ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Improved Data Integrity and Storage Security in Cloud Computing

P Nageswara Rao[1], Dr. K.Venkatesh Sharma[2]

Research scholar, Shri Venkateshwara University, UP, India[1]

Associate Professor, Dept of CSE, Shri Venkateshwara University, UP, India[2]

ABSTRACT: In this paper, a well secured and useful AES based framework is 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. 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 entirely 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.

KEYWORDS: Advanced Encryption Standard (AES), TPA, Cloud Computing.

I. INTRODUCTION

Cloud Computing pays vital role since from last 10years. Cloud empowers the storage of a few categories of data. Cloud is very versatile with regards to wide-ranging data and can give never-ending record-keeping resources on request... Clients can utilize cloud services with no establishment, and the data transferred on the cloud is open from any side of the world, all it should be gotten to is a PC with dynamic web association on it. The clients can buy in outstanding services of data and programming which lives exclusively on the remote servers and appreciate the arrangement of the on-request arrangement of services. As adjustable assuming assets and a colossal measure of storage space are given by Internet-based online services, the move to online storage has contributed extraordinarily in distributing out the overhead of neighborhood machines in storage and upkeep of data. The cloud gives a few advantages, for example, adaptability, calamity recuperation, pay-per-utilize and simple to access and utilize the model which adds to the explanation behind moving into the cloud.

An immense measure of clients store their noteworthy data in the cloud without keeping a solitary duplicate of this data in their neighborhood PCs. In this way, cloud helps free up space on the nearby plate, consequently likewise called 'A Hard-circle in the sky.' Even however monstrous favorable circumstances are offered by the cloud, a part of security concerns still exist in it. The most troubling concern is its storage security. A large portion of the circumstances, the client does not keep up any duplicate of outsourced data in their neighborhood framework. The inquiry with respect to data security ends up plainly vital with regards to classified data. The respectability of the data must be viewed genuinely to pick up client trust and fulfillment.

Be that as it may, keeping up security is a testing errand. Imagine a scenario in which the storage server itself isn't dependable. For instance, the server or the Cloud Service Provider (CSP) may erase some less as often as possible got to data to spare the storage space. It might likewise endeavor to conceal blunders if there should arise an occurrence of

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Secretiveimperfections to keep up their bad reputation. Hence, despite the fact that outsourcing data into the cloud may look monetarily appealing, the data honesty and accessibility factor may hinder its appropriation by clients.

The client must have the learning whether his/her data is secured. The client should be persuaded in regards to the security of remotely put away data. Nonetheless, it isn't doable for the client himself to check his data. There exist numerous frameworks that have attempted to take care of the issue of data honesty. The inspecting can be performed in two ways viz. Private and Public. In Private Auditability, the client is in charge of confirming the data. Nobody else with the exception of the client can scrutinize the server in regards to the data respectability, though, Public Auditability is more helpful and favored over Private Auditability since it enables a third party to perform trustworthiness check in the interest of the client. The client isn't exclusively in charge of it, thus it to a great extent diminishes client's weight.

We refer this third party as the Third Party Auditor (TPA).The other imperative piece in keeping up client data in the cloud is the reestablish framework. If under some offensive circumstance, the trustworthiness of data is lost, eventually Cloud Service Provider is in charge of it, and there ought to be some arrangement to recuperate the circumstance. This is on the grounds that what a client needs is his/her data in unique its shape regardless of what issue happened at the server. Thinking about this reality, the proposed framework is furnished with a recuperation framework which stores a reinforcement of the client data. This adds to the accessibility of data whenever.

II. REVIEW OF LITERATURE

[8] Homomorphic encryption has long been acclaimed solution for data security and privacy problems in cloud computing. However, the high complexities of operations associated with the existing schemes have prohibited them from being used for practical applications. In this paper we propose a new protocol for verifying the integrity of the data stored at the remote cloud server, based on a practical version of integers based homomorphic encryption. The proposal is the first attempt in combining the data integrity and confidentiality in new ways to provide an impending solution.

[7] With the increasing popularity of cloud computing, privacy has become one of the key problem in cloud security. When data is outsourced to the cloud, for data owners, they need to ensure the security of their privacy; for cloud service providers, they need some information of the data to provide high QoS services; and for authorized users, they need to access to the true value of data. The existing privacy-preserving methods can't meet all the needs of the three parties at the same time. To address this issue, we propose a retrievable data perturbation method and use it in the privacy-preserving in data outsourcing in cloud computing.

