Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing Data in Cloud Storage Using Regenerating Code and Visual Cryptography

Geeta. F. Nadlamani*, Prof. Shabnam Shaikh
Computer Department & UoP
India

Abstract*— The regeneration code provide fault tolerance with low repair bandwidth. In regeneration coded data, there exists remote checking method providing private auditing, which includes data owners to stay online, which is impractical . To avoid this, public auditing scheme for regenerating code is proposed, proxy is used to solve problem of regeneration problem used to generate failed authenticator in public auditing system. This scheme eliminates data owners from online burden.

Keywords*— Visual cryptography, regenerated code, public audit scheme, privacy preserving, cloud storage.

I. INTRODUCTION

Cloud service providers may hide data loss, may act dishonestly and claim that data is stored correctly in cloud to maintain reputation. Public auditing for generating code based cloud storage is proposed to save users computation resources, online burden and data integrity. TPA is implemented with regeneration and integrity checking. Proxy is separated on behalf of data owners.

Cloud service provider provides efficient data storage service with a lower cost than traditional approach to check integrity of data in cloud storage is doubtful as data stored in cloud can easily be lost due to errors. There are some services which are used to verify integrity of data of public cloud, which is cloud storage auditing.

II. PROBLEM STATEMENT

The data/file is stored directly into cloud, there is no backup of same data/file in any other machine. This will affect the user to access data whenever needed. There is no such scenario exists which will regenerate lost data/file in case of system failure. So concept of privacy preserving public auditing along with regeneration code has been introduced.

III. SYSTEM MODEL

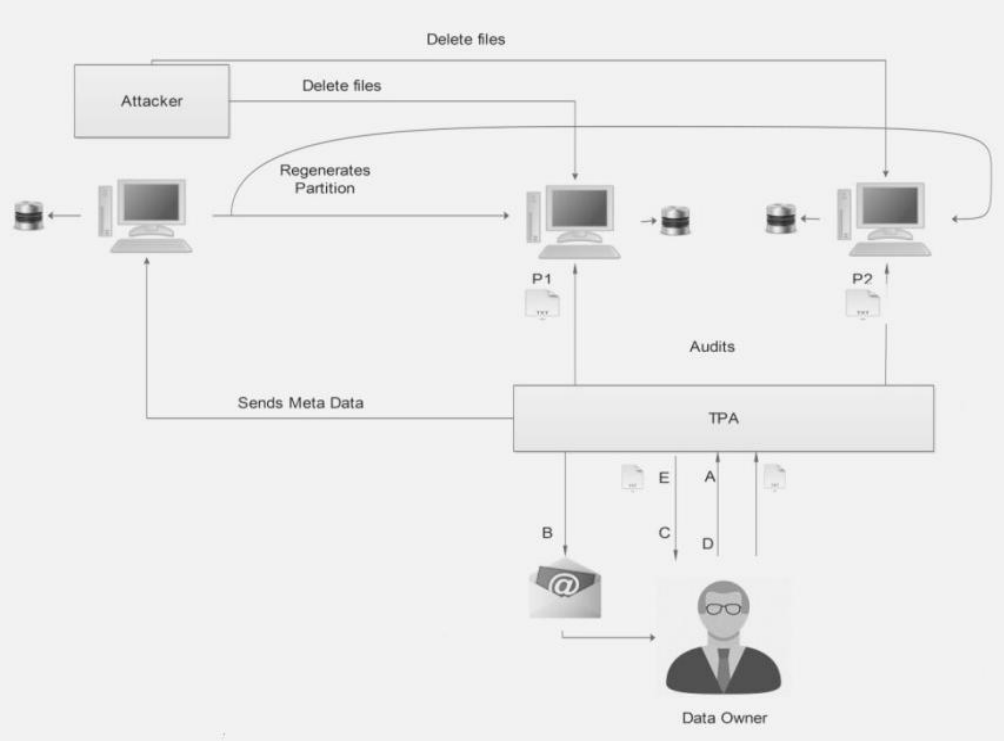


Fig. 1. The system model

It consists of entities like data owners, server, proxy, TPA, Attacker .

