ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification

Anila Ashrafiwala[1], A.V Patil[2]

P.G. Student, Department of Computer Science and Engineering, Mathoshri Pratishthan Group of Institutions, Khupsarwadi, Nanded, Maharashtra, India[1]

Associate Professor, Department of Computer Science and Engineering, Mathoshri Pratishthan Group of Institutions, Khupsarwadi, Nanded, Maharashtra, India[2]

ABSTRACT: Cloud computing is evolving and considered next generation architecture for computing. Typically cloud computing is a combination of computing recourses accessible via internet. Historically the client or organizations store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data.However in cloud computing, since the data is stored anywhere across the globe, the client organizations have less control over the stored data. To build the trust for the growth of cloud computing the cloud providers must protect the user's data from unauthorized access and disclosure. To achieve data security over cloud computing, one technique could be encrypting the data on client side before storing it in cloud storage. In addition to that could be computing hash of data and verifying integrity of data by same cloud storage provider or other trusted third party. The main purpose of this project is, to achieve data security in terms of data correctness through remote auditing mechanism.This project proposes a solution in order to eliminate or reduce data integrity problems. The solution proposed is to provide data auditing with privacy preserving. System is implemented using two levels of security (RSA and AES Encryption) technique and integrated with Message Digest Authentication. This technique is applied to the cloud to ensure data correctness.

KEYWORDS:Cloud Computing, confidentiality, integrity, Cloud storage, privacy preserving, authenticator regeneration

I.INTRODUCTION

Cloud computing, also known as 'on-demand computing', is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. Cloud,which is the best thing in the new world. If you are on correct cloud with right services and using it in right manner then you are definitely on cloud 9 and you can take the best shower of technology anytime, be anywhere; otherwise it is a nightmare. Cloud computing is also called distributed computing over the network i.e. the ability to execute an application or a program on many computers at the same time.

Cloud computing has emerged as a long-dreamt vision of the utility computing paradigm that provides reliable and resilient infrastructure for users to remotely store data and use on-demand applications and services. Currently, many individuals and organizations mitigate the burden of local data storage and reduce the maintenance cost by outsourcing data to the cloud. However, the outsourced data is not always trustworthy due to the loss of physical control and possession over the data.

As a result, many scholars have concentrated on relieving the security threats of the outsourced data by designing the Remote Data Auditing technique as a new concept to enable public auditability for the stored data in the cloud. The Auditing is a useful technique to check the reliability and integrity of data outsourced to single or distributed servers.

DOI: 10.15680/IJIRCCE.2018.0603020

II. RELATED WORK

Authors wanted to show that is criticism about privacy in cloud model, because of the fact that administrator have access to data stored in the cloud. They can unintentionally or intentionally access the client data. Traditional security or protection techniques need reconsideration for cloud. Except for private cloud where organization does not have control over the equipment, the progress of cloud is seems little slow, because organizations think instead of compromising on the security of the data, they are still willing to invest in buying private equipment to setup their own infrastructure. Security issues which are of concern to the client can be classified into sensitive data access, data segregation, bug exploitation, recovery, accountability, malicious insiders, and account control issues. Like different disease have different medicines, different cloud security issues have different solutions, like cryptography, use of more than one cloud provider, strong service level agreement between client and cloud service provider. Heavy investment is needed to secure the compromising data in cloud.Following are some of the concerns

A.System Complexity

Compared to traditional data center the cloud architecture is much more complex. Therefore while considering security, security of all these components and interaction of these components with each other needs to be addressed.

B. Shared Multi-tenant Environment

Since the cloud needs to provide service to millions of client, a logical separation of data is done at different level of the application stack . Because of which attacker in the face client can exploit the bugs gaining access to data from other organizations.

C. Internet-facing Services

The cloud service which is accessed over the internet via browser, the quality of service delivered on the network is another concern.

D. Loss of control

As the data of client is stored anywhere across the world control loss over physical, Logical of system, and alternative control to client's assets, mismanagement of assets Are some additional concerns.

In proposed system mechanism,authors shows the original user acts as the group manager, who is able to revoke users from the group when it is necessary. In the proposed design, a hash service data integrity verification, encryption/decryption service, and provision for defining list of people which can access data securely is provided, which is separate from the storage cloud provider.Data owner registers himself as data owner in proposed system. He is responsible for uploading the data for customers. But before uploading contents, encryption will take place at owner side and then will go to cloud server. So it achieves higher security and minimizes transmission security concerns.

Other entity is responsible for key distribution, named KDC .There can be multiple KDCs, which might be scattered. For example, these may be servers in several components of the globe. A data owner on presenting registered id to KDCs receives keys for encryption/decryption .The ciphertext C is distributed to the cloud. Cloud stores the ciphertext C. The auditor is responsible for audit the data which is stored in the cloud. Auditing the data is very useful while we fetch our data from the cloud. Once a reader wants to read, the cloud sends C. If the user's id is in Permitted list under specific data owner KDC will give him/her keys, it will decipher and acquire back original message.

