INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

IJARnD

(Volume2, Issue7)
Available online at www.ijarnd.com

Survey on Proof of Violation in Cloud Storage

Sindhu J. P[1], Divyashree .J[2]
[1]*Student, Computer Science & Engineering, SJB Institute of Technology, Karnataka, India*
[2]*Assistant Professor, Computer Science &Engineering, SJB Institute of Technology, Karnataka, India*

ABSTRACT

It mainly determines the Proof of Violation (POV) scheme in the cloud storage systems, this scheme is used in which it allows the users to produce some cryptographic proofs, to determine whether the violation has been occurred by the user or whether he is innocent by providing cryptographic proofs. Since Security and reliability are the two major concerns about cloud storage. However, clients lose control of files when uploading to the cloud storage. Files may be unexpectedly exposed to a third party or modified without permission or the hackers may take an advantage of such files. The cloud may not follow user's instruction to safely store files. For example, if files are damaged or lost, users usually do not have any precise proof to prove it. Since customers cannot make informed decisions about the risk of losing data stored since their incentive to rely on these services is reduced. Hence a new scheme approach i.e., proof of violation is been developed in which it can be achieved using SLA Agreement, in which it can be used to provide the mutual non-repudiation guarantee with the service provider in the cloud storage. Auditing of files must be done since it keeps tracks of each file operation and determines if there is any violation in the SLA. The result of all these file operations and hash values of the downloaded files are stored in the cloud server and hence can achieve real-time auditing through it. Therefore the cloud must provide security features so that only authorized person can access and provide authentication for each file to improve better security features and back-up the lost data files. Therefore in order to enhance better performance and efficiency through which maximum time effort can be reduced.

Keyword: Cloud Security, Cloud Storage, Proof of Violation, Service-Level Agreements.

1. INTRODUCTION

Cloud storage is a model of networked online storage where data are stored in virtualized storage pools that are hosted by service providers in the cloud. Some of the cloud storage systems include Google Drive, Drop box, One Drive etc. Clients are not likely to entrust their data to another company without a guarantee. The basic security features include authentication, confidentiality, data integrity, freshness, the first three of which can be easily implemented using cryptographic cloud storage in [2]. Each file stored in cloud storage needs to be associated with encryption that is generated by the private key of the user, so as to guarantee the file integrity. However, the user still cannot ensure that his/her files will not be lost or that the files retrieved from cloud storage are the latest ones. Consider the situation that some files of the user stored on a cloud storage system are damaged or destroyed because of some kind of internal errors or malicious attack, the service provider is likely to then restore the files using a backup of an early version of the files. However, till today none of the cloud storage systems provides guarantees for such properties in their service-level agreements (SLAs). If we want to include more guaranteed properties in an SLA, Therefore new scheme is developed so that the service provider can prove their innocence or the users can prove the service provider's guilt when the user makes false accusations or the service provider violates the desirable properties.

1.1 Proof of Violation (POV)

The proof of violation enables the users or the service providers to produce the certain proofs, to prove either user has done the violation or he is innocent. First, it should define a set of properties through an SLA agreement in which the service provider must not violate those rule during an ongoing operation. Second, proofs are based on SLA rules, in which the messages are sent via email in which it binds the users to the requests they make via the secret-key/OTP in the cloud server. Third, auditing can be performed according to collected proofs to prove if properties are violated or not in the cloud server in [5]. If all the rules are not violated it shows successful operation at the cloud server and proves the user or the client is innocent. Otherwise, shows violation occurred due to failure in the SLA which proves the failure of the operation.

2. SYSTEM ARCHITECTURE

The system architecture involves a cloud storage, a synchronization server, and some client devices that user employs to access his/her account in the cloud storage.

