# Enhanced public auditability & secure data storage in cloud through a novel third party auditor (Tpa)

**Anbarasu V***
Dept of IT, Jeppiaar Engineering College
***Corresponding author: E-Mail:anbarasukv@gmail.com**

## ABSTRACT

Cloud computing will be a web built registering model that empowers helpful also ahead request organize get to an imparted pool of configurable registering assets. It gives different sorts of benefits. Information managers could remotely store their information in the cloud. The information manager might depend on an outsider evaluator (TPA) to the information auditing errand. Owners can post challenges to the TPA to verify data integrity. The TPA should be able to efficiently audit the cloud data storage without local copy of data and without any additional online burden for data owners. TPA uses a data structure called MERKLE HASH TREE and an authentication technique namely homomorphic authentication technique. Since TPA handles both the maintenance of data and auditioning of data, there is a chance that TPA can behave as a rogue administrator. The existing system assumes that the TPA, who is in the business of auditing, is reliable and independent. The objective of this paper is to distribute privacy protection and auditioning as loosely coupled cloud services, to enable the verifiability of TPAs trustworthiness.

**KEY WORDS:** TPA, MHT, Data owners, homomorphic authentication.

## 1. INTRODUCTION

Cloud computing is a comprehensive solution that delivers IT as a service. It will be an Internet-based registering result the place imparted assets would furnished in power dispersed on the electrical grid. Pcs in the cloud need aid arranged should worth of effort together and the Different provisions utilize the aggregate registering force Concerning illustration if they need aid running with respect to An solitary framework. Those adaptability about cloud registering may be a work of the allotment from claiming assets for interest.

This facilitates the utilization of the system's combined resources, negating those requirement should relegate particular fittings to an undertaking. In the recent past cloud computing, sites also server-based requisitions were executed on a particular framework. With the coming for cloud computing, assets are utilized as a total apples and oranges virtual workstation.

Inasmuch as those web gives open entry should huge numbers Web-based IT resources, a cloud may be normally privately possessed Also offers entry to it assets that is metered. Associations utilize the cloud clinched alongside an assortment of diverse administration models (SaaS, PaaS, IaaS) Also organization models (Private, Public, Hybrid). There is An number of security issues connected with cloud registering Anyway these issues fall into two wide categories: (i) Security issues confronted Toward cloud suppliers (ii) Security issues confronted by their clients in A large portion cases, the supplier must guarantee that their base will be secure and that their client's information What's more provisions would secured same time the client must guarantee that those supplier need taken the best possible efforts to establish safety should ensure their data.

Cloud privacy & techniques to ensure it have started to evolve in recent years. Third party auditioning is one of the important things among them (Cong Wang, 2010). Rogue Administrator- new challenge (Deyan Chen, 2012). An attack often posited by this insider is theft of sensitive information, resulting in loss of data confidentiality and/or integrity. Life cycle of data's privacy has also been a point of motivation (Shuai Han, 2011). To decentralize privacy protection and verifiability, to avoid single source of authentication since the design TPA undergoes single source of authentication (Cong Wang, 2010). Usage of cloud services is the cutting edge technology to utilize various services over internet. These things had motivated us to propose a system to solve rogue administrator problem in privacy related issues of cloud.

**Problem Statement:** TPA which acts as a centralized entity constructs MHT out of user's data and audits them using homomorphic authentication technique. TPA also ensures that users privacy is protected or not (Sowmya, 2013; CongWang, 2010). There are many threats found inside the cloud. Rogue administrator is one among the recently identified insider threat. In this work, we are decentralizing the maintenance of privacy protection and privacy auditioning as two different cloud services assigned to distribute TPAs.

**Existing System:** There are several techniques available in the existing system. But none of the existing system deals with rouge TPA. Every framework needs its identity or favorable circumstances Also restrictions. Some of the existing frameworks would examine underneath. Merkle hash tree to cryptography furthermore PC science and hash tree or Merkle tree (Qian Wang, 2011; Wang, 2010; Sowmya, 2013; CongWang, 2010; Rosaria Gennaro, 2012; William R Claycomb, 2012) is a tree over which each non-leaf hub will be marked for those hash of the labels of its Youngsters hubs. Hash trees are helpful in light they permit proficient and secure confirmation of the substance of bigger information structures.

**An Merkle hash tree (MHT)**: may be An great contemplated Confirmation structure, which will be planned should proficiently What's more safely demonstrate that An situated for components would undamaged Also unalterably. It will be constructed similarly as a double tree the place the abandons in the MHT need aid the hashes about bona fide information qualities. MHT may be regularly utilized with validate the values from claiming information squares.

