International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

Threshold Cryptography Based Data Security in Cloud Computing

Swati Swaraj[1], Chaitrali Pawar [2], Pragati Singh[3], Abhilasha Pawar[4], vaishali suryawanshi[5]

[1234]Student, Dept. of Information Technology, MIT College of Engineering, Maharashtra, India
[5]Professor, Dept. of Information Technology, MIT College of Engineering, Maharashtra, India

---

Abstract: *Cloud computing is the long dreamed idea of computing as an effectiveness. Besides all the benefits of the cloud computing security of the stored data need to be considered while storing sensitive data on the cloud. Cloud users cannot rely only on cloud service provider for the security of their sensitive data stored on the cloud.*

This paper proposes two schemes to address security issues associated with cloud storage first one is of public auditing and the second one is threshold cryptography. The technique of Third Party Auditor (TPA) checks the integrity of data stored on the cloud for data owner. In Threshold, Cryptography scheme data owner generates the secret key for every file before uploading it to the cloud and split the key into a number of parts and distribute these parts to data users.

Key Word: **Threshold Cryptography, Third Party Authenticator, Cloud Service Provider, Checksum, Data Integrity Check**

1. INTRODUCTION

Clouds have become the buzzword in computing. Security issues of cloud computing may lead to loss of sensitive data of cloud users. The sensitive data on the cloud can be compromised by various means such as cloud service provider (CSP), users own improper operations, unauthorized user etc. Cloud data can be compromised by both CSP and data users. Studies of deployed large-scale storage systems show that no storage service can be completely reliable; all have the potential to lose or corrupt customer data.

To ensure the security and integrity of Owners data stored on cloud Data Owner need to rely on security protocols provided by CSP otherwise he needs to manually check the integrity of data. Both of these solutions are not feasible as it may become the tedious job to check such a huge amount of data manually on the other hand CSP may leak the data to unauthorized person for malicious purposes.

This system is composed of three entities a CSP, a DO and many users associated with DO. Initially, all Users are registered at DO. During registration users send their credentials to DO. We assume that user's credentials are sent securely to DO. DO then divides users into groups and provides encryption keys, tokens, algorithm and other necessary things for secure communication to user groups in a response to registration. A user can get data from CSP in a confidential manner after successful authentication of himself at CSP. We assume that CSP has a large capacity and computational power. We also assume that no one can breach the security of CSP. Further, we assume that the algorithm which is used to generate the secret keys for encryption is secure at DO. DO have the storage capacity to store some files and data and, he can execute programs also at CSP to manage his files and data. We are using modified public key cryptography to secure communication between CSP and user.

Cloud computing mostly two important security requirements are keep data secure and efficient access control for data. Sometimes we focus on data security we not concentrate on system performance access control and have to focus on DO, CSP, users. Like sometimes we use the keys for secure data.

All keys are confidential so need to be kept secure and maintain these keys which are additional work. These additional works affect the performance of the system. Hence it is needed to reduce these keys so our system help for reducing keys to provide data security as well as increased the performance of the system. Many schemes are suggested to meet these requirements.

1.1 Overview

This System defines the group-key scheme. In this scheme, there is single key for the one user group for decryption process and this single key used by each user in group. These scheme help for the reduce key but simultaneously it will be cause for collusion attack as many cloud service providers can attack and there is a user a single malicious user can access the hole data of group and leak whole data of the group to Cloud Service Providers. As we know that Cloud Service Provider is not trusted party. Cloud service providers can access data owner's data for the commercial benefit.

n the Proposed system can define data security and data access. In this scheme data encrypted by symmetric key and this symmetric key are only known to the data owner and corresponding data users. Data owner can encrypted data same will be uploaded on cloud server. CSP can't see data stored at it as data are encrypted. Data are further encrypted by one time session key which is secret.

1.2 Problem Statement

This system proposes two schemes to address security issues associated with cloud storage first one is of public auditing and second one is threshold cryptography. The

technique of Third Party Auditor (TPA) checks integrity of data stored on cloud for data owner.

In Threshold Cryptography scheme data owner generates secret key for the every file before uploading it to cloud and split the key into number of parts and distribute these parts into data users.

2. RELATED WORK

Users can store their data and take advantage from the on-demand high-class applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. but in reality the fact that users no longer have physical control of the outsourced data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, users can have remedy to a third-party auditor (TPA) to check the integrity of outsourced data and be worry-free.

Paper[1] propose the privacy-preserving public auditing system for cloud storage . The TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

[2] Two schemes to address security issues associated with cloud storage first one is of public auditing and second one is threshold cryptography. The technique of Third Party Auditor (TPA) checks integrity of data stored on cloud for data owner. In Threshold Cryptography scheme data owner generates secret key for the every file before uploading it to cloud and split the key into number of parts and distribute these parts into data users. This scheme helps to achieve data security.