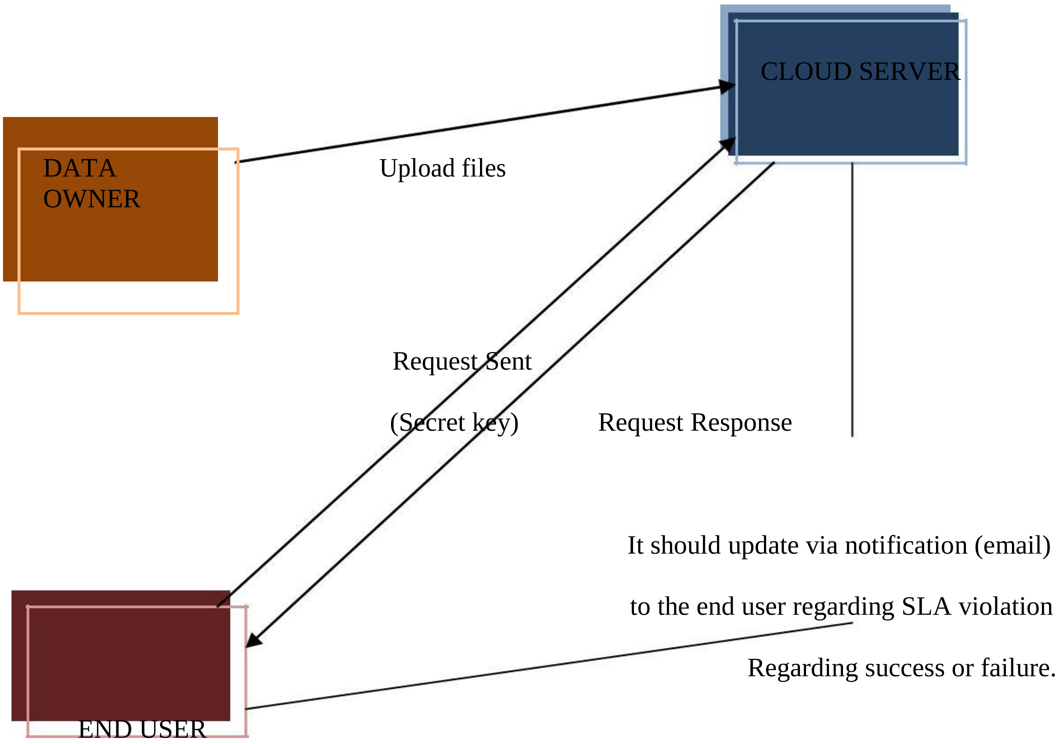
CLOUD SERVER
DATA OWNER
Upload files
Request Sent
(Secret key)
Request Response
It should update via notification (email)
to the end user regarding SLA violation
Regarding success or failure.
END USER

Fig -1: SLA Proof of Violation Architecture.

In above fig the system involves the following:

- Data owner
- End-user
- Cloud server

In the SLA certain agreement rules need to be added and must be followed by data owner and the end-user such as only authorized person need to access, File size must not exceed 5MB and time limit of 60sec need to be given for the downloading of the file. Failure in these rules leads to SLA Violation and message is sent through the End-user site via email. Hence a proof is provided for each success and failure operation. The detailed description is given below

2.1 Data Owner

The data owner refers to one who owns the data, first, he needs to register to the cloud and then login. The owner first uploads the file within the specified size limit and after that, the owner encrypts the file and makes a secured file and is protected with a secret-key/OTP. Data auditing and file verification are done via Third party auditors.

2.2 End user

The end-user needs to first register and then login. The End-user then requests a secret-key for a particular file which he needs to download to the cloud server. If the download is a success then file message is decrypted back to its original form. Otherwise its failure then the message is sent back via mail for SLA violation. A request response is obtained through authorized mail-id of the user. For each end-user, a unique id is created and a hash-key is generated for the file downloaded.

2.3 Cloud Server

All the files uploaded are stored at the cloud server site and contains data owner and end-user details. Hence it views all the files details and also determines the auditing of files where it keeps track of all file operation and further determines the execution of files. It also allocates the user space in the cloud and hence it determines the status of the operation whether success or failure. It also updates via email notification regarding SLA Compliance to the cloud server.

If in case there is no sufficient internet due to network traffic, another option can be implemented in POV scheme in which internet connection is not required & can be achieved through SMS Gateway in which the secret-key is sent through mobile as message/OTP to their registered clients for secure file transactions and operations in cloud through which real-time auditing can be achieved in cloud storage.

3. IMPLEMENTATION

The implementation is done through AES Algorithm and SHA-256 algorithm through which encryption and decryption are achieved. It is as described below

3.1 AES Algorithm

It stands for Advanced Encryption Standard it determines a symmetric-key algorithm (private key). In which the plain text can be converted to cipher-text form through which the secured data operation is carried out. It mainly determines security line of encryption against attackers and unauthorized users. Data will be encrypted while being stored in the cloud to prevent cloud providers from accessing or tampering the data. Also, data will be encrypted while being transferred between entities in the system or while being stored in some temporary locations. In the POV scheme AES algorithm is been deployed & its features include:

- **Security:** Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.
- **Cost:** Intended to be released on a global, non-exclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- **Implementation:** Algorithm and implementation characteristics to be evaluated included the flexibility and suitability of the algorithm which is to be implemented in hardware or software and overall, the relative simplicity of implementation.

3.2 SHA-256

It stands for Secure Hash Algorithm. It converts the message to a unique representation of the message that is a multiple of 512 bits in length, hence without loss of information about its exact original length in bits, the SHA-256 works well with AES algorithm. A hash is not encryption it cannot be decrypted back to the original. This makes it suitable when it is appropriate to compare hashed versions of texts, as opposed to decrypting the text to obtain the original version. Such applications include hash tables, integrity verification, challenge handshake authentication, digital signatures. It was designed as the algorithm to be used for secure hashing as Digital Signature Standard.