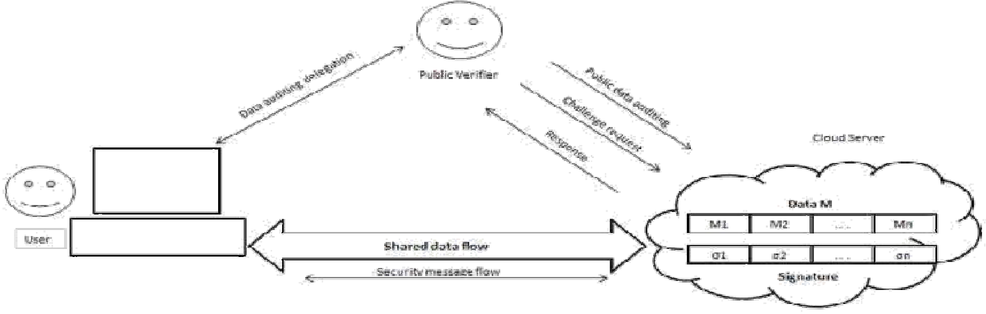

FIGURE: WORKFLOW OF PROPOSED SYSTEM

III. PROPOSED ALGORITHM

A. Description of the RSA Algorithm:

Aim of the proposed algorithm is to maximize integrity. The security of RSA is derived from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplication of these two numbers is easy, but determining the original prime numbers from the total factoring is considered infeasible due to the time it would take even using today's super computers. The proposed algorithm comprises of 3 steps:

Step1: Consider "A" generatesRSA keys by selecting two primes: p=11 and q=13. The modulus n=p×q=143. The totient of n $\phi(n)=(p-1)x(q-1)=120$. Thus "A" chooses 7 for RSA public key e and calculates RSA private key using the Extended Euclidean Algorithm which gives 103.

Step2:Consider "B" wants to send "A" an encrypted message M so "B" obtains "A" RSA public key (n,e) which in this example is (143, 7). The plaintext message is just the number 9 and is encrypted into ciphertext C as follows:

$M^e \bmod n = 9^7 \bmod 143 = 48 = C$

Step 3: When "A" receives "B" message , "A" decrypts it by using RSA private key (d, n) as follows:

$$C^d \bmod n = 48^{103} \bmod 143 = 9 = M$$

To use RSA keys to digitally sign a message, "A" would create a hash or message digest of their message to "B", encrypt the hash value with RSA private key and add it to the message. "B" can then verify that the message has been sent by "A" and has not been altered by decrypting the hash value with public key. If this value matches the hash of the original message, then only "A" could have sent it (authentication and non-repudiation) and the message is exactly as "A" wrote it (integrity). "A" could, of course, encrypt message with "B" RSA public key (confidentiality) before sending it to "B". A digital certificate contains information that identifies the certificate's owner and also contains the owner's public key. Certificates are signed by the certificate authority that issues them, and can simplify the process of obtaining public keys and verifying the owner.

IV.PSEUDO CODE

A. Key Generation Algorithm

```
1. Choose two very large random prime integers:p and q
2. Compute n and $\varphi(n)$:$n = pq$ and $\varphi(n) = (p-1)(q-1)$
3. Choose an integer e, $1 < e < \varphi(n)$ such that:$gcd(e, \varphi(n)) = 1$(where gcd means greatest common denominator)
4. Compute d, $1 < d < \varphi(n)$ such that:$ed \equiv 1 \pmod{\varphi(n)}$
```

- the public key is (n, e) and the private key is (n, d)
- the values of p, q and $\varphi(n)$ are private
- e is the public or encryption exponent
- d is the private or decryption exponent

DOI: 10.15680/IJIRCCE.2018.0603020

B. Encryption

The cipher text C is found by the equation 'C = M^{e} mod n' where M is the original message.

C. Decryption

The message M can be found form the cyphertext C by the equation 'M = C^{d} mod n'.

V. SIMULATION RESULTS

In this section we explain about the algorithm time complexity with the proposed result.

A. Simulation Environment

Three major components of the RSA algorithm are exponentiation, inversion and modular operation. Time complexity of the algorithm heavily depends on the complexity of the sub modules used. We can take the liberty to perform modular addition in cryptography in *O(log n)*where *n* is the number of digits in any number in Z. Now modular multiplication using squaring and multiply technique to get m^emod N can be shown as multiplying the digits of m log e times. Considering the complexity of multiplication $O(\{log\ n\}^2)$ i.e. repeated addition of two number of logn bits each, the complexity of the modular exponentiation is about $O(\{logn\}^3)$Using Euclidean extended GCD from, inverse of a number can be calculated in $O(\{log\ n\}^2)$.Thus overall time complexity of the key generation algorithm will be $O(N^2)$ encryption and decryption algorithm using squaring and multiply technique will be O(N^3):For N digit number space.