**Homomorphic authenticatication:** Cong Wang (2010), Rosaria Gennaro (2012), would exceptional confirmation about metadata produced starting with unique information blocks, which might a chance to be safely total apples and oranges to such an approach on guarantee TPA that a straight blending from claiming information squares may be effectively registered by checking just the total apples and oranges authenticator. In this plan anybody camwood perform discretionary computations in those verified information Furthermore transform an short tag that authenticates the bring about shortages of the calculation. Those clients verifies this tag with her private magic to guarantee that the guaranteed bring about shortages will be In fact those right yield of the specified calculation again formerly verified information without expecting on think the underlying information itself.

A fully homomorphic algorithm is a quadruple of probabilistic polynomial time algorithms

HE= (HE.KeyGen,HE.Enc,HE.Dec,HE.Eval) defined as HE.KeyGen(1n)- (pk,evk, sk): Outputs a public encryption key

pk, a public evaluation key evk and a secret decryption key sk.

HE.Encpk(b) - c: Encrypts a bit b under public key pk. Outputs ciphertext c.

HE.Decsk(c) - b: Decrypts ciphertext c using sk to a plaintext bit b.

HE.Evalevk(g, c1, .. , ct) -c: The deterministic evaluation algorithm takes the evaluation key evk, a set of t ciphertexts c1,,

ct. It outputs the result ciphertext c.

Clump Auditing as cloud servers might simultaneously handle different confirmation sessions from separate clients, provided for k marks for Kdistinct information files starting with k clients, it may be additional invaluable on aggravator know these marks under An solitary short one and verify it at one time.

For those station from claiming privacy-preserving state funded auditing done cloud Computing, TPA might simultaneously handle different auditing (Qian Wang, 2011; Wang, 2010; CongWang, 2010) delegations upon diverse clients solicitations. Those single person auditing about these assignments to TPA could be dully What's more exact wasteful. A clump auditing not best permit TPA on perform the different auditing errands simultaneously, as well as incredibly diminishes those calculation cosset on the TPA side.

**Multi Writer Model:** Cloud data storage not only provides dynamic and scalable storage services, but also allows easy on-demand file sharing. A difficult problem is support for services with legacy users, who may not only access but also modify the owner’s data in the cloud. Under this, there are two types of forgeries namely (Sowmya, 2013; CongWang, 2010).

**Type 1 Forgery:** Even when the legitimate user modifies the data, it falls under Type 1 forgery.

**Type 2 Forgery:** When a certain data has been authenticated using a particular program P and when we again try to authenticate the same program using some other program using P1. It will be reported as Type 2 Forgery. This model solves one of the forgeries discussed here.

**Encryption Techniques Used By TPA:** a) RSA (Rivest-Shamir-Adleman) (Tamal Kanti Chakraborty, 2013; William R Claycomb, 2012), Each user is allocated a pair of keys which are necessary for the cloud access control .For each data file, users add a message header before sending it to cloud. RSA is used to encrypt the data packet with the allocated keys.

b) Elliptic curve cryptography (ECC) (Veerraju Gampala, 2012; Tamal Kanti Chakraborty, 2013; William R Claycomb, 2012), Elliptic curve cryptography [ECC] is a public-key cryptosystem. Every user has a public and a private key. Public key is used for encryption / signature verification. Private Key is used for decryption/signature generation.

The Elliptic curve cryptography (ECC) is proposed to ensure the data integrity, confidentiality and authentication of data between clouds and also on the remote server. The scheme implements the concepts of the provable data possession (PDP) to make the data operations dynamic. The presence of data can be checked out by challenging the server using the proof of retrievability (PoR) scheme.

**Data Coloring and Watermarking:** Data coloring is the process of changing original input of RGB color image file into a gray scale image file and Water marking is the process of adding the user text behind of image files. In this system they have used, both data coloring and water marking process (Ushadevi, 2012), in order to store the data or image in the cloud server by assigning the public key, and this key and watermarking and data coloring images are send to third party and third party have full authority to check the key and send it to the server. Third Party Auditor must have public key whenever the data must be retrieve. In the watermarking process, the security level is high so the data or images cannot be identified by the attackers in the cloud. These techniques are used to protect shared data objects and software modules and also safeguard multiway authentications and tighten the access control for sensitive data.

