International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - I (Online): 2454- 1966

Research Manuscript Title

PERFORMANCE ANALYSIS OF PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN CLOUD USING RSA AND AES ALGORITHMS

Parimala Raghavan, Dr. S. Subasree,

P.G.Scholar, Professor & HOD,
Department of CSE,
NCERC, Pampady
Thiruvilwamala, Thrissur, Kerala

E-Mail: neelima.raghavan@gmail.com, hodcse@gmail.com

March – 2016

www.istpublications.com

International Journal of Future Innovative Science and Engineering Research (IJFISER), Volume - 2, Issue – I,
ISSN (Online): 2454- 1966 www.istpublications.com.

PERFORMANCE ANALYSIS OF PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT USER REVOCATION IN CLOUD USING RSA AND AES ALGORITHMS

Parimala Raghavan, Dr. S. Subasree,

P.G.Scholar, Professor & HOD,
Department of CSE,
NCERC, Pampady
Thiruvilwamala, Thrissur, Kerala

E-Mail: neelima.raghavan@gmail.com, hodcse@gmail.com

ABSTRACT

Cloud computing is a very familiar term used for the recent development of internet. It is computed in which very large group of remote servers is networked and provide centralized data storage and online access to computer services. Considering Cloud computing, Data security becomes more and more important. When users put their large size of data in the cloud, the data integrity protection is challenging. Public auditing of cloud data storage security is very essential. Encryption is the one of the most important secured ways of preventing unauthorized access. RSA is widely used public-key algorithm, generally it's considered more secure than other encryption algorithms. RSA security is based on integer factorization problem. Small encryption and decryption key were quickly factored and discovered. To overcome this problem we have made use of the AES algorithm because AES requires less encryption and decryption time as well as less space as compared to RSA algorithm. In this paper, we have compared RSA and AES algorithm in terms of uploading time and key size. Based on the comparison results AES algorithm outperform RSA in terms of uploading time. From the analysis we have identified that AES algorithm is best and secured algorithm for Cloud Environment.

Keywords— Cloud computing, Public Auditing, TPA, RSA, AES

I. INTRODUCTION

Cloud computing, is kind of Internet-based computing, where data, information and shared resources are provided to computers and other devices on-demand. It is the new technology that share computer resources through internet instead of using software. Cost saving is the main advantage of cloud computing and the prime disadvantage is data security. The data stored in cloud is accessible to everyone so security is not guaranteed. To ensure data security effective third party auditor is introduced. In the auditing process TPA performs audits for multiple users simultaneously and efficiently. Public verifier efficiently check the correctness of data without downloading the entire data this is commonly referred to as public auditing mechanism. TPA will help data owner to make sure that his data are safe in the cloud and less burdening to data owner.

Network security has become an important issue. Encryption is the best way to overcome the solution, and plays an important role in information security system. Each encryption methods have advantages and disadvantages. RSA is commonly used Public-Key algorithm, generally it's considered more secure than other encryption algorithms. RSA security based on the integer Factorization problem. The security of the RSA cryptosystem is implemented on two mathematical problems: the problem of factoring large numbers and the RSA problem. Small encryption and decryption key were quickly factored and discovered. To overcome this problem introduce advance encryption standard algorithm. AES algorithm used not only for security but also it provides great speed. From the analysis we have identified that AES algorithm is best and secured algorithm for Cloud Environment.

This paper organized six sections. In section 2 discuss about related work. Section 3 describes problem statement followed by system architecture in section 4. Performance analysis of this paper in section 5. In section 6 discuss about result and discussion.

II RELATED WORKS

To protect the integrity of data in the cloud, numbers of mechanisms have been proposed. All these mechanisms each block of data a signature is attached, and the integrity relies on correctness of these signatures. Most of the previous work focus on auditing the integrity of personal data but some recent works [2][4] focus on how to preserve identity privacy when auditing the integrity of shared data. The public mechanism proposed by Wang *et al.* [2] is able to preserve confidential data from the TPA based on random masking. In this paper, use the technique of providing more security by using the TPA. The TPA allows the user to know the information about the data stored in the cloud. When anyone tries to modify the data TPA informs the user by verifying the data. The TPA does not even allow CSP (cloud service provider) to read the data of the user.