[9] Cloud computing offers a new way of services and has become a popular service platform. Storing user data at a cloud data center greatly releases storage burden of user devices and brings access convenience. Due to distrust in cloud service providers, users generally store their crucial data in an encrypted form. But in many cases, the data need to be accessed by other entities for fulfilling an expected service, e.g., an eHealth service. How to control personal data access at cloud is a critical issue. Various application scenarios request flexible control on cloud data access based on data owner policies and application demands. Either data owners or some trusted third parties or both should flexibly participate in this control.

[10] Cloud computing is a rapidly growing model of computation. It is the delivery of computing services by shared resources, software and information over the network (Internet or Intranet). It allows user to store large amount of data in cloud storage and use as when required from any part of the world by networks. Cloud computing is network based technology since security issues like privacy, data security, confidentiality etc. are encountered.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

[11] In cloud computing, the sensitive data are required to be encrypted before being outsourced to the server, which introduce a heavy computation overhead for key derivation and data management when dynamic hierarchical access control is desired. In this paper, we address this challenging problem by delegating the computation intensive task, such as data re-encryption, key distribution and derivation to cloud servers. Only bilinear pairing and random padding are used in our construction. Extensive analysis shows that the proposed scheme achieves scalability and dynamic simultaneously, and is proved to be secure formally.

III. PRESENTED SYSTEM

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 securely. When compared with past systems, this system reduces the server computation time.

Merkle-Hash Tree:

- It is an authenticated structure.
- When a given set of entries are undamaged or unchanged, it will be used as a proof.
- While the computation of MHT it helps in reducing the server time.
- To authenticate file blocks some of the cryptographic methods are used.
- The leaf nodes of the MHT are the hash values of original file blocks.
- The main aim of MHT is to break the file intosome blocks.
- For the original file, blocks apply hashes to authenticate and combine them.
- 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.
- The client generates the MHT and is stored by both server and client.
- Thattreeneeds four leaf beet hubs m1, m2,m3 What's more m4. Initially, we apply hash looking into each of these fileblocks 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, andhere, we get hb. Here, h will be An secure hash work. This might be 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).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

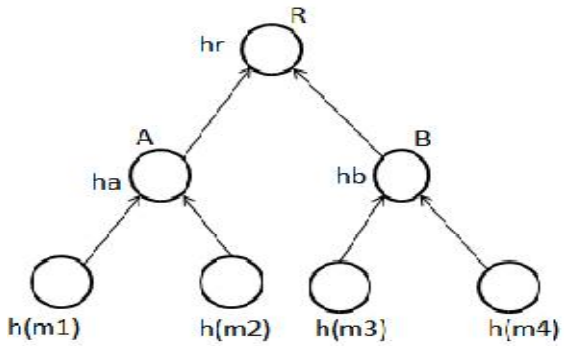


Figure 1: MERKLE-HASH TREE

Third Party Auditor:

- The Third Party Auditor is a model that acts as on behalf of the client.
- It has various efficient operations that a client does not have.
- Theyreduce theload of the work of the client by handling the work of integrity verification; theclient need not verify the data in aserver on its own.

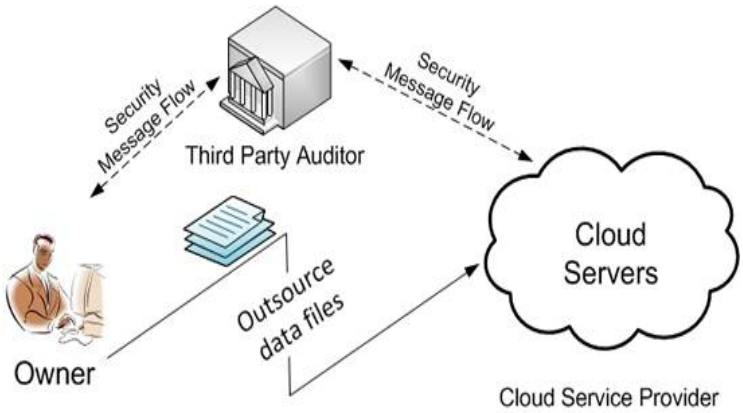


Figure 2: THIRD PARTY AUDITOR

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 frequently verifies the client's data and integrates the data and sends security alert messages to the client.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

IV. 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 who 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 thecloud.

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

Inorder should secure the information for expanding technologies,we need two sorts of techniques:

1. Information Hideyo nosuch 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 integumentabout 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.

