International Journal of Engineering & Technology, 7 (2.32) (2018) 68-70

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enhance Data Integrity For Data Storage In Cloud Computing

Maddhukuri.Shiva Krishna, Sravani.D, Anjana Triveda.B

Department of Computer Science, K L E F, Vijayawada, Andhra Pradesh, India.

Abstract

In this paper, a well secured and effective AES based framework is proposed for proposed for evaluating individual records put away at the untrusted server. The gadget guarantees the of certainties respectability and accessibility. The gadget bolsters open reviewing with the guide of using TPA and privateness holding by a method for not releasing the data to TPA amid trustworthiness check system. Through regular respectability checking, the machine guarantees records ownership at a remote server.

Keywords: *Data Security, Data integrity, Advance encryption standard (AES), Merkle-Hash Tree, HOMOMORPHIC ALGORITHM.*

1. Introduction

Overcloud information security is a standout amongst that primary issue of information capacity. Customer store information clinched alongside cloud, erase neighborhood duplicate of information Also totally rely on upon cloud server for safety Furthermore maintenance. For guaranteeing customer information auditing may be fundamental. On the beat, this issue of information security propelled encryption Standard(AES) based capacity may be presented. Merkle hash tree may be utilized for Confirmation of record Also integument confirmation. Recuperation framework will be given At whatever point the information is passing or At whatever point those document may be saved In server side is defiled.

2. Existing approaches:

Cloud has become one of the emerging standards which bring the different technologies and computing solutions for internet with different benefits. A large number of storage servers are provided by a cloud which can be accessed anywhere in the cloud at any time. Many of the data outsourcing in cloud facing a large number of security concerns, outsourcing providers like companies that provide data centers and or data center services. Frequent integrity checking is necessary to maintain data safely. In this paper proposed a scheme is of Merkle Hash Tree and AES algorithm to maintain data integrity by untrusted servers or users. To relieve the client burden by not forcing responsibility on the user to verify stored data, Third party auditor is indulged into which acts as a client for data integrity verification and sends a pop-up message to know the status of the data which is stored. The proposed solution also maintains the recovery of data in case of corruption or loss of data. This aims at maintaining the user data is integrated and data is stored in a secure way. When compared with past systems, this system reduces the server computation time.

Merkle-Hash Tree:

1. It is an authenticated structure.
2. When a given set of entries are undamaged or unchanged it will be used as a proof.
3. While the computation of MHT it helps in reducing the server time.
4. To authenticate file blocks some of the cryptographic methods are used.
5. The leaf nodes of the MHT are the hash values of original file blocks.
6. The main aim of MHT is to break the file into a number of blocks.
7. For the original file, blocks apply hashes to authenticate and combine them.
8. And rehash the result hash codes and combine them in a tree like a structure and this procedure is repeated till we get a single root.
9. The client generates the MHT and is stored by both server and client.
10. that tree needs four leaf beet hubs m1, m2,m3 What's more m4. Initially, we apply hash looking into each of these file blocks Furthermore acquire h(m1), h(m2), h(m3) What's more h(m4). Then, h(m1) and h(m2) need aid hashed Also joined together. Comparatively this procedure happens for pieces m3 and m4 and here, we get hb. Here, h will be An secure hash work. This might a chance to be communicated Concerning illustration. Ha = h(h(m1)|| h(m2)) Also hb = h(h(m3)|| h(m4)). Further, ha What's more hb need aid joined What's more rehashed will get the root Concerning illustration hr. This camwood is communicated Similarly as hr= h(ha|| hb).

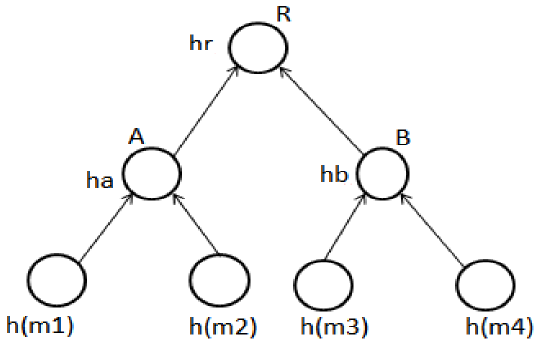


Figure 1: Merkle-Hash Tree

3. Third Party Auditor:

1. The Third Party Auditor is a model that acts as on behalf of the client.
2. It has various efficient operations that a client does not have.
3. They reduce the load of the work of the client by handling the work of integrity verification, the client need not verify the data in a server on its own.