To operate multiple auditing tasks from different users efficiently, this mechanism support batch auditing. One recent work [4] proposed a mechanism for public auditing shared data in the cloud for a group of users. In this paper based on ring signature scheme with homomorphism authenticators, the TPA can verify the integrity of shared data but is not able to reveal the identity of the signer on each block. It supports an external auditor to audit user's outsourced data in the cloud. The main advantages of this mechanism are public auditability, storage correctness and privacy preserving but one main drawback is it is not support user revocation when auditing the data.

The auditing mechanism in [3] is designed to preserve identity privacy for a large number of users. However, it fails to support public auditing.

Most of previous works in cloud data security is considering with the correctness of data at remote servers. Deswarte et al. in [5] use RSA based encryption method to verify the data file stored in remote servers. One of the main limitations of this scheme is computational complexity.

III PROBLEM STATEMENT

In this paper, we are planning to implement public auditing in cloud using two encryption techniques. In RSA takes more time for uploading compared to AES so we plan to implement AES algorithm in a cloud environment. In this section describes public auditing system architecture and public auditing mechanism and encryption methods using these mechanisms.

IV SYSTEM ARCHITECTURE

System model consisting three entities: the cloud, TPA or public verifier and users who share data as a group.

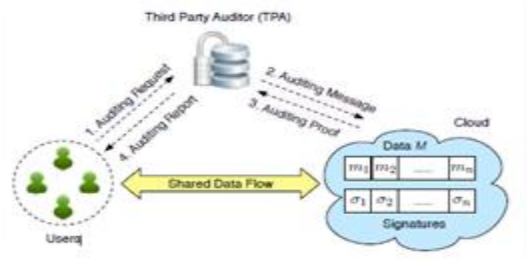

Fig (1) : System Model

The cloud provides data storage and sharing services. The public verifier or third party auditor utilizes cloud data for particular purposes such as searching, computation and data mining etc. TPA provides verification services via challenge-and-response protocol. In a group, there is one original user who creates the data and shares data with other users in the group through the cloud. Once a user is revoked, the signatures computed by the revoked user become invalid. In this case the cloud is able to re-sign the blocks, which were already signed by the revoked user.

The important design objectives are correctness, efficient user revocation, public auditing, scalability and network security. The public verifier checks the correctness of data. The cloud data can be efficiently shared among group users, and TPA is able to handle large number of auditing tasks simultaneously. Considering this paper one of the important design goals is to achieve network security. Encryption is the best way to overcome this solution.

Public Auditing Mechanism **–** To protect the integrity of data a signature is attached to each block of data this mechanism commonly referred to as public auditing mechanism. In this mechanism public verifier efficiently checks the correctness of data without downloading the entire data. TPA efficiently audits the cloud data without demanding the copy of data.

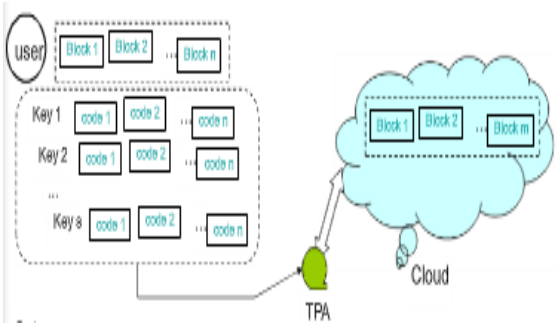

Fig (2) : Verification process

In the verification process simply downloading the data by the user is not practical in this case introducing third party auditor. TPA can do it and provide an audit report. In auditing process contains setup phase and audit phase. In setup phase user uses keys and computes MAC (message authentication code) for blocks of data. User shares the keys and MACs with TPA. In auditing phase TPA gives a key to cloud service provider and request MAC for the blocks and compares with MACs demand the random number of blocks and code from cloud service provider. The main advantage of this scheme is TPA doesn't see the data so data in cloud keeps being confidential.