From existing system, Data owners should be able to use cloud storage, without worrying about the need to verify its integrity. With completely guarantee information security and save information owner’s calculation resources, there must make publicly auditable cloud stockpiling services, the place information owners might depend on an outer outsider evaluator (TPA) should check the outsourced information At required. Outsider auditing gives a transparent yet expense profit investigation strategy to making trust between information holder Furthermore cloud servers.

Based on the audit result from a TPA, the released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform.

**Proposed System:** The aim of this work is to Decentralize TPA s functionalities as loosely coupled cloud service as Privacy Protection as a Service (PPaaS) and Privacy Auditioning as a Service (PAaaS). Actors involved in the proposed system are:

1. Data owner
2. Users
3. Cloud storage 1
4. Cloud storage 2
5. TPA 1
6. TPA 2

The architecture of the proposed system is shown in Figure 2.

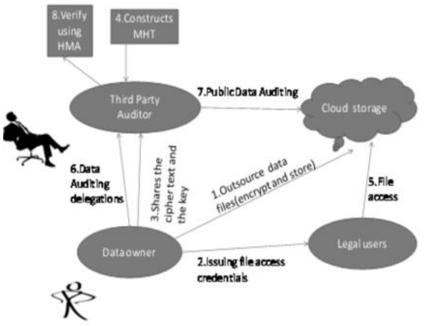

8.Verify using HMA
4.Constructs MHT
Third Party Auditor
7.PublicData Auditing
Cloud storage
6.Data Auditing delegations
3.Shares the cipher text and the key
1.Outsource data files(encrypt and store)
5.File access
Dataowner
2.Issuing file access credentials
Legal users

**Figure.1. Existing system**

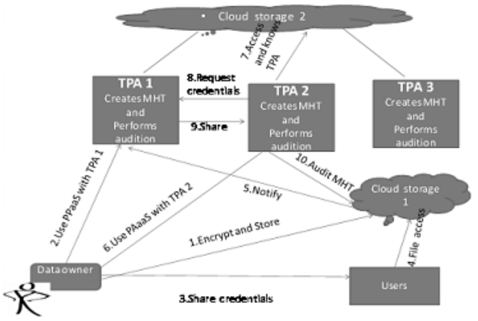


**Figure.2. Proposed Architecture system**

**Merkle Hash Tree:** It is constructed similarly as a double tree the place the abandons in the MHT would the hashes from claiming bona fide information values. MHT is regularly utilized on validate those qualities from claiming information obstructs. The thought of the outsider evaluator is with check Also change those information around sake of the customer. Information stockpiling may be finished utilizing a Merkle hash tree (MHT) accomplishing speedier information entry.

**Privacy Protection and Audition as Cloud Services:** The implementation consists of five steps, namely

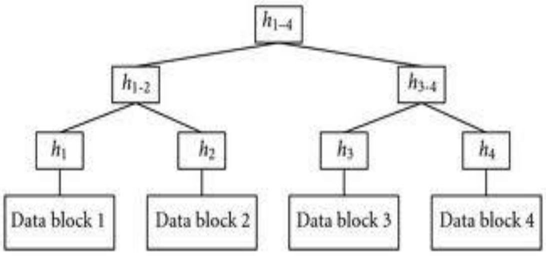
1. Setting TPA to store and retrieve.
2. PPaaS on local application server.(Privacy Protection As A Service)
3. PAaaS on local application server.(Privacy Auditioning As A service)
4. Migrating the above two services to cloud and testing them.
5. Intrusion of rogue administrator and identifying false TPA.

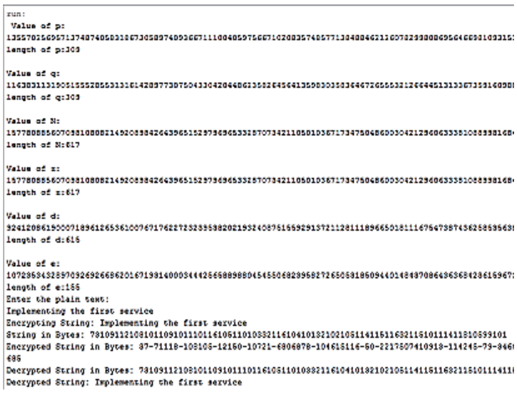
**Steps Involved In Creating And Running An Application Client:** Those to start with step will be should make endeavor provisions that hold a basic session bean furthermore a java class library undertaking that holds a remote interface for the session bean. Then create an application client that accesses the session bean through the remote interface in the class library. The class library JAR that contains the remote interface is added to the classpath of the enterprise application and the application client.

