

## LOCALITY PARAMETERS FOR PRIVACY PRESERVING PROTOCOL AND DETECTION OF MALICIOUS THIRD PARTY AUDITORS IN CLOUD COMPUTING

<sup>1</sup>K Kishore Kumar, Research scholar,  
JIT University, Jhunjhunu, Rajasthan.

<sup>2</sup>Dr.K Rajendra Prasad, Professor  
CSE Department, Institute of Aeronautical Engineering, Hyderabad

### ABSTRACT:

Cloud computing is an anticipated and an inevitable solution for large storage capacities, virtual presence of ownership and universal accessibility which extends the boundaries of a user today. These benefits also open up a challenge for being too exposed for welcoming attackers to steal potential information from those cloud environments. Irrespective of types of data, information stored on these cloud environments vary from databases to coding of software and raw and processed information of various organisations including governments. To ensure confidentiality and integrity of data input from various users, cloud service providers employ third party auditors to verify the safety measures are intact and maintained. As the name predicts, an auditor may not possess a responsibility to protect the data after their intended verification is over. Third Party Auditors have the function of confirming that the saved data has the same integrity as of original data, does not seek any information in near future to disturb the integrity and finally do not introduce any loopholes for new attacking attempts from external sources. This proposal intends to derive a mechanism to limit the resources provided to third party auditors in the architecture. The location of data and users is protected in this approach along with locking of data segments to enhance the security of the architecture. The simulation results compare the technique and prove that this method outperforms the previous techniques when addressing the sturdiness, communication complexity and time consumption concerns.

Keywords: public auditing, location based privacy preserving, third party auditor (TPA), cloud client (CC), cloud service provider (CSP), security and privacy of storage (SPS), panda public auditing (PPA).

### INTRODUCTION

Enhancing the technological services in storage and computation, many resources are now available to the common man for cheaper and faster rates. These services are preferred more than ever before and technologies are advancing the second we speak. Limitations of handheld devices with minimal storage capacity, processing speed and computation complexity were answered in cloud computing. The concept of master and slave computing has evolved to a great new extent which was never imagined. New features [2] are added to existing cloud computing technologies every day by various cloud service providers (CSP). These resourced technologies have opened a universal access theory with endless benefits. The space offered by public or private data centres is virtually segmented, assigned and

dedicated to users. The space is utilized for storage through request and automatic back up from registered devices. Cloud computing demands innovations for several automated processes like allocation of memory spaces, extension and reuse of resources, billing and protection plays a significant role in defining a standard for versatility [3][4].

An Internet service is the background and fundamental component of cloud computing. This establishes and completes the connection between the user and remote data centres for data storage, processing and retrieval [1]. Based on the functionality of these cloud servers, the service is categorized into an environment which acts either as Software, Platform or an Infrastructure. Software as a Service is a component designed for simplicity to both sides of users being end users or administrators. The next category will encourage the users to implement carefully designed software into the cloud environment. An Infrastructure defines how the components of the cloud, users and data are supposed to function in a given virtual space [1].

Despite these advantages, the openness of such a cloud is susceptible as the same leniency applies to attackers present in the same domain. The challenge comes when the data owners have the belief that their data is safe and sound in a very open sphere of influence. Protective measures are defined and imposed in spite of growing attacking mechanism, and this proposal intends to give a promising solution for identifying malicious attacks from so called third party auditors. The solutions to these problems should be confined to consume less energy and cost of a cloud service provider. Third party auditors gained the confidence of data owners and cloud service providers as they charge a lesser cost delivering a trustworthy comment on existing security standards. The rate of increasing users is exponential and thus imposes additional challenge for a cloud service provider to audit and periodically report to its users.

The challenges in protecting the data in a cloud are categorized based on the following factors. Access to clients with potential information, partiality of service to different clients, location of data and data owners, uniform service through a standard administration, technical support, retrieval and overall maintenance are the factors which needs to be balanced when security implementations are enforced.