1) Data Owners

1. One whose going to access files, one who owns file, who requires his data to be secure.
2. Data owners are responsible for encrypting the data by generating private key.
3. Data/File is encrypted using AES Algorithm
4. Data owner sends data/file to TPA and takes help of TPA.
5. Data owner is responsible for captcha generation. Owner is going to access half of information from application and half of information through e-mail and need to combine it and send it to TPA.
6. Data owner is provided with log window to see how TPA is working and get report of the same.
7. Data owner pays to TPA to get security of its data and can access valuable data at anytime.

2) Server

1. One whose going to access files, one who owns file, who requires his data to be secure.
2. Two different servers are used to store half –half information into each servers.
3. Not necessary that both the servers are different but they can be same.
4. TPA is responsible for splitting data/file into two parts so as to secure the data.
5. Attacker can attack either of the servers or both. Attacking both servers can be rare , there is a possibility of attacking one server at a time.
6. So, if both the servers are the same then its easier for attacker to retrieve data easily from these both servers.
7. Ever since data is in encrypted format, its probably difficult for attacker to decode it ; but this will ultimately lead to data owner to suffer in one or the other way.
8. In order to solve this problem metadata is stored for each server content into proxy server.
9. Suppose size of data stored in server 1 is 2GB and similarly size of data stored in server2 is 2 GB. So backup of these two servers require 2GB space.
10. If we are using metadata to store backup of these servers it will probably require less storage size i.e less than 2 GB.

3) TPA(Third Party Auditor)

1. There are basically three types of audits product, process and system. Audits are name according to there purpose.
2. Audits are classified into internal or external, depending upon relationship of participants.
3. Internal audits are performed within an organization by employees.
4. External audits are performed by Third party agent or outside agents.

A. First –party audit

It is an internal audit performed within organization to measure strength and weakness against its own procedure.

B. Second-party audit

1. It is external audit , performed on behalf of customers by a contracted organization.
2. They have to sign contract law since they are providing contractual direction from customer to supplier.
3. They are more formal than first-party audit. Since they may help to change decision of customer.

C. Third-party audit

1. Audit is performed by an organization free from customer supplier relationship.
2. It results into certification, registration and recognition.
3. Used to conduct public audit on data in cloud, its trusted and its audit result is imparted for both owners and servers.
4. It maintains the audit record of when the data was corrupted and when it was corrected.
5. It maintains session log of the same and keeps it feasible so that data owner can see the work of TPA.
6. Data owners pay to TPA for auditing there data and securing there data from malicious users.
7. TPA is responsible for splitting data/ file into two parts and generate digital signature for each part using SHA1 algorithm and finally keep it in two different servers respectively.

4) Proxy Agent

1. Its semi-trusted, acts in place of data owners to regenerate with authenticators.
2. Proxy which is always online , is supposed to be more powerful than data owners but less powerful than cloud servers for computation and memory storage capacity. As compared to traditional public auditing system, proposed system includes additional proxy agents.
3. There are few properties which proposed auditing scheme should attain to efficiently verify integrity of data keep stored file available for cloud storage. Public auditability, storage, soundness, privacy preserving, authenticator regeneration error location.

5) Attacker

1. Attacker can delete file from either of servers.
2. Attacker can get the data but cant decrypt the encoded data/file which will result into inconvenience of data to end user.

IV. PROPOSED SCHEME

Auditing scheme includes three procedures setup, audit and repair.

1) Setup

Three polynomial time algorithms are used:

i) KeyGen (1k) → (pk, sk) : By taking security parameter 'k' as input data owners run this algorithm to initialize there public and secret parameters.

ii) Delegation (sk) → (x) : Interaction between data owners and proxy, proxy receive practical secret key 'x' from data owners.

iii) Sinand blockgen (sk, F) → (ϕ, Ψ, t) : Its run by data owners which take input as secret parameter sk and file F and outputs coded block ϕ, authenticator Ψ and file tag t.