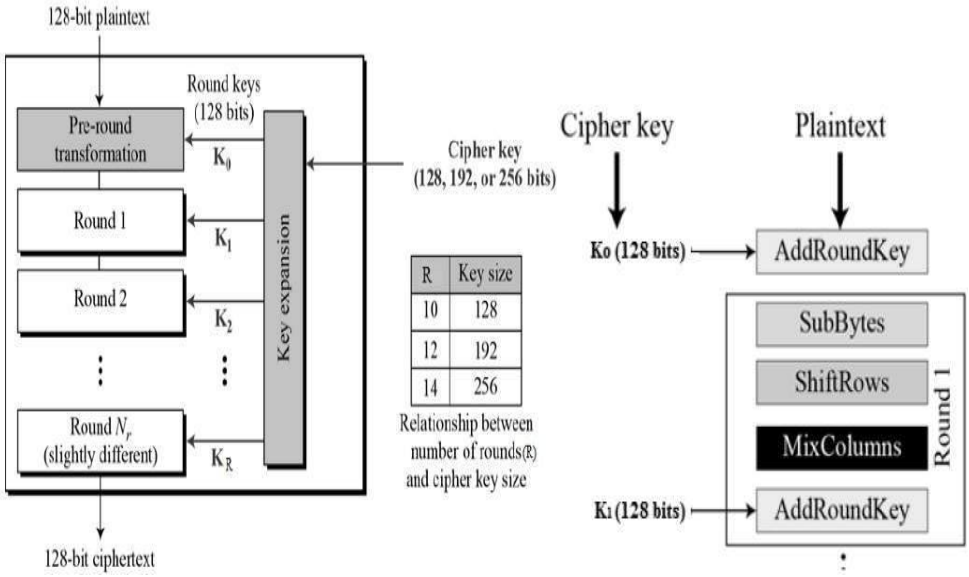
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017



ADVANTAGES:

MERKEL HASH TREE:

ADVANTAGES:

- The main advantage is it is believed to be resistant to quantum computer algorithms.
- This hash trees could be used to check any information stored, took care of What's more exchanged done What's more between Pcs.
- 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.
- Utilized within ipfs,btrfs Furthermore zfs document systems, bit torrent protocol, dataprotocol, apache wave protocol. Also used in MySQL systems like Apache,Cassandra,risk,and dynamo.

DISADVANTAGES:

- It is stateful.
- It also uses collision resistant hash functions how to construct the craft from specific assumptions such as thehardness of factoring.
- Some messages to be known in advance which are to be signed.
- Length of thesecret key is too long which is proportional tosome messages signed.

AES ALGORITHM:

ADVANTAGES:

- AES is more secure.
- The AES supports larger key sizes than 112 or 168 bits.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

- This is faster in both software and hardware.
- AES 128 bit block size makes it less open to attacks via the birthday problem.
- Many latest US and international standards use this AES algorithm.

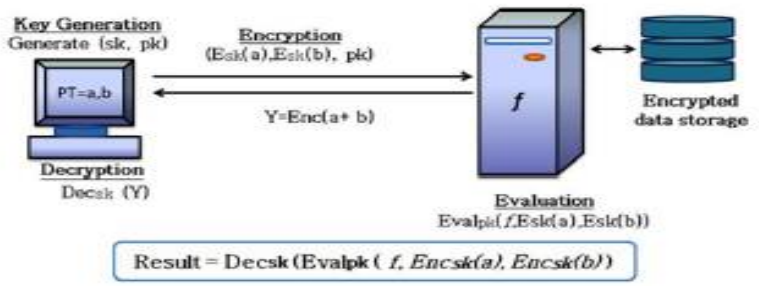
DISADVANTAGES:

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

V. 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 make numerous calculations to secure the operations What's more stockpiling of information. Mostly the Homomorphic calculations are utilized for preserving security. In this, we have four capacities 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 theserver. The serverneeds 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 inorder to process the required results and also decrypting the required results which areto be resulted and analysed.so,using homomorphic algorithm we can achieve ate the good data preserving and security for the future purpose.

VI. CONCLUSION

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

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 efficient. We continually trust on these advantages of the supported systems 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 computingenvironments by Hassan Rasheed of Taif University Deanship of Information Technology, Saudi Arabia.
6. Improving Data Integrity for Data Storage Securityin Cloud Computing by Poonam M. Pardeshi, Prof. Bharat TidkeUniversity of Pune, Flora Institute of Technology, Pune, Maharashtra, India.
7. Pan Yang; et.al 2014, "A retrievable data perturbation method used in privacy-preserving in cloud computing", **ISSN:** 1673-5447, Volume: 11, Issue: 8, Pp: 73 – 84.
8. Y. Govinda Ramaiah; G. Vijaya Kumari,2013, "Complete Privacy Preserving Auditing for Data Integrity in Cloud Computing", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp: 1559 – 1566.
9. Zheng Yan; et.al 2017, "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing", **ISSN:** 2168-7161, Volume: 5, Issue: 3, pp: 485 – 498.
10. Ran Yang; et.al 2012, "Enforcing scalable and dynamic hierarchical access control in cloud computing", IEEE International Conference on Communications (ICC), pp: 923 – 927.