## **BACKGROUND STUDY**

The Third Party Auditor is believed to be a common implementer of both cloud service provider and data owners where they test how the mechanism works and if the data are really secured. The question is whether the third party auditor has the intentions to steal potential information as they possess credibility to access the same. Provided with better benefits than auditing alone, bribed auditors may also lead to loss of information and degrading the integrity of data. The following section illustrates how a system is defined to check on such malicious attacks from trusted third part auditors. This system gives relief to either benefactors of the cloud service and ensures that only trusted auditors are appointed to ensure the protective schemes. Adding to the time and computation complexity of overall processes, this mechanism should utilize minimal resources for defining a strategy for identifying

dishonest third party auditors. A protocol was defined for certifying security and conserving the privacy details of data owners when they use cloud storage [7]. The protocol has limited the accessibility of third party auditors using RSA encryption and preventing the exposure of owners' data but with details required for auditing. This technique enabled users to modify, add and delete data whenever needed. Participants of this model were the data owners, cloud service provider and third party auditors. The data owners will compare the services of different cloud service providers and prefer one based on the economical norms. The cloud service provider will offer the space required and provide mechanisms to protect the data. The data owners will decide to use the service as a platform or service as mentioned in previous sections. The benefits of one CSP will be justified by a third party auditor but the decision depends on how trustworthy they are. The TPA cannot be blindly believed to be reliable and honest as they are no way in connection with either of the other participants. Both the parties cannot confirm that their data is protected when a third party auditor is involved. This led to the absolute necessity of an algorithm for securing the data, commencing the encryption through RSA.

- 1) A public and private key is generated by the data owners for encrypting the data. The public key is shared with the CSP for outsourcing for auditing process to complete. Audit process is initiated from the TPA side and sent to CSP for providing sufficient resources.
- 2) The encrypted data is transferred to TPA when this request is initiated from Audit.
- 3) The encrypted data will be verified by TPA once the public key is received from the data owners through the CSP.

Evaluation of this technique is done in two different analyses. One for estimating the time taken for transfer of encrypted data between the cloud space and third party auditor is communication time. The next is the computation cost, which is consumed by TPA to audit the given data and confirm that information integral.

The next methodology implements the usage of a modern cipher text [8] for encrypting the data before it is sent to TPA. This scheme does not require a copy of the data which removes redundancy cost and concentrates more on storage of integrated data. Five steps are included in the procedure, namely data owners, CSP, TPA and algorithms for encryption and sharing. A function KeyGen is used by TPA and data owners to generate private and public keys like other encryption schemes. After verifying the data in cloud space, TPA generates a metadata about verification done on data in cloud space using the function SigGen. CSP then generates the proof that the data stored is at the right place and time by the function GenProof which is later used by TPA to verify and authenticate that data is integral by the function VerifyProof.

The public key is generated for sharing between the data owners, cloud service providers and third party owners once the owned data is shared. Whereas the private key is used protect data which will not be revealed to third party auditors. The cloud service provider will establish a communication medium between TPA and data owners to share the keys and data for verifying the correctness. The data requested by TPA will be verified and a Proof will be generated. This proof will be forwarded back to data owners through CSP. The verified proof

should match with the key generated by the data owners. This confirms that the data is not disturbed by any factors internally and externally [8]. Performance is evaluated in terms of communication cost, computation cost and storage/retrieval cost. The aim of this study is to impose a stronger encryption standard with a lesser computational cost. Requests and responses are made shorter to reduce the communication cost.

The foundation of this privacy preservation commenced with homomorphic linear authenticator scheme [3]. Original content is marked by an arbitrary masking technique which prevents the need of a local copy when verification process is done by third party auditors. The operations are dependent on exchange of keys without the need of preparing a local copy for verification processes. Privacy is preserved with the same set of algorithms used in previously mentioned schemes [10].

The next scheme introduced the scheme of auditing the data in terms of batches without exposing all the available data. This is modified in our previous paper to lock certain modules based on the importance of data. The importance is defined by the data owners themselves. The method implements a bilinear map for encryption process [5]. The background study explains the common terms used for encryption and transferring of data to and fro. KeyGen is used for producing two sets of keys for public and private usage. The public key will be transferred to third party auditors who are authorised by CSPs. A signature is generated by cloud service providers before outsourcing the data files for auditing. After auditing process, a proof for integral data and outsourced files are compared for ensuring that verification process is complete [12]. A challenge based authentication process is also provided in the literature survey [6]. The schemes' complexity is constant even with the different approaches are implemented and investigated [13].