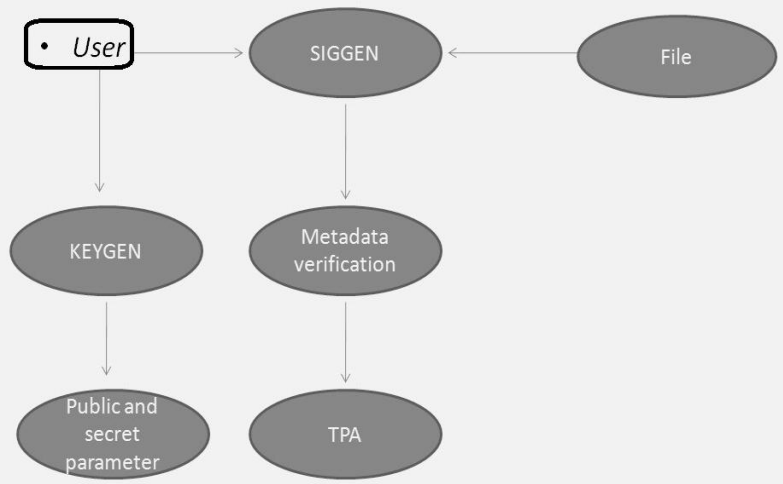


Fig. 2 Setup Phase of proposed scheme

2) Audit

Cloud server interacts with TPA taking random sample or blocks.

i) Challenge (Finfo) → (C) : Its performed by TPA, *Finfo* file information and C challenge.

ii) Proofgen (C,ϕ,Ψ) → (P) : Its run by almost all cloud server.

iii) Verify (P, pk, C) → (0, 1) : Its run by TPA as soon as it receives proof. If output 1 verification is successful, else 0.

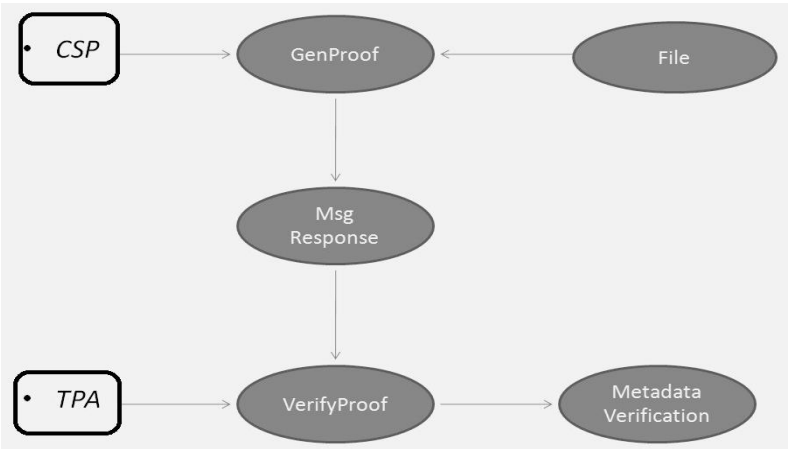


Fig. 3 Audit Phase of proposed scheme

3) Repair

Proxy interacts with cloud server in absence of data owners used to repair wrong server detected by the auditing process .

i) Claimforrep (Finfo) → (Cr) : Its same as challenge algorithm in audit phase.

ii) Genforrep (Cr,ϕ,Ψ) → (BA) : Cloud servers run this algorithm and output authenticators set BA with input set Cr, ϕ, Ψ.

iii) Blockandsigregen (Cr,BA) → (ϕ′,Ψ′,⊥) : This algorithm is implemented by proxy with claim Cr and output a new coded block set Ψ′, authenticator set ϕ′.

V. ALGORITHM FOR FILE ENCRYPTION

A. AES Algorithm

Its Advanced Encryption Standard use Rijndael block cipher.