The procedure is used to send a non-secret but signed message from sender to receiver. In such a case following steps are followed:

- Sender feeds a plaintext message into the SHA-l algorithm and obtains a 160-bit SHA-l hash.
- Sender then signs the hash with his ASA private key and sends both the plaintext message and the signed hash to the receiver.
- After receiving the message, the receiver computes the SHA-l hash himself and also applies the sender's public key to the signed hash to obtain the original hash H.

3.3 Sequence diagram

It determines the graphical representation of different elements of the system analysis through which its interaction and behaviour can be determined. It mainly determines the operation between data owner, end - user and cloud server during file transaction. Consider the POV scheme operation as shown below:

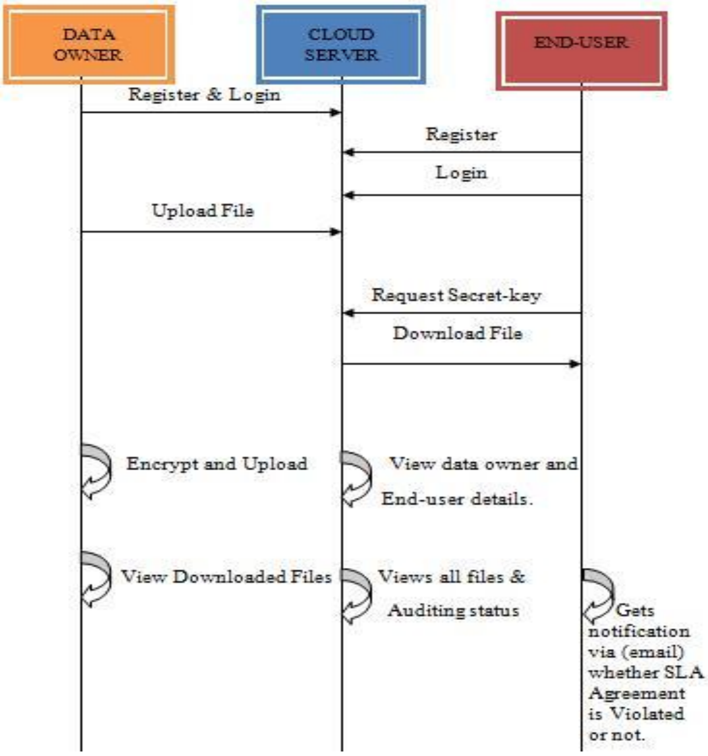
DATA OWNER
CLOUD SERVER
END-USER
Register & Login
Register
Login
Upload File
Request Secret-key
Download File
Encrypt and Upload
View data owner and End-user details.
View Downloaded Files
Views all files & Auditing status
Gets notification via (email) whether SLA Agreement is Violated or not.

Fig -2: Sequence diagram

CONCLUSION

It is important to have a scheme that can audit consistency of files stored on cloud storage. The clients and service providers should both agree on the result of auditing and obey to the agreement on SLAs. However, there is no existing mechanism supported by the existing service providers. Clients may lose their protection on files. To solve the problem, a new scheme is developed in which clients can use it to check the violation on files and prove the violation to service providers at any time through the cloud server. It is called as Real-time Prove of Violation scheme. Using which cloud security is enabled for each file operation in which the efficiency is increased and twice the maximum time is reduced through file operations in cloud storage system.

ACKNOWLEDGEMENT

I take this opportunity to extend my earnest gratitude to my college SJB Institute of Technology and my guide Mrs. Divyashree J, & finally to my parents and all my friends who have directly or indirectly supported me throughout this research.

REFERENCES

[1]. https://www.google.com

[2]. Gwan-Hwan Hwang and Hung-Fu Chen "Efficient real-time Auditing and Proof of Violation in Cloud Storage Systems" *The 6th IEEE International Conference on Cloud Computing Technology and Science*, November 2016.

[3]. KS Suneel, DHS Guruprasad "A novel scheme for SLA Compliance monitoring in cloud computing" *The International Journal of Innovative Research in Advanced Engineering (IJIRAE) vol-2,* February 2015.

[4]. R.A. Popa and J.R. Lorch. "Enabling Security in Cloud Storage SLAs with CloudProof*," USENIX Annual Technical Conference (USENIX),* pp.31-32, January 2011.

[5]. Gwan-Hwan Hwang, Wei-Sian Huang, and Jenn-Zjone Peng, "Realtime Proof of Violation for Cloud Storage," *The 6th IEEE International Conference on Cloud Computing Technology and Science*, pp. 27-29, December 2014.