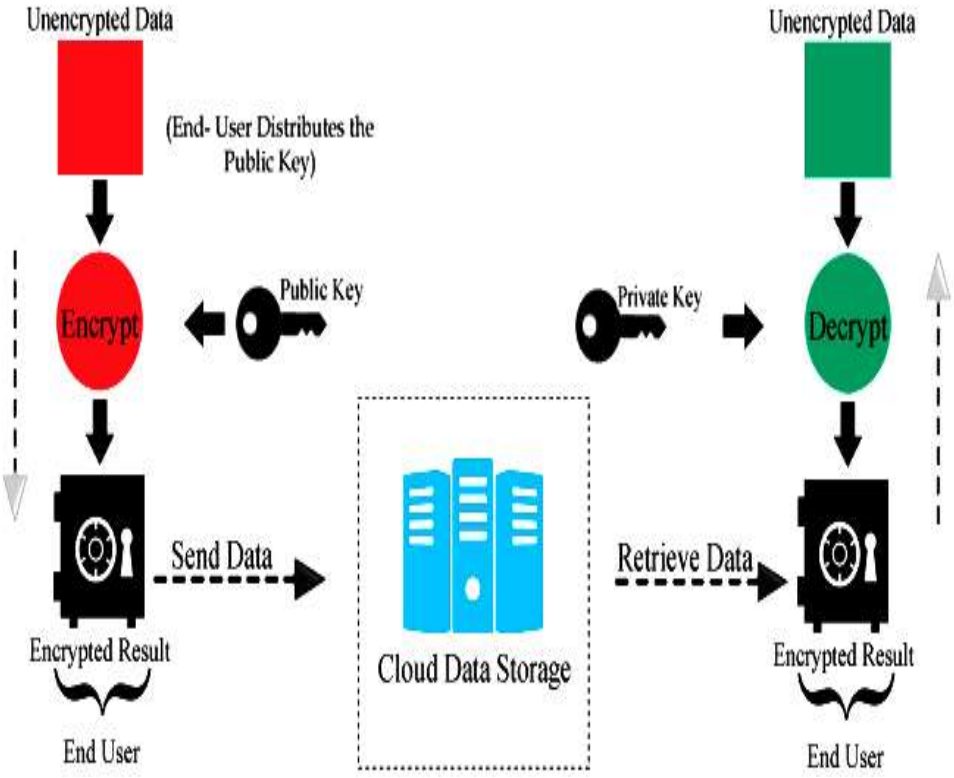


Fig. 2 Public- Private Key Cryptography

3. ALGORITHM:

3.1 RECORD UPDATION:

Step 1: Client requests CSP to access a file.
Step 2: CSP asks client to provide Login ID and Password for authentication purpose.
Step 3: Client provides his credentials to the CSP via a secured gateway.
Step 4: CSP validates the password

IF correct
User is provided access as requested.
ELSE
Move to Step 2.
Step 5: Client side decryption of file is done using RSA Algorithm.
Step 6: Client makes changes to the file and sends it to TPA and CSP with a message as follows-
M_m as (E' ¥ M) and E'
Here, E'= Encrypted File ¥= Digital Signature M= Modification
Step 7: CSP checks the signature for authenticity
IF correct
CSP compares both the file versions
IF similar
CSP drops the packet and moves to Step 2.
ELSE
CSP replaces the file in its records and moves to Step 8.
ELSE
Move to Step 9.
Step 8: CSP sends the same message (E', M_m) to client and TPA after replacing the file.
Step 9: EXIT

3.2 RSA ALGORITHM:

RSA is a public key algorithm which shows that it is easy to compute the product of two large prime nos. but extremely difficult to factor the product into its original primes. RSA generates public and private keys- each as a pair of values.
A Public Key is denoted as $P_k(e,n)$ and Private Key as $Pr_k(d,n)$ which are obtained as follows:
Step 1: Choose two large prime nos. p & q
Suppose p=3 and q=11
Step 2: Find the product n=p*q
n= 3*11
n= 33
Step 3: Compute z= (p-1)*(q-1) where z is co-prime to n
z= (3-1)*(11-1)
z= 2*10
z= 20
Step 4: Discard variables p &q
Step 5: Select a variable e such that 1<e<z where e is also co-prime to n
Suppose e=7
Step 6: Choose a prime variable d such that (d*e) mod z=1
(d*7) mod 20=1
If suppose we put d=3
(3*7) mod 20=1 which is true
Thus, Public Key is denoted as $P_k(7,33)$ and Private Key as $Pr_k(3,33)$
Message m can be encrypted as $c=m^e \bmod n$ where c is the encrypted message.
Let m=2
$c=2^7 \bmod 33$
c=29
Message c can be decrypted as $m=c^d \bmod n$ where m is the decrypted message.
$m=29^3 \bmod 33$
m=2