## **PROPOSED ALGORITHM**

The technique used in this proposal is dependent on the algorithm and its phases. Key exchange is regulated between the cloud service providers, data owners and third party auditors.

### **Algorithm I: Authentication of Keys**

The cloud service provider is asked to prepare a list of random numbers along with legitimate secret keys. Data owners will be asked to segregate the data based on the importance and save the credential information into the locked modules [1]. Testing process is initiated once these keys and random numbers are shared with the data owners. Using these secret keys, data is encrypted. Now the request for auditing is initiated from the TPA side. Unless the keys exist in both lists obtained from CSP and TPA, malicious activity is detected. The data owners will prevent the transfer of encrypted data to TPAs who exist without the right keys.

**Initialization:** (*kk*: known key; *sk*: Secret key; *TPAT*: Third Party Auditor Test; *TPATR*: Third Party Auditor Test Result; *CSPR*: Cloud Service Provider Result; *DO*: Data Owner; *pn*: prime number, *rn*: random number, and *V*: validation) Input: *Dc*

**Input:** (*kk*; *sk*; *TPAT*; *rn*; *p*) /\* Other than Locked modules

**Output:** (*TPATR* ; *CSPR*; *V*)

Select *rn* within range  $1 < rn < p$

Compute *Srn* /\* Set of random numbers

*DO* initiates *TPAT*

Declare *TPAT* = *Srn*

*DO* computes *CSPR* = *Srn.K*

*SPres* to *CC*: *Srn.K*

*DO* computes *TPAT* = (*kk*)*rn*

*DO* checks if *TPAT* = *Srn.K* = *CSPR* then

*DO* confirms successful *V*

else if *CC* determines the malicious activity of *TPA*

End if

End else if

### Algorithm II: Trust Helmet

The trust helmet is a common party which maintains the common keys to be shared within all the participants. The trust helmet will issue security checks over the keys and participants, making sure that keys are confined within the group. When the keys are shared with the *TPA* by the *CSP*, *TOA* also checks for the presence of those keys in Trust Helmet. If the keys are verified to be present, then the process continues. Similarly, the same process is also confirmed with Data owners. At any given time, the keys should be commonly present in all participants,

**Initialization:** (*Srk* : Set of Random keys to be shared; *Sk*: *Hk*: Hidden key; *p*: prime number; *rk*: Random key; *TPA*: Third Party Auditor; and *TH*: Trust Helmet)

**Input:** (*Srk*; *CSP*; *Sk*; *TH*)

**Output:** (*TPA*; *HK*)

*DO* & *CSP* use *rk*

Set  $1 < rk < p$  && *TPA* knows *Srk* && *Srk* belongs to *T*

*CSP* to *TPA*:  $HK = Sk + rk \text{ mod } p$

*TPA* examines *SHK* if  $Srk \text{ Ssk} = Ssk + rk \text{ mod } p$  then

Set  $SHK = Srk + rk$

Else if *Srk rk* not equal to  $Srk + rk$  then

Set *CSP* to *SHK*

End if

End else-if

*TPA* to *CS* belongs to *HK*

*CC* computes  $HK - rk = Srk \text{ mod } p$  if  $DO = HK$  then

Set *TPA* = *DO*

End if

The CSP will assign a trusted key to the Data owners for encryption following which the auditors will request for verifying the integrity. Now if the auditors will ensure that data owners possess the same set of keys as given by the cloud service providers or else, the presence of manipulated entries are present either in the auditing or cloud service providers. The following section implements these concepts into a model and examines the possible outcomes. Previous strategies are also compared to provide a detailed report on the advantages of this proposed system.

## RESULTS AND DISCUSSIONS

Green Cloud simulator is utilized for investigating the performance of privacy preserving third party auditing using locality parameters. This is an open source simulation tool which can be implemented with C++ and results demonstrate the computational cost and energy consumption. Simulated results were obtained as the scenarios will portray the real time occurrences. The conditions that were initialized are portrayed in the next table.