In public auditing scheme mainly four algorithms are consisting

1) KeyGen

2) SigGen

3) GenProof

4) VerifyProof

User uses key generation algorithm to set up the scheme. This algorithm is used to create a unique key. In this paper this algorithm used to encrypt the key which has to be tested for two different encryption methods RSA and AES and we have identified AES is the best for cloud environment.

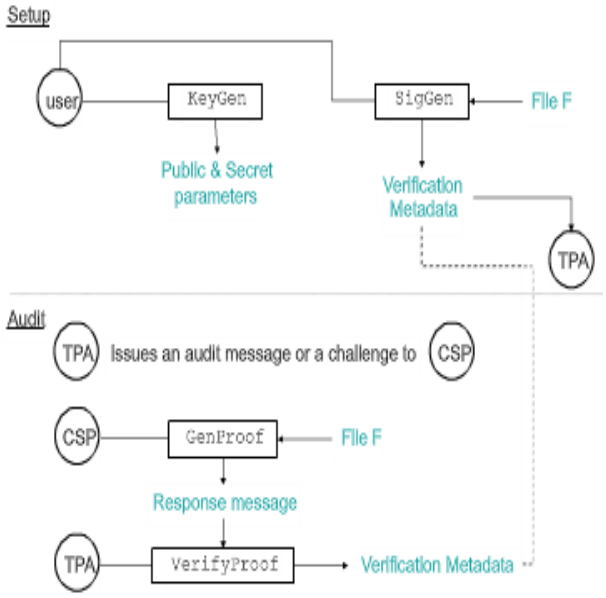

Fig (3) : Public Auditing Scheme

In SigGen (signature generation) used by the user to generate verification of metadata, which may consist of MAC signatures or other information used for auditing. Proof generation (GenProof) algorithm run by the cloud server to generate a proof of data storage correctness. In VerifyProof algorithm run by the TPA to audit the proof from the cloud server.

Public Auditing Using RSA & AES algorithms

In cloud environment network security has become an important issue. Encryption has come up a solution and plays an important role. The main cryptographic goals are authentication, confidentiality, integrity, non-repudiation and service reliability. In this paper we implemented two encryption techniques RSA and AES and compare their performance based on the analysis of uploading time.

RSA Algorithm – Rivest, Shamir and Adelman introduced a new method of public key cryptography in 1977. This new method is named as RSA. In RSA two keys are using for encryption and decryption. RSA is based on public key cryptography. In this public key used for encrypting the data and private key used for decryption.RSA key selection is very complex and time consuming. The prime condition of RSA algorithm is selection of two prime numbers. The product of this prime number is the part of private and public key so the method used for selecting prime numbers must be efficient in the case of RSA. RSA algorithm contains primality test and integer factorizing problem. In primality test algorithm determine whether the input number is prime or not. A file message encrypted and is treated as one large number. When encrypting the data file, it is raised to the power of the key, and divided with remainder by a fixed product of two primes. By repeating the process with the other key, the plain text can be retrieved again.RSA algorithm mainly involves three steps. That is Key Generation, encryption and decryption. In this scheme we had using 1024 bit key size for RSA operation.

AES algorithm – AES is most frequently used algorithm and this algorithm based on several operations like substitutions, permutations and linear transformation etc. Those operations repeated several times called as rounds. Each round, a unique roundkey is calculated out of the encryption key and it is incorporated in the calculations. It's a symmetric encryption algorithm. The algorithm was developed by Joan Daemen and Vincent Rijmen. It supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES has 10 rounds for 128 bit keys and each round consists several processing steps. AES provides fast and flexible encryption. It can be easily implemented on various platforms. AES has a speedy key setup time and it is suitable for limited-space environment. It makes efficient use of resources which results in a very efficient software performance.