3.3 DIGITAL SIGNATURE ALGORITHM:

Step 1: Choose public parameters (p,q,g) that may be shared between different users of the system.
Say, q=71 (a prime number)
Select p such that (p-1) must be a multiple of q.
So, let p=18*71+1
p= 1279 (another prime number)
Compute $g=h^{(p-1)}/q \bmod p$. Here, h=3 (1<h<p-1)
$g= 3^{18} \bmod 1279$
g=1157

Step 2: Choose Private Key X randomly where 0<X<q
Suppose X=15

Step 3: Public Key Y is calculated as $g^X \bmod p$
$Y= 1157^{15} \bmod 1279$
Y= 851

Thus, X=15 and Y=851

Step 4: Generate a random value k where 0<k<q
Suppose k=10

Step 5: Calculate $r= (g^k \bmod p) \pmod q$
$r= (1157^{10} \bmod 1279) \pmod{71}$
r=32

Step 6: Calculate $s= k^{-1} (M+X.r) \bmod q$
$s=10^{-1} (123 + 15*32) \bmod 71$
$s= (123 + 15*32)*64 \bmod 71$
$s= 38592 \bmod 71$
s=39

(The modular inverse $10^{-1} \bmod 71=64$ is calculated using Fermat's Little Theorem.)

In the unlikely case when either r or s or both are equal to 0, start again with a different k.
For message m=123 the pair (r,s)= (32,39) is the obtained signature.

VERIFICATION OF DSA:

If 0<r<q or 0<s<q is not satisfied signature is rejected.

Calculate $w=s^{-1} \bmod q$
$w=39^{-1} \bmod 71$
w=51

Calculate $u_1=m.w \bmod q$
$u_1=123*51 \bmod 71$
$u_1=25$

Calculate $u_2= r.w \bmod q$
$u_2= 32*51 \bmod 71$
$u_2=70$

Calculate $v= (g^{u1} y^{u2} \bmod p) \bmod q$
$v= (1157^{25} * 851^{70} \bmod 1279) \bmod 71$
$v= 316 \bmod 71$
v= 32

Thus, the signature is valid unless v=r.

4. CONCLUSION:

Cloud Computing has emerged as the new paradigm of computing. Number of cloud users and cloud service providers are growing rapidly. Stated thus, the need to provide security and resolve integrity issues. A Third Party Auditor is necessary to ensure a reliable connection between a CSP and user. Data integrity verification by a third party is a major advantage of the proposed system. The paper also solves the dilemma of intrusion presented with a TPA via the use of Advance Encryption Techniques to secure users' data

5. REFERENCES:

1. Bhavna Makhija, Vinit Kumar Gupta, Indrajit Rajput, "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.
2. Prabodh S. Nimat, Prof. A. R. Itkikar, "Efficient Data Sharing in Cloud with Third Party Auditor: A Review Study", Journal of Engineering, Computers & Applied Sciences, Volume 2, No. 6, May 2013.
3. Ashish Bhagat, Ravi Kant Sahu, "Cloud Data Security while using Third Party Auditor", International Journal of Computer Applications, Volume 70, No. 16, May 2013.
4. Poornima Kapoor, Bhavya Goel, Maitraiye Saxena, "Security in Cloud Computing", SRM International Journal of Engineering & Sciences, Volume 2, Issue 1, September 2014.
5. R. K. Ramesh, P. Vinoth Kumar, R. Jegadeesan, "N^{th} Third Party Auditing for Data Integrity in Cloud", Asia Pacific Journal of Research, Volume 1, Issue 12, January 2014.
6. Laurasa, "Information Security- Digital Signature ElGamal and DSS- Algorithm and Examples", in MSDN Blogs, October 2012.
7. K. Govinda, V. Gurunathaprasad, H. Sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud through Digital Signature using RSA", International Journal of Advanced Scientific and Technical Research, Volume 4, Issue 2, August 2012.
8. Ashish Bhagat, Ravi Kant Sahu, "Using Third Party Auditor for Cloud Data Security: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.