Conditions	Statistics
Number of Chassis Switches in L4	1980
Packet Size	1260 KB
Line cards at L4	1630
Ports at L4	72
Number of racks at L4	16
Number of Chassis Switches at L3	432
Line Cards at L3	164
Ports at L3	48
Number of racks at L3	128
Used virtual machines	1800
Number of Servers	64
Maximum number of Cloud Service Users	18000
Hosts in each rack	132
Each Host supports	16 processors
Memory with each processor	256 GB
Storage Memory	512 GB
Virtual Disk Memory	430 GB
Bandwidth for L4	256 GB/Sec
Bandwidth for L3	128 GB/Sec
Bandwidth for L2	64 GB/Sec
Bandwidth for L1	16 GB/Sec
Queue delay	0.005 Seconds
Burst time	0.0056 Seconds
Idle time	0.0032 Seconds

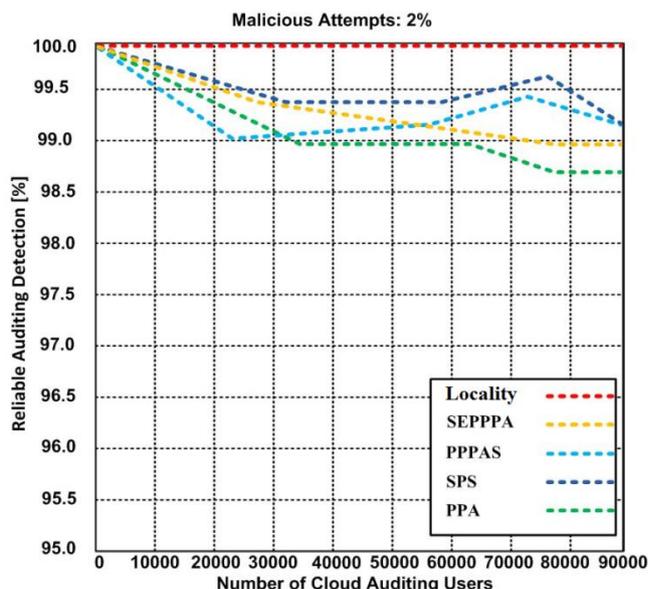


Figure 1: Reliable Auditing Detection

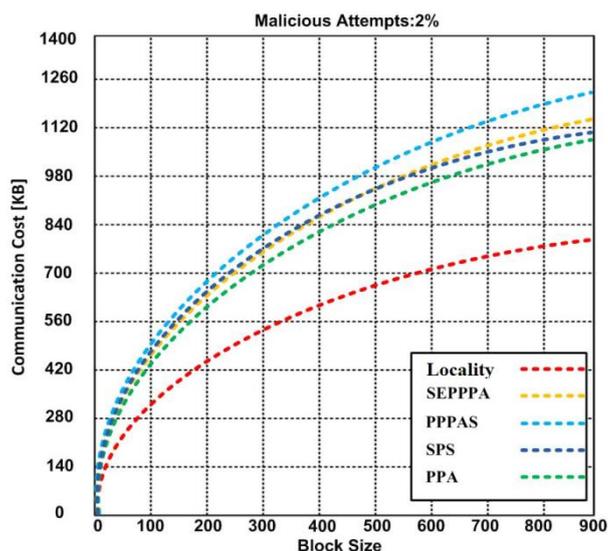


Figure 2: Communication Cost

These investigations are tested with dishonesty rates of 0 to 5% of Third Party Auditors. The proposed algorithms have shown that this method has outperformed the previous strategies and the results are shown in the following graphs for malicious attacks of 2%. The model was tested to express how the trustworthy third party auditors are identified in an environment. The next set of results demonstrates the communication cost of this system in spite of a new scheme introduced. The first figure provides sufficient evidence that when the number of cloud users i.e. data owners increase, the durability of locality based privacy preserving scheme remained constant at 100%, where the other models produced results of 99% approximately. This simulates the real time environment where the actions and users are dynamic in nature. Subsequently, the system was tested for time taken for auditing actions by the third party auditor. The proposed scheme also demonstrated reduced false positives than the other methods. Communication cost was also estimated with increasing number of blocks, ranging from 0 to 900. The simulation results show that the proposed model took 830 KB while the previous methods cost around 1100KB. These evidences provide enough justification to prove that this model is outperforming the existing standards.