Table: RSA Algorithm-Time complexity is better than previous

Private Key length (bits)	**Total execution Time in (ms)**
64	86.00
128	91.33
256	110.33
512	142.67
1024	363.67
2048	1221.67

D. Performance Results

The time complexity of RSA is analysed by varying the private key length in bits and noting the execution time for each. The above table shows the details of each private key length. These keys are measured in bits. For each key the number of execution time is measured. Here, we can see that the RSA algorithm time complexity is measured for each private keys length. Starting from 64 bits to 2018 bits. Upon the bits the time complexity of the proposed is far better.

DOI: 10.15680/IJIRCCE.2018.0603020

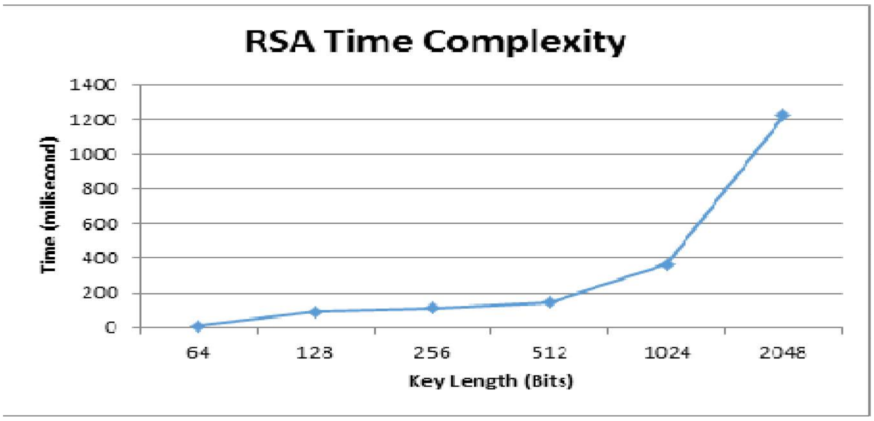

FIG.1: TIME COMPLEXITY OF RSA ALGOTITHM IS MUCH BETTER

As you see the total execution time is measured in milliseconds.As time complexity of the key generation algorithm will be $O(N^2)$ encryption and decryption algorithm using squaring and multiply technique will be O(N^3).The proposed system shows the better results than previous.An algorithm with time complexity O(n) is a linear time algorithm, an algorithm with time complexity O(n^α) for some constants $\alpha \geq 1$ is a polynomial time algorithm.

VI. CONCLUSION AND FUTURE WORK

Cloud computing is world's biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. It increases the ease of usage by giving access through any kind of internet connection. As every coin has two sides it also has some drawbacks.Privacy security is a main issue for cloud storage. This report categories the methodologies in the literature as encryption based methods and auditability schemes. Even though there are many techniques in the literature for considering the concerns in privacy, no approach is highly developed to give a privacy-preserving storage that overcomes all the other privacy concerns. Thus to handle all these privacy concerns, we need to develop privacy– preserving framework which handle all the worries in privacy security and strengthen cloud storage services.

REFERENCES

1.Boyang Wang, Baochun Li and Hui Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud”, IEEE Transactions on services computing, vol. 8, no. 1, January/February 2015.
2.Dr. PrernaMahajan&AbhishekSachdeva , “A Study of Encryption Algorithms AES, DES and RSA for Security”,Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013
3.G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores”, Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), pp. 598-610, 2007.
4.C. Wang, Q. Wang, K. Ren ,“Privacy-Preserving Public Auditing for Secure Cloud Storage Auditing”, IEEE transaction on computer, 2013.
5.M. Blaze, G. Bleumer, and M. Strauss, “Divertible Protocols and Atomic Proxy Cryptography,” in the
Proceedings of EUROCRYPT 98. Springer-Verlag,pp.127– 144,1998.
6. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing”,Proc. 14th European Conf. Research in Computer Security (ESORICS09), pp. 355-370, 2009.
7. H. Shacham and B. Waters, “Compact Proofs of Retrievability”, Proc. 14th Intl Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT08), pp. 90-107, 2008.
8. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores”, Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), pp. 598-610,2007.
9. G. Ateniese and S. Hohenberger, “Proxy Re-signatures: NewDefinitions, Algorithms and Applications,” in the Proceedings ofACM CCS 2005, pp. 310–319, 2005.
10. Tao Jiang, Xiaofeng Chen, and Jianfeng Ma,” Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”IEEETransactions on Computers,, Issue -10.1109/TC.2015.2389955,2015.
11.MeeraHanumantRanadive, Prof.BhavanaPansare,” A Survey on Privacy-Preserving PublicAuditing For Regenerating-Code-Based CloudStorage Using AttributeBasedApproach”, International Journal of Innovative Research in Computerand Communication Engineering,

Vol. 3, Issue 12, December 2015
12.AsmaKhatoon and Dr.Ataul Aziz Ikram," Performance Evaluation of RSA Algorithm in Cloud Computing Security", International Journal of Innovation and Scientific Research, Vol. 12 No. 1 Nov. 2014.
13.Gartner, "Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services", http://www.gartner.com/it/page.jsp?id= 1064712
14.G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson, and D. Song, "Provable DataPossession at Untrusted Stores," Proc. 14th ACMConf. Computer and Comm. Security (CCS '07), pp.598-609, 2007.