In this paper, we are focusing uploading time for different data files and the experiment is conducted using two different encryption algorithms RSA and AES. From this we can say that AES algorithm is efficient for cloud environment.

V PERFORMANCE ANALYSIS

We had implemented public auditing in cloud with efficient user revocation using RSA and AES encryption algorithms and we identified AES algorithm is more efficient and secure than RSA. In this scheme we have using 1024 bit key size for RSA operation and 128 bit key size for AES operation. In that condition also we analyze AES is better performance compared to RSA

Data Size(bytes)	Uploading Time in ms(RSA)	Uploading Time in ms(AES)
1.91MB	109	57
326KB	62	31
124 KB	47	15
41 KB	16	0.2

Table (1) : Uploading time Comparison between RSA Vs AES

The above table shows uploading time for different files using RSA and AES algorithms and the time taken in milliseconds. We had uploaded different data files and we identified RSA taking more time compared AES. The following figure shows the graphical representation of the table values.

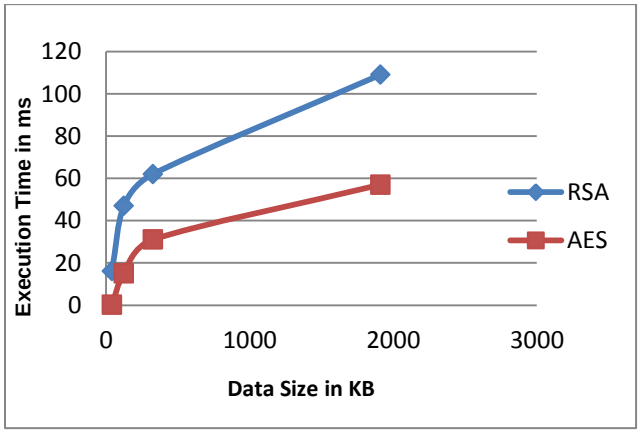

Fig (4) : Execution time between RSA Vs AES

VI RESULT AND DISCUSSION

In this paper, we are focusing public auditing in the cloud using different algorithms with efficient user revocation. We proved uploading time taking AES is very less compared to RSA algorithm. From this we can identify that AES algorithm is efficient for cloud environments.

In this mechanism provides a number of advantages in cloud computing. The main advantage is TPA can save encrypted data file on cloud and perform the integrity verification without downloading the entire file. Once the user is revoked in the group, the cloud themselves re-sigh the blocks so the efficiency of the user revocation is significantly improved in this scheme.

VII CONCLUSION

In cloud computing, data security is the biggest challenge. A number of research work carried out in this area. TPA can perform multiple auditing tasks simultaneously this provides better efficiency. Encryption is the one of the most important secured ways of preventing unauthorized access. Different kinds of encryption techniques applied in a cloud computing environment. In this way hacking can be prevented. In this paper, we have compared RSA and AES algorithm in terms of uploading time. Based on the comparison results AES algorithm outperforms RSA in terms of uploading time. From the analysis we have identified that AES algorithm is the best and secured algorithm for Cloud Environment.

REFERENCES

[1] Boyang Wang, Baochun Li, and Hui Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud", *IEEE Trans. On Services Computing*, VOL. 8, NO. 1, pp. 92-106 ,Jan-Feb 2015.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- preserving public auditing for data storage security in cloud computing," in *InfoCom2010, IEEE*, March 2010.

[3] B. Wang, B. Li, and H. Li, "Knox: Privacy Preserving Auditing for Shared Data with Large Groups in the Cloud," *Proc. 10th Int'l Conf. Applied Cryptography and Network Security,*PP.*507-525,*June *2012*.

[4] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," *IEEE Tns On Cloud Computing,*VOL.2, NO. 1, pp. 43-56, Jan-March 2014.

[5] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote integrity checking", In Proc. of Conference on Integrity and Internal Control in Information Systems (IICIS'03), November \2003.