The approach has been an adept technique to identify the presence of malicious third party auditors even before the encrypted data is shared among the participants in the domain. The Cloud Service Provider, Data Owners, and Third Party Auditors can rely on this methodology for efficient and secured communication for auditing and privacy preserving. The proposed method has shown 100% reliability even in the presence of 90000 users at the same time. The rate of false positives was addressed and this approach has been more efficient than existing methods. The third simulation proves that computation cost also turned up lesser for blocks of size 900KB. The processing and communication time was considerably reduced after enhancing the security mechanism.

## CONCLUSION

Organisations including governmental operations are deploying their services through cloud environments. The data owners believe that along with unlimited benefits of accessing a cloud environment, security will also be achieved. Yet the system is susceptible in a number of cases. This proposal introduced a scheme for authenticating the third party auditor to ensure that data is secured when verification is one. The CSPs rather than being economical need to be more secure in this virtual world with no boundaries.

Having these objectives in mind, computational and processing overhead cannot be compromised when security is added. This proposal intends to address all these defects in a mechanism to authenticate the third party auditors based on their locations. The method was to signify that auditors are trusted users who participate just to verify the integrity of data stored. Schemes were introduced to regulate the exchange of keys between the typical participants. An external trust helmet was maintained and referred whenever there is a need to transfer data in an encrypted form. Instead of passing data, the keys were shared and compared before original data is at stake. Results from simulation have shown promising results at an affordable computation and processing time. In the future, tracing back to the location where the system failed to preserve the privacy of data owners is to be derived with betterments to this scheme.

## REFERENCES

- [1] Akheel Mohammed, D.Vasumathi. "Restrictive Ambiguity and Add-On Architecture Prototype For Privacy Preservation In Cloud Auditing" International Journal of Computational and Theoretical Nanoscience, American Scientific Publishers, SCOPUS
- [2] Razaque, Abdul, and Syed S. Rizvi. "Privacy-preserving model: a new scheme for auditing cloud stakeholders, " Journal of Cloud Computing 6, no. 1 (2017): 7.
- [3] Wang, Cong, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for secure cloud storage." IEEE transactions on computers 62, no. 2 (2013): 362-375.
- [4] Razaque, Abdul, and Syed S. Rizvi. "Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment." Computers & Security 62 (2016): 328-347.
- [5] Rizvi, Syed, Abdul Razaque, and Katie Cover. "Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment." In Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2<sup>nd</sup> International Conference on, pp. 31-36. IEEE, 2015.
- [6] Moghaddam, Faraz Fatemi, Omidreza Karimi, and Maen T. Alrashdan. "A comparative study of applying real-time encryption in cloud computing environments." In Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on, pp. 185-189. IEEE, 2013.

- [7] Wei, Lifei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, and Athanasios V. Vasilakos. "Security and privacy for storage and computation in cloud computing." *Information Sciences* 258 (2014): 371-386.
- [8] Hussien, Z.A., et al. Public auditing for secure data storage in cloud through a third party auditor using modern ciphertext. in *Information Assurance and Security (IAS), 2015 11th International Conference on*. 2015. IEEE.
- [9] Wang, Boyang, Baochun Li, and Hui Li. "Panda: Public auditing for shared data with efficient user revocation in the cloud." *IEEE Transactions on services computing* 8, no. 1 (2015): 92-106.
- [10] Rizvi, Syed, Abdul Razaque, and Katie Cover. "Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment." In *Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2<sup>nd</sup> International Conference on*, pp. 31-36. IEEE, 2015.
- [11] Worku, Solomon Guadie, Chunxiang Xu, Jining Zhao, and Xiaohu He. "Secure and efficient privacy-preserving public auditing scheme for cloud storage." *Computers & Electrical Engineering* 40, no. 5 (2014): 1703-1713.
- [12] Yang, Kan, and Xiaohua Jia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." *IEEE transactions on parallel and distributed systems* 24, no. 9 (2013): 1717-1726.
- [13] Lee, W-B., and C-C. Chang. "Efficient group signature scheme based on the discrete logarithm." *IEE Proceedings-Computers and Digital Techniques* 145, no. 1 (1998): 15-18.