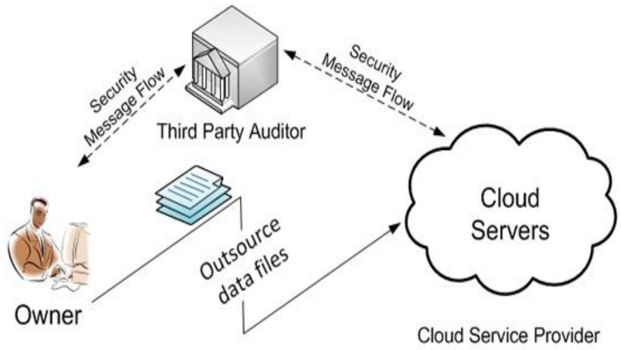


Figure 2: Third Party Auditor

Figure 2 above shows the storage architecture of cloud which consists of Owner, Cloud service provider, and Third-party auditor. A cloud service provider provides the storage server where the client stores the data. The third-party auditor verifies frequently the client's data and integrates the data and sends security alert messages to the client.

4. Advanced Encryption Standard (AES):

Propelled encryption standard (AES):. This recommended model may be utilized fundamentally for accomplishing information integument. So, to enhance information integument two encryption calculations need aid utilized to each information transaction transfer What's more download:

1. ElGamal.
2. Sha-2.

Elgamal algorithm may be used to scramble that information for customers which will be setting off to store in the cloud.

Sha-2 will be utilized for encrypting those keys just.

For further build Previously, information integrity, we concentrate on four principle parts they would.
1.Customer provision machine: this mostly keeps tabs around a trusted neighborhood machine, which speaks to the execution of calculations utilized to accomplishing information integument confirmation.

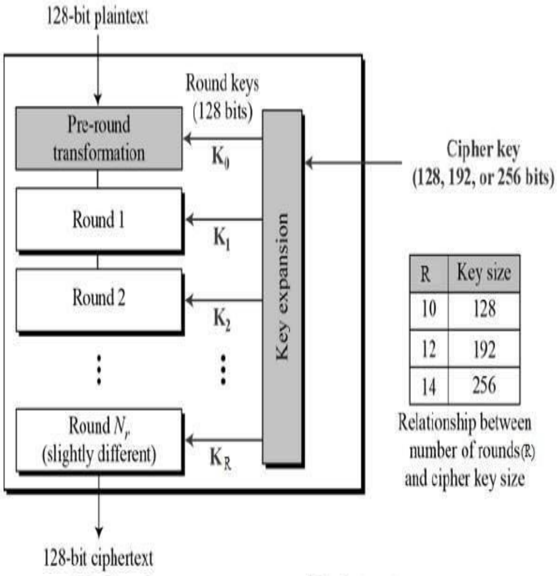
2. Key: in this those fact that saved on the neighborhood machine as said to start with part Furthermore when that information is downloaded we compelling reason to match these both way. Currently though the nearby enter What's more produced way matches, we might say that the information may be secured.

3. Integument checking: checking for those integument of the information which will be saved for the cloud.

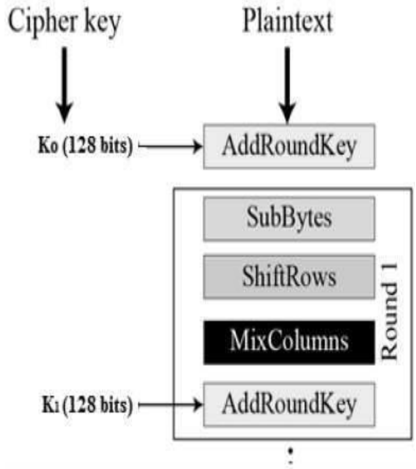
4. Virtual cloud environment: cloud sim, is An kind of instrument steel to the cloud, used to make the virtual cloud nature's domain.

In order should secure the information for expanding technologies, we need two sorts of techniques:
1. Information Hideyo no guchi architecture: with ensure the information protected from attackers or thefts, information will be encrypted utilizing a standout amongst the most recent calculation known as ElGamal which may be utilized When sending the information to cloud earth.

2. Keeping up that integument about data: keeping up for integument will be carried out utilizing hash codes. Those hash codes are matched toward the client limit and the server conclusion which serves to guarantee the integument for information.



R	Key size
10	128
12	192
14	256



Advantages:

1. The main advantage is it is believed to be resistant to quantum computer algorithms.

2. This hash trees could be used to check any sort of information stored, took care of What's more exchanged done What's more between Pcs.
3. Fundamental utilization of those hash trees is on verify that information obstructs gained starting with different associates in a companion with companion system are accepted undamaged Furthermore actually should weigh that the opposite companions don't lie a send fake bocks.
4. Utilized within ipfs,btrfs Furthermore zfs document systems, bit torrent protocol, data protocol, apache wave protocol. Also used in MySQL systems like Apache, Cassandra, risk, and dynamo.