[3] This paper propose a scheme that uses threshold cryptography in which data owner divides users in groups and gives single key to each user group for decryption of data and, each user in the group shares parts of the key. In this paper, we use capability list to control the access. This scheme not only provides the strong data confidentiality but also reduces the number of keys. Cloud computing is very popular in large and small scale organization as it will store a large amount of data and provide low-cost service. Hence it was created daily new challenges to provide secure authorization, integrity and access control. Some approaches are ensuring security but there is also some lack of these approaches and issues due to the collusion attack, heavy computation. To solve this concern we projected a scheme it's threshold cryptography in which data holder can divide users in the group and provide the single key with the user key each user in the group can access the data. In these studies, we use capability list to control the access. In this scheme not only provide data security but also provide reduce the number of keys.

The paper [4] presents Semi anonymous privilege control scheme. Anony Control to address not only the data privacy, but also the user identity privacy in existing access control schemes.

3. PROPOSED SYSTEM

This System defines the group-key scheme. In this scheme, there is single key for the one user group for decryption process and this single key used by each user in the group. These scheme help for the reduce key but simultaneously it will be cause for collusion attack as many cloud service providers can attack and there is a user a single malicious user can access the hole data of group and leak whole data of the group to Cloud Service Providers. As we know that Cloud Service Provider is not trusted party. Cloud service providers can access data owner's data for the commercial benefit.

In the Proposed system can define data security and data access. In this scheme data encrypted by a symmetric key and this symmetric key is only known to the data owner and corresponding data users. Data owner can encrypted data same will be uploaded to the cloud server. CSP can't see data stored at it as data are encrypted. Data are further encrypted by one-time session key which is secret.

Data Security and checksum generation

Data Owner uploads document, metadata, the checksum on the cloud after encryption using keys from Data Owner and Cloud Service Provider. Also, a copy of metadata and checksum is sent to Auditor.

Data Access Via Permission model

Registered users send access request and receive encrypted file if authorized. User calculates checksum to compare with original and reports to Data Owner if checksum mismatch occurs.

Multiparty Authentication Protocol for file access

Requestor initializes key and puts his component in keyset and forwards to other users in the group for updating. After all, users have updated keyset, requestor receives complete key and uses to decrypt file.

Data Integrity Check by Third Party Authenticator (TPA)

Auditor Receives metadata after upload. Performs periodic or on-Demand integrity checks by sending challenges to Cloud Service Provider. On response from Cloud Service Provider, Auditor confirms response and reports status to Data Owner.

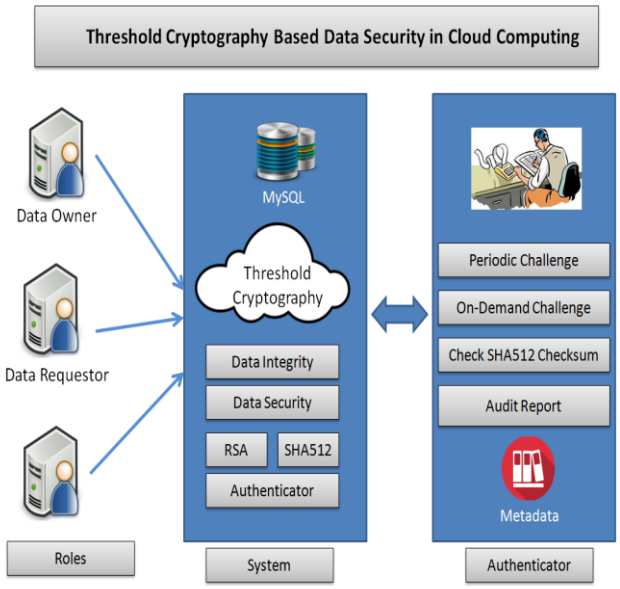

Fig.1 Architecture diagram for Threshold Cryptography Based Data Security in Cloud Computing

4. PROPOSED METHOD

Algorithm Used:

1. AES Algorithm

The key size of AES is in general 128 bits. Whereas 256 bits and 512 bits keys are also possible to use. The package javax.crypto of the Java has the implementation of the AES algorithm. For 256 bit key encryption/decryption special policy files should be copied into the \jre\lib\security directory, which can be downloaded from Oracle's web site.

a. Encryption

- You follow the consequent AES steps of encryption for a 128-bit block.
- Get the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the preliminary round key to the initial state array.
- Perform nine rounds of state manipulation.
- Complete the tenth and final round of state handling.
- Rewrite the last state array out of the encrypted data (cipher text).

Every round of the encryption method requires a sequence of steps to alter the state array these steps involve four types of operations called:

1. Sub-Bytes
2. Shift-Rows
3. Mix-Columns
4. Xor-Round Key

b. Decryption

In AES decryption we convert the information into read-able to only those possessing special knowledge, usually referred to as a key.

Decryption involves reversing all the steps taken in encryption using contrary functions:

1. InvSub-Bytes
2. InvShift-Rows
3. InvMix-Columns

Operation in decryption is: Perform initial decryption round:

- Xor-Round Key
- InvShift-Rows
- InvSub-Bytes

1. Perform nine full decryption rounds:

   Xor-Round Key
   InvMix-Columns
   InvShift-Rows
   InvSub-Bytes

2. Perform final Xor-Round Key

2. RSA Algorithm

The keys to the RSA algorithm are generated the following way:

1. Prefer two different prime numbers p and q.

- For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits to make factoring harder. Prime integers can be efficiently found using a primary test.