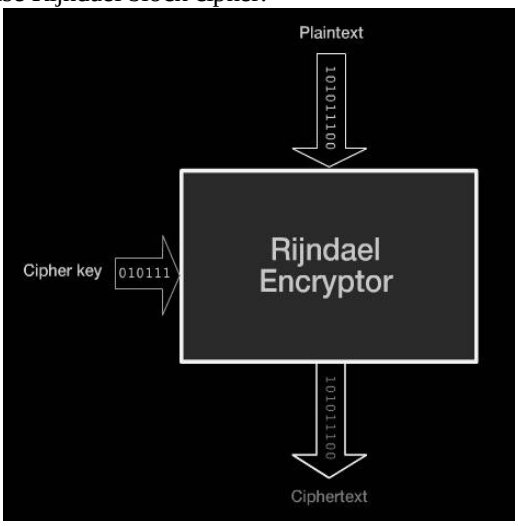


Fig. 4 AES Algorithm using Rijndael Encryptor

Input : State (block from plaintext msg to be encrypted) Cipher Key.
Two Phases:

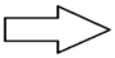
To Encrypt process.
To key schedule.

i) To Encrypt process: Perform encryption of the given plaintext block using four different transformation in the initial round, nine main rounds and final round.

(1) Initial round : add round key.
(2) Main round : Four transformation
    SubBytes
    ShiftRows
    MixColumn
    AddRoundKey
(3) Final round : Include only three transformation
    SubBytes
    ShiftRows
    AddRoundKey

Output : Generate Ciphertext.
The Four Types of transformation includes :
a) SubBytes : State is converted into Hexadecimal using S-Box byte substitution table.
b) ShiftRows : ShiftRow operation is performed in. substituted state.

S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}



S00	S01	S02	S03
S11	S12	S13	S10
S22	S23	S20	S21
S33	S30	S31	S32

c) MixColumn : This shifted row then undergoes mix column operation .
Four numbers of 1st column are modulo multiplied in Rijndael's Galois field by given matrix.
d) AddRound Key : Mixed column is xor with round key produced during key schedule.
Final round include 3 transformation i.e subbytes shiftrows mixcolumn i.e 10th round.
Output : Ciphertext.
ii) Key Schedule :
Expansion of given cipher key into partial key used in the initial round, the nine main rounds and final round.

(1) The expanded key can be seen as an array of 32-bit words(column) numbered from 0 to 43.
(2) 1st 4 column are filled with given cipher text.

Words in the position that are a multiple of 4 (W4,W8,…..W40) are calculated by :

(1) Applying the rot word and sub bytes transformation to the previous word wi-1.
(2) Adding (XOR) this result to word 4 position earlier wi-4 plus a round constant Rcon.

Remaining 32-bit words Wi ,calculated by adding(XOR) the previous word wi-1,with the word 4 position earlier wi-4.

B. SHA-1 Algorithm

It is used for digital signature

(1) It is a hashing algorithm having same structure to MD5, but producing a digest of 160 bits(20 bytes).
(2) Since its having large digest size, it is less likely that 2 different msgs will have the same SHA-1 msg digest
(3) Hence SHA-1 is recommended as compared to MD5.

VI. VISUAL CRYPTOGRAPHY

Additional concept of visual cryptography is introduced, where owner receives half share from e-mail and other part of share from application these two shares are nothing but two transparent images .Once these two shares are obtained they are merged together to form captcha ,authenticated user need to enter this right captcha and access of the data/file .Due to which data is more secure only authenticated user is allowed to access file not unauthorised user .It is very difficult for hackers to hack the data because of double security provided to data/file. First is visual cryptography and second is dividing data file into two servers separately, which will not allow hacker to access data easily.

VII. CONCLUSION

This paper has introduced public auditing for regenerating code based cloud storage system, which includes TPA, data owners, cloud servers and proxy server. Few schemes are proposed like setup audit and repair; whereas in previous topics of privacy preserving public auditing for cloud storage only two schemes where proposed audit and setup. But this topic includes additional scheme repair due to regeneration concept. Concept of proxy is introduced which solves problem of regeneration in case of authenticator failure.

REFERENCES

[1] Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian, "Privacy-Preserving Public Auditing forRegenerating-Code-Based Cloud Storage," *IEEE TRANSACTIONS ON INFORMATION AND SECURITY*, vol. 1, Nov. 2015.

[2] Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," *IEEE TRANSACTIONS ON CLOUD COMPUTING*, vol. 2, pp. 43-56, January-March. 2014.

[3] 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*, vol.62, pp. 362-375, Ferbruary. 2013.

[4] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, " Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", *in IEEE INFOCOM*, 2010, pp. 1-15.