Disadvantages:

1. It is stateful.
2. It also uses collision resistant hash functions how to construct the crhf from specific assumptions such as the hardness of factoring.
3. A number of messages to be known in advance which are to be signed.
4. Length of the secret key is too long which is proportional to a number of messages signed.

5. AES Algorithm:

Advantages:

1. AES is more secure.
2. The AES supports larger key sizes than 112 or 168 bits.
3. This is faster in both software and hardware.
4. AES 128 bit block size makes it less open to attacks via the birthday problem.
5. Many latest US and international standards use this AES algorithm.

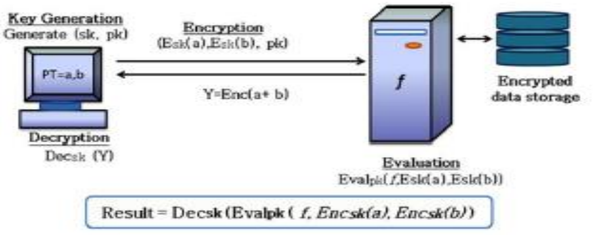
Disadvantages:

1. It needs more processing. It requires more rounds of communication when compared to DES.
2. High efficiency, not complex.

6. Techniques To Be Added:

Homomorphic Algorithm:

It is an encryption algorithm, operations utilized looking into encrypted information. This algorithm may be utilized Eventually Tom's perusing utilizing Different general population magic calculations. At whatever point the information will be exchanged of the state-funded area, there would Numerous calculations with secure the operations What's more stockpiling of information. Mostly the homomorphic calculations are utilized for preserving security. In this, we have four capacities basically way generation, encryption, decryption, assessment. For way era customer will produce a one set of keys government funded way Furthermore mystery way to the encryption about plain quick. Utilizing mystery magic customer will scramble Also produce those CIO content which may be once more sent to the server. The server needs An work f for assessing this CIO content. Created CIO content will once more employments those mysteries enter for decrypting Furthermore returns once again that unique outcome. The steps took in this algorithm may be Concerning illustration quell as takes after:



Security is the primary requirement because the cyber crimes are increasing nowadays.Today the public environment is needed for securing the preserving data.There are many private environments but it is expensive than public area.Hence everyone is convenient for storing the data in the cloud that is the internet.So using this homomorphic algorithm we can overcome the cyber crimes and by encrypting the data we are yet to preserve the data securely or safely from hackers or stealers.the main idea in proposing this algorithm is taking the operations that are to be performed and then encrypting the data in order to process the required results and also decrypting the required results which are to be resulted and analysed.so, using homomorphic algorithm we can achieve ate the good data preserving and security for the future purpose.

7. Suggestions to Overcome:

In this paper, we talked about over privacy-preserving state-funded auditing framework to information capacity security Previously, Cloud Computing, the place TPA can perform those stockpiling auditing without requesting those nearby duplicate for information. We use those homomorphic authenticator Furthermore random mask strategy will surety that TPA might not gain any knowledge something like the information substance saved on the cloud server during the productive auditing process, which not best dispenses with those burden of cloud client starting with those repetitively Furthermore conceivably unreasonable auditing task, as well as alleviates those users' dread of their outsourced data leakage. Recognizing TPA might simultaneously handle different audit sessions from distinctive clients for their outsourced information files, we further augment our privacy-preserving open auditing protocol into a multi-user setting, the place TPA camwood perform those different auditing tasks done a clumping manner, i. E., all the while. Broad security and execution dissection indicates that those recommended schemes are probably secure and profoundly effective. We trust constantly on these advantages of the recommended schemes will shed light on economies of scale to cloud registering.

References:

[1] http://www.iosrjournals.org/iosr-jce/papers/Vol19-issue3/Version-5/E1903052327.pdf

[2] http://paper.ijcsns.org/07_book/201506/20150615.pdf

[3] http://ceur-ws.org/Vol-1366/paper13.pdf

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

[5] Data and infrastructure security auditing in cloud computing environments by Hassan Rasheed of Taif University Deanship of Information Technology, Saudi Arabia.

[6] Improving Data Integrity for Data Storage Security in Cloud Computing by Poonam M. Pardeshi, Prof. Bharat Tidke University of Pune, Flora Institute of Technology, Pune, Maharashtra, India