2. Compute n = pq.

n is used as the modulus for both the public and private keys. Its span, usually expressed in bits, is the key span.

3. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n-(p+q-1)$,

where φ is Euler's totient function. This value is kept private.

4. Select an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.

5. Determine d as

$d = e^{-1} \pmod{\varphi(n)}$;

i.e., d is the modular multiplicative inverse of e (modulo $\varphi(n)$)

- e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. on the other hand, much slighter values of e (such as 3) have been revealed to be fewer secure in some settings.
- e is released as the public key exponent.
- d is kept as the private key exponent.

The confidential key contain modulus n and the confidential (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be reserved secret because they can be used to calculate d.

SHA 512 Algorithm

a. Append Padding Bits and Length Value:

This step makes the input message an exact multiple of 1024 bits:

b. Initialize Hash Buffer with Initialization Vector:

Before we can process the first message block, we need to initialize the hash buffer with IV, the Initialization Vector

c. Process Each 1024-bit (128 words) Message Block Mi:

Each block is taken throughout 80 rounds of dispensation.

d. Finally:

After all the N message blocks have been processed, the content of the hash buffer is the message digest.

5. EXPECTED RESULT

In this scheme data owner generates secret key for the every file before uploading it to cloud and split the key into number of parts and distribute these parts into data users. The result is discussed using graph. Graph represents(figure 2)the expected outputs of proposed system. X- axis shows the file size in Kilobytes and Y- axis shows the time required for key generation in milliseconds. And figure 3 shows operation time for different key sizes.

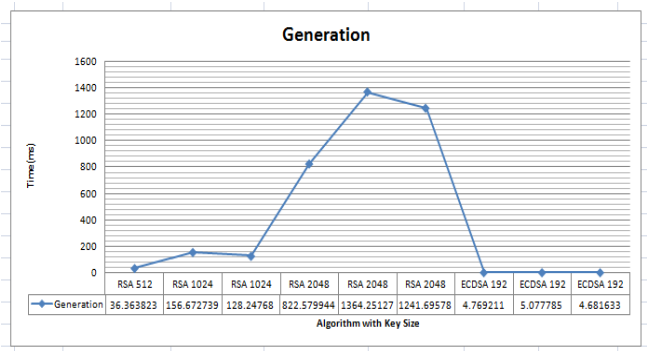

Fig-2: Time With Respect to Key Size

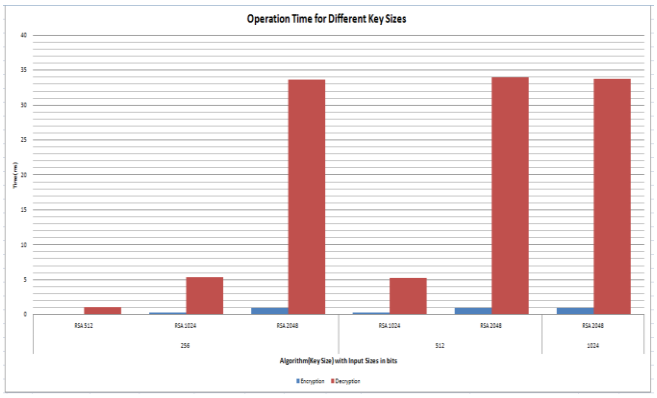

Fig-3: Operation Time For different Key

6. CONCLUSIONS

We have two schemes to address security issues associated with cloud storage first one is of public auditing and the second one is threshold cryptography. The technique of Third Party Auditor (TPA) checks the integrity of data stored in the cloud for data owner. In Threshold, Cryptography scheme data owner generates the secret key for every file before uploading it to a cloud and split the key into a number of parts and distribute these parts to data users.

REFERENCES

[1] Q. Wang, C. Wang, K. Ren, W. Lou, Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.

[2] Reshma B. Suryawanshi, S.N.Shelke"Privacy-Preserving Public Auditing and Threshold Cryptography Scheme for Improving Cloud Storage Security" FIFTH POSTGRADUATE CONFERENCE OF COMPUTER ENGINEERING, CPGCON 2016.

[3] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, Sundaram Vats, "Threshold Cryptography Based Data Security in Cloud Computing", 2015 IEEE International Conference on Computational Intelligence Communication Technology

[4] Taeho Jung, Xiang-Yang Li, Senior Member, IEEE, Zhiguo Wan, and Meng Wan, Member, IEEE"Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015.

[5] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Stephen S. Yau,"Efficient audit service outsourcing for data integrity in clouds", The Journal of Systems and Software 85 (2012) 1083 1095.International Journal of Network Security Its Applications (IJNSA), Vol.3, No.1,

January 2011.International Journal of Network Security Its Applications (IJNSA), Vol.3, No.1, January 2011.

[6] Mehul A. Shah, Ram Swaminathan, Mary Baker, "Privacy-Preserving Audit and extraction of Digital Contents", HP Laboratories, Palo Alto HPL-2008-32R1 April 30, 2008.