International Journal of Scientific & Engineering Research Volume 11, Issue 6, June-2020
ISSN 2229-5518

Analysing Third Party Auditor (TPA) Role in Cloud Data Storage

Ashish Bhardwaj, Dr. Surendra Yadav

Abstract: Cloud storage is turning out to be well known nowadays due to further its potential benefit that the information can be gotten to whenever and from anyplace. But by providing ease in the data availability, cloud storage suffers from security issues, and the proposed security measures are required in order to protect the data. A third-Party audit is becoming very popular, in providing the proper security measures for protecting cloud data storage from unauthorized access and maintaining data integrity. This paper reviews the concept of cloud storage and emphasizing the role of TPA in cloud data storage. This paper focuses over the analysis of research work by other authors and highlights the concepts used by them for privacy-preserving and for maintaining data integrity.

Index Terms: Cloud computing, Cryptography, Data auditing, Data integrity, Data storage, Security issues, Third party auditing

1 Introduction

Cloud Storage is the storage-based service model which provides a facility for data exchange and remote storage. In such an isolated environment, data is managed remotely, backup is made and is also accessible to the users on the network. In simple terms, cloud storage is just like a virtual locker for data which can make remotely any data available at any time. Some of the primary examples of cloud storage services which we come across in our daily life are Google Drive, iCloud Services by Apple and One Drive Services by Microsoft. The users of cloud data storage services are being charged as per the storage consumption, and the billing criteria will be on a monthly or yearly basis. In the case of Cloud Storage, data is stored and replicated over several hard drives. In cloud storage, data reliability is more which is achieved by server farms. The server farm is a concept of replicating servers and the data on them at different locations around the world.[1]

Cloud storage models come in three main parts, namely public, private and hybrid.

- *Public Cloud Storage Model*: - It refers to multiple users storage environments. Here, the users are charged based on data usage. The overall charges of the cloud storage will depend on the number of times cloud servers accessed and also on the volume of data accessed. In such a storage prototype, the data can spread over various locations, so such prototype is being followed in services like Google Cloud Storage, Amazon Simple Storage Service and more. [2]
- *Private Cloud Storage model*: In this model data are related to an organisation is stored at in-house storage-based services which are based on cloud computing and the cloud storage technology. In contrast to public cloud storage, it is not accessible publicly, and data stored in this prototype under the ownership of the single organization, which can only be accessed by those organizations and its related external partners. Private Cloud storage is feasible for those users that require some sort of customization in cloud services and also full control over their cloud data. [2]
- *Hybrid Cloud Storage Model*: It comprises of private and public Cloud, in which private Cloud-like feature of the cloud services being managed by a user and public Cloud like a feature of some services being led by a third party is observed. It includes cloud storage services which make use of both of the local and off-site resources.[3]

Although Cloud storage had advantages of Data availability from anywhere and at any point in time, but they are subject to security issues. The problems and issues are related to the protection of data from unauthorized access. Thus, in such an environment, cloud auditing services required, which will be responsible for making an evaluation of security controls and checking the performance of the services offered by the cloud storage provider.

In this way, here the job of TPA comes as a client in the cloud condition, liable for keeping up the honesty of the cloud information and shielding it from assaults of gatecrashers and unethical programmers. [4]

2 TPA in Cloud

In the case of cloud services, there is a data exchange between cloud service providers and network users. Such data exchange includes a transfer of user personal information, some passwords, banking related data and even more. In order to provide security across a cloud-based environment, concepts like SSL, PPTP, and VPN are generally used. But when looking at the history of hacking attempts and attacks by intruders, they observed attackers easily crack these security measures. So, in such an environment, we can use the third-party authentication concept. It is helpful when the trading of information is between the clients and the cloud specialist organizations. To give appropriate security the board in a cloud domain, TPA will watch out for the exercises of the cloud specialist co-op and cloud client. TPA has the

capacity to guarantee and check the uprightness of the information put away in the cloud condition, without influencing the security of the clients.

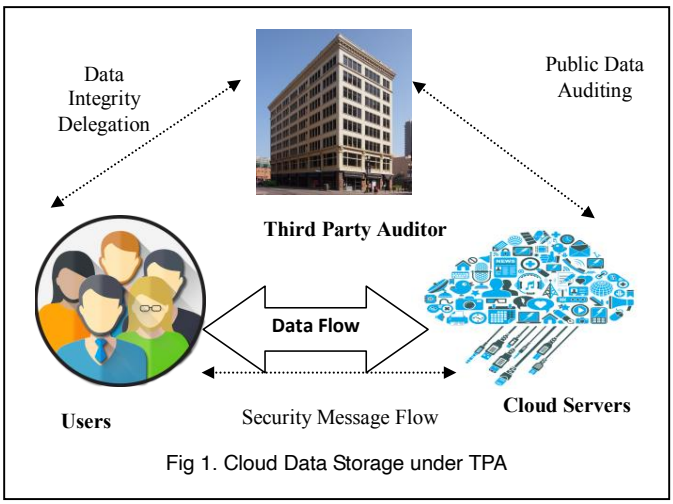

Fig 1. Cloud Data Storage under TPA

TPA working in a Cloud Data Storage Environment can be summarized in the following three processes,