(i) Creating the Java Class Library
(ii) Creating an EJB Module
(iii) Creating the Session Bean
(iv) Adding a Business Method
(v) Deploying the Enterprise Application
(vi) Creating the Application Client
(vii) Adding the Class Library
(viii) Running the Application Client

**Methods of Algorithm on Oracle Weblogic Server:** RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. RSA includes a government funded enter Also a private magic. People in general magic could make referred to by Everybody Also will be utilized to encrypting messages. Messages encrypted with people in general enter might main a chance to be decrypted utilizing the private enter. The keys for the RSA algorithm are produced the emulating way:

Step 1. Pick two unique prime numbers p and q.
Step 2. Figure n = pq. N is utilized as the modulus to both people in general furthermore private keys. Its length, usually expressed in bits, is the key length.
Step 3.Compute (n) = (p)(q) = (p 1)(q 1), where is Euler's totient function.
Step 4.Choose an integer e such that 1 ¡ e ¡ (n) and gcd(e, (n)) = 1; that is e and (n) are coprime.
Step 5.Determine d such that d is the multiplicative inverse of e(modulo (n)).
Step 6.d is kept as the private key exponent.



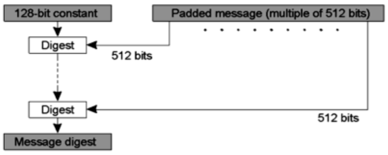


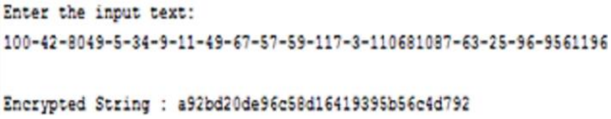
```
run:
 Value of p:
1355702569571374074050318673058974093667111004059756671020835748577138408462116078233800695646698103315
length of p:309

Value of q:
11630311319051555285531316142897730750433042044862358264564135983035836467265553212664451313367355160508
length of q:309

Value of N:
1577808856070581080821452085842643965152979696533257073421105010367173475048600304212960633351088398168
length of N:617

Value of z:
1577808856070581080821452085842643965152979696533257073421105010367173475048600304212960633351088398168
length of z:617

Value of d:
924120861950071896126536100767176227232895382021932408751669291372112811189665018111676473874362585856
length of d:616

Value of e:
1072863432897092692668620167193140003444256688988045455068289682726505818609440148487086436368428616967
length of e:155
Enter the plain text:
Implementing the first service
Encrypting String: Implementing the first service
String in Bytes: 7310911210810110910111011610511010332116104101321021051141151163211610111411810599101
Encrypted String in Bytes: 87-71118-108106-12160-10721-6806878-104615116-60-2217507410918-114245-79-846
686
Decrypted String in Bytes: 7310911210810110910111011610511010332116104101321021051141151163211610111411
Decrypted String: Implementing the first service
```

**Figure.3.Merkle Hash Tree** **Figure.4. Result after encryption and decryption**

**Implementing Md5 Algorithm On Oracle Weblogic Server:** Those MD5 message-digest algorithm will be a broadly utilized cryptographic hash capacity generating a 128-bit (16-byte) hash value, commonly communicated as a 32 digit hexadecanoic corrosive number. The MD5 calculation will be expected for advanced mark applications, the place an extensive record must a chance to be"compressed" for a secure way.

The steps involved in this algorithm are:
Step 1. Append Padding Bits
Step 2. Append Length
Step 3. Initialize MD Buffer
Step 4. Process Message in 16-Word Blocks
Step 5. MD5 result after encryption is shown in the figure 6.

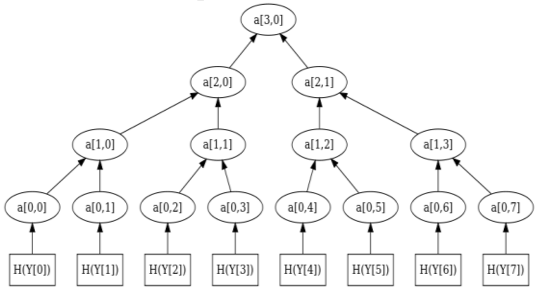


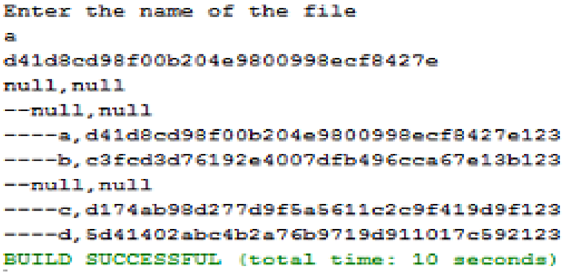


```
Enter the input text:
100-42-8049-5-34-9-11-49-67-57-59-117-3-110681087-63-25-96-9561196

Encrypted String : a92bd20de96c58d16419395b56c4d792
```

**Figure.5. MD5 Algorithm Structure** **Figure.6. Result after encryption**

**Results and Discussion of Merkle Hash Tree on Oracle Weblogic Server:** A Merkle hash tree is a tree of hashes in which the leaves are hashes of data blocks in, for instance, a file or set of files. Nodes further up in the tree are the hashes of their respective children. Hash 0 = hash (hash 0-0—hash 0-1).





```
Enter the name of the file
a
d41d8cd98f00b204e9800998ecf8427e
null,null
--null,null
----a,d41d8cd98f00b204e9800998ecf8427e123
----b,c3fcd3d76192e4007dfb496cca67e13b123
--null,null
----c,d174ab98d277d9f5a5611c2c9f419d9f123
----d,5d41402abc4b2a76b9719d911017c592123
BUILD SUCCESSFUL (total time: 10 seconds)
```

**Figure.7. Structure of MHT** **Figure.8. Result of MHT**

**Metrics Comparisons:**

**Table.1. Metrics**

| | **Exiting System** | **Proposed System** |
|---|---|---|
| Public Verifiability and Privacy Preserving | Yes | Yes |
| No of TPA's Involved | One | Many |
| Computational Approach | Centralized | Distributed |
| Fault TPA's Included | No | Yes |
| Detecting Fault TPA's | No | Yes |
| Measuring TPA's Correctness | No | Yes |
| Levels of Encryption / Decryption for auditing | One | Two |
| No of cloud storage | One (User's data | Two (User's and TPA's data) |
| Data sharing | Data owner to legal users | 1. Data owner to legal users<br>2. TPA to TPA<br>3. Clients to Clients |
| Time complexity | 0(1) (single) | O(1) (Parallel) |

## 2. CONCLUSION

In this paper we actualize the entire cloud capacity security component recommended. This will think as of cloud building design for three gatherings to be specific cloud administration provider, outsider evaluator furthermore cloud customer. Those customers could perform information progress also unable will agent the auditing errand will outsider auditors. The security components permit general population auditability. It does mean that the verification services can be used by all users. The third party auditor is responsible to monitor all transactions for verification of integrity. There are two challenges resolved in this solution. The ability to support multiple verifications at a time and the ability to support on – demand block verification for integrity. These are achieved using bilinear aggregate signature and Merkle Hash Tree respectively. Provide all security features the third party auditor is capable of proving third party auditing services to public. We built a prototype, a custom Java simulator that demonstrates the proof of concept

## REFERENCES

CongWang and Kui Ren andWenjing Lou and Jin Li, Toward Publicly Auditable Secure Cloud Data Storage Services, in IEEE, 2010.

Deyan Chen, Hong Zhao1, Data Security and Privacy Protection Issues in Cloud Computing, International Conference on Computer Science and Electronics Engineering, 2012.

Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud.IEEE Transactions on Parallel and Distributed Systems, 2011.

Rosaria Gennaro and Daniel Wichs, Fully Homomorphic Message Authenticators. in IEEE, 2012.

Shuai Han, Jianchuan Xing, Ensuring data storage security through a novel third party auditor scheme in cloud computing .Proceedings of IEEE CCIS, 2011.

Sowmya B, Shahul Hamead H, Third Party Auditing with Multi-Writer Model.International Journal of Systems, Algorithms &Applications, 3(3), 2013.

Tamal Kanti Chakraborty, Anil Dhami, Prakhar Bansal and Tripti Singh,Enhanced Public Auditability & Secure Data Storage in Cloud Computing,on 2013 3rd IEEE International Advance Computing Conference (IACC), 2013.

Ushadevi R, Rajamani V, A Modified Trusted Cloud Computing Architecture based on Third Party Auditor (TPA) Private Key Mechanism .International Journal of Computer Applications (0975 8887), 58(22), 2012.

Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, Data Security in Cloud Computing with Elliptic Curve Cryptography,International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, 2(3), 2012.

Wang C, Privacy-Preserving Public Auditing for Storage Security in Cloud Computing. Proc, IEEE INFOCOM 10, 2010.

William R Claycomb, Alex Nicoll, Insider Threats to Cloud Computing, Directions for New Research Challenges, IEEE 36th International Conference on Computer Software and Applications, 2012.