- *Generation of Keys*: The owner does the process of the generation of a private key. There are two keys, private and public. The owner of data generates the private key; it is used for encrypting the data whereas the Public one is general.
- *Prompting for Server Integrity*: TPA used for prompt or interrogate the server for proof of identity and server is responsible for showing or sending the proof of identity.
- *Verification and Validation of Integrity*: TPA is responsible for receiving the integrity proof from the server and maintaining the data integrity.[5]

3 Literature Survey

In the literature survey, we review various papers related to TPA and divided the papers into the following categories:

3.1 TPA Based Cloud Storage

Yun Xue et al. (2019) [6] suggested an ensured and effective information sharing plan for dynamic user groups. For keeping up the information uprightness and ensuring for unapproved get to, creators utilized the Rights Distribution Center (RDC) in their plan. To guarantee the security of end-client character, they are playing out the TPA to check the information steadfastness, distinguishing on a specific framework is inconceivable. Thusly, the balance of the review can be progressed.

Imad El Ghoubachab et al. (2019) [7] suggested an inspecting plan that gives clients a profoundly secure and capable method to approve their re-appropriated information. The suggested plot has a lower investigative overhead on the end-clients. It enables them to dole out the information confirmation method to an outside examiner or TPA while keeping up a lower scientific and correspondence overhead without jeopardizing the mystery of the putaway information.

Mohamed Ben Haj Frej et al. (2019) [8], they focus on improving trust and tempt reception between cloud clients (CC) and cloud service providers (CSP), presented another worldview of relying upon a TPA. The suggested protocol is lightweight as far as preparing and correspondence costs. This was suggested in a recently presented scientific prototype for privacy-preserving and integrity checking.

C. Noorjahan and H. Noordean (2017) [9] suggested a hypothesis that uses a confided in TPA, who can check the information uprightness on demand. In the suggested system, TPA accomplishes confirmation work for the client and moreover for Cloud Storage Server (CSS). Along these lines, TPA first gets the information and utilize CSS for keeping up information uprightness.

S. H. Abbdal et al. (2014) [10] suggested another TPA model which incorporates three key parts: the cloud client (information proprietor), the TPA, and the cloud server (CS), where for the information client has the position, and he/she oversees various segments as services. This prototype aides in safeguarding information respectability and protection.

L. Yang and L. Xia (2016) [11] likewise suggested a safe audit mechanism which supports dynamic activity and straightforward verification. Authors used BLS short signature method, which is based on the arrangement & implemented B+ Hash Tree-like structure, as a result of which, the audit scheme is quite successful. The scheme works as a coordinator in the auditing procedure and TPA not able to manipulate any data. In this manner, the TPA scheme is straight forward. Then, the scheme uses a bilinear aggregate and random mask signature technology to acknowledge batch audit and privacy assurance.

Q. Wang et al. (2011) [12] presents a superior methodology for Cloud Computing information stockpiling. In particular, they consider the task of allowing TPA, to check the honesty of the dynamic information. To keep up the information uprightness, creators utilized Merkle Hash Tree advancement for block tag authentication.

S. A. El-Booz et al. (2015) [13] suggested a novel made sure about distributed storage structure to improve the security confirmation level security by using double validation techniques, first is Time based One Time Password (TOTP) for cloud client check and the other is Automatic Blocker Protocol (ABP) to shield the system from ill-conceived outsider examiner totally.

S. D. Thosar and P. Sonewar (2016) [14 suggested a prototype by utilizing the BLS signature to confirm the integrity of data. Storage trouble is limited because of limited size; for example, 160-piece BLS signature so overcomes this problem used external auditor, also known as TPA is utilized for audits. In this way, the end-user may utilize cloud data without stressing over its uprightness.

P. Kharmate and R. Suryawanshi (2016) [15] suggested a system dependent on using the own auditing dependent on the token age. The recuperation issue of shelled approved clients without information proprietors disentangled through an intermediary, which is utilized to recoup the approved

clients into the standard open evaluating structure. The system supports public auditing and secures protection.

H. Tian et al. (2017) [16] suggested an inventive open reviewing hypothesis for made sure about distributed storage relies upon the dynamic hash table (DHT), which is another two-dimensional information structure arranged at a TPA to consider the dynamic examining of the information property. Creator's hypothesis depends on information security insurance by joining the homomorphic authentication dependent on the open key with the random masking delivered by the TPA, and achieve batch auditing by means of using the total BLS signature procedure.

L. Yeh (2016) [17] recommended TPA model for cloud storage service focused on secure the properties of classification, respectability, and accessibility. Additionally, the TPA can't understand the substance of the putaway record during verification. Authors' scheme likewise gives a valuable capacity to quantify the disappointment time of the CSP.

J. Raja and M. Ramakrishnan (2017) [18] presented the Data Privacy protection model utilizing TPA which serves to audit the data integrity without requesting the nearby data duplicacy and any extra weight. They used bilinear aggregate signatures so that TPA can deal with numerous customer auditing demands simultaneously.

3.2 TPA Based Cloud Storage involving Cryptography

Manish M Saunshi e. al (2019) [19] introduced a model on secure document trading on Cloud utilizing SHA-256 calculation which is equipped for illuminating data security, authentication, and trustworthiness issues of records on the Cloud. Cryptography algorithms improve data security. The rightness of data is checked by presenting strategies.

R. Singh et al. (2017) [20] to achieve the security ensuring open for evaluating, the creators suggested explanation for Third Party auditor using three-way handshaking protocol over the Extensible Authentication Protocol (EAP) with freed encryption standard. Creators made module Verify-Proof utilized by TPA for confirming honesty. Despite this segment, the personality of each section in the shared information are kept avoided the open evaluators. Also, rather than affirming the examining task in stages, this will have the option to play out the diverse evaluating tasks simultaneously.

A.S. Kalyana Kumar and DR. K. Abdul Razak (2019) [21] suggested a Secured Crypto based Data Outsourcing Model (SCDOM), which uses privacy safeguarding scheme for distinguishing inconsistencies, an upgraded Blowfish method for executing encryption and unscrambling. Here, while accepting user encoded data, MAC-Message Authentication Code is created and afterwards transmitted to Third Party Auditor (TPA) for verification. From the experimentation results, it has been observed that suggested SCDOM gives upgraded results than the traditional strategies.

N. Shimbre and P. Deshpande (2015) [22] looks at the archive dissemination and SHA-1 method. Creators talk about the treatment of some security issues like Fast mistake limitation, information genuineness and information security. The suggested structure licenses clients to review the information with lightweight correspondence and figuring cost.

S. Hiremath and S. Kunte (2017) [23] suggested a capable open evaluating methodology using TPA to affirm the dependability of information set aside in the Cloud. Here the creator proposes the utilization of Advanced Encryption Standard for calculation for encrypting and Secure Hash Algorithm (SHA-2) figuring to make confirmed metadata or message overview to approve information honesty. The examination shows that the recommended hypothesis is without a doubt secure and TPA sets aside a consistent exertion to review records of different sizes

B. L. Adokshaja and S. J. Saritha (2017) [24] introduced another examining plan uses, proprietor of the information, TPA and cloud server. TPA can check the decency of information on solicitation of the clients. Hence, no additional weight given on the cloud server. It is used remarkably to save the encoded blocks of information. The TPA and information proprietor play out all the errand for the plan. The suggested idea utilizes the AES calculation for encryption reason and utilizes hashing calculations for keeping up information respectability.

S. Shaikh and D. Vora (2016) [25] suggested a scheme which consolidates the encoding system combined with identity verification technique. The encoding scheme makes use of ElGamal and SHA-256 hash for authentication of users.

S. Hiremath and S. R. Kunte (2018) [26] used the Advanced Encryption Standard (AES) count for encoding customer's data and Secure Hash Algorithm (SHA-2) to process message digest. The system is implemented in Amazon EC2 on network operating system.

R. Suryawanshi and S. Shelke (2016) suggested two plans to ensure the information security over the Cloud. The main plan is open inspecting where homomorphic straight authenticator is utilized with random masking, for the examining. The subsequent plan depends on Threshold Cryptography in where to control the information Capability of rundown used is checked. While the fundamental plan ensures that TPA won't increment any data about the fragile information during the inspecting procedure, the other one guarantees that malevolent clients couldn't mishandle the information set aside on mists.

3.3 Secure Cloud Storage with Multiple TPA's

S. Patii and N. Rai (2017) [28] perceived that the usage of TPA for checking the respectability of information limits the hot work of persistent checking. To overcome the burden on single TPA, the authors introduced the concept of multiple TPA's. Authors utilized Merkle Hash Tree (MHT) and AES algorithms for maintaining data integrity and data privacy.

S. H. Abbdal et al., (2016) [29] makes use of multiple TPA's and homomorphic straight authentication and an elliptic curve digital signature are used in the modules related to data transfer and TPA functionality.

4 Conclusion and Future Work

There are various TPA based approaches reviewed in this paper. In future, we will also try with the three-model concept involving, Data owner, Cloud Server and TPA. We would like to propose some approach related to the formation of chunks for data shared and for this purpose will follow some clustering algorithms. We will also explore various algorithms like AES, blowfish and others, for the encryption of chunks. Also, for TPA integrity checking purpose, will explore hashing algorithms, MD5, SHA-1, SHA-2 etc.

References

[1] N. Shimbre and P. Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm," in *IEEE Int. Conf. Comput. Comm. Cont. Automat.*, Feb. 2015, pp. 35-39.

[2] G. F. Nadlamani and S. Shaikh, "Preserving privacy using TPA for cloud storage based on regenerating code," in *IEEE Int. Conf. Recent Trends Inf. Technol.(ICRTIT),* April 2016, pp. 1-5.

[3] S. Rizvi, A. Razaque and K. Cover, "Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment," in *IEEE 2nd Int. Conf. Cyber Sec. Cloud Comput.,* Nov. 2015, pp. 31-36.

[4] A. K. Udagatti and N. R. Sunitha, "Fault tolerant public auditing system in cloud environment," in *IEEE 2nd Int. Conf. Appl. Theoret. Comput. Comm. Technol. (iCATccT),* July 2016, pp. 359-362.

[5] S. Patii and N. Rai, "An effectual information probity with two TPAS in cloud storage system," in *IEEE 3rd Int. Conf. Sci. Technol. Engineer. Manage. (ICONSTEM),* March 2017, pp. 432-434.

[6] Y. X. Yan, L. Wu, W. Y. Xu, H. Wang and Z. M. Liu, "Integrity audit of shared cloud data with identity tracking," *Sec. Comm. Net.*, 2019.

[7] I. El Ghoubach, R. B. Abbou and F. Mrabti, "A secure and efficient remote data auditing scheme for cloud storage," *J. King Saud Uni. Comp. Inf. Sci.*, 2019.

[8] M. Ben Haj Frej, J. Dichter and N. Gupta, "Lightweight Accountable Privacy-Preserving Protocol Allowing the Cloud Client to Audit the Third-Party Auditor for Malicious Activities," *Appl. Sci.*, vol. 9, p. 3034, 2019.

[9] C. Noorjahan and H. Noordean, "Recovery based TPA in cloud for providing security to outsourced data using CloudSim," in *IEEE Int. Conf. Ener, Comm., Data Analyt. Soft Comput. (ICECDS),* Aug. 2017, pp. 625-630.

[10] S. H. Abbdal, H. Jin, D. Zou and A. A. Yassen, "Secure Third Party Auditor for Ensuring Data Integrity in Cloud Storage," in *IEEE 11th Int. Conf. Ubiquitous Intellig. Comput.* and *IEEE 11th Int. Conf. Autonom. Trusted Comput.* and *IEEE 14th Int. Conf. Scalable Comput. Comm.,* Dec. 2014, pp. 510-517.

[11] L. Yang and L. Xia, "An Efficient and Secure Public Batch Auditing Protocol for Dynamic Cloud Storage Data," in *IEEE Int. Comp. Symp. (ICS),* Dec. 2016, pp. 671-675.

[12] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in *IEEE Tran. Para. Distribut. Sys.*, vol. 22, pp. 847-859, 2011.

[13] S. A. El-Booz, G. Attiya and N. El-Fishawy, "A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol," *EURASIP J. Inf. Sec.*, vol. 1, p. 13, 2016.

[14] S. D. Thosar and P. Sonewar, "Data integrity verification privacy preserving approach of cloud using Third Party Auditor and multithreading," in *IEEE Int. Conf. Comput. Comm. Cont. Automat. (ICCUBEA),* Aug. 2016, pp. 1-4.

[15] P. Kharmate and R. Suryawanshi, "Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud," in *IEEE Int. Conf. Adv. Electr., Comm. Comp. Technol. (ICAECCT),* Dec. 2016, pp. 116-121.

[16] H. Tian, Y. Chen, C. C. Chang, H. Jiang, Y. Huang, Y. Chen and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Tran. Ser. Comput.*, vol. 10, pp. 701-714, 2015.

[17] L. Y. Yeh, "A practical third-party auditor prototype for cloud storage service," in *7th IEEE Int. Conf. Softw. Engineer. Ser. Sci. (ICSESS),* Aug. 2016, pp. 796-799.

[18] J. Raja and M. Ramakrishnan, "Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment," in *IEEE Int. Conf. Intellig. Comput. Cont. Sys. (ICICCS),* June 2017, pp. 1200-1205.

[19] M. M. Saunshi, N. Manoj, M. Ramesh, B. T. Nithyashree, M. Vaidehi, "Efficient and Secure Data Storage in Cloud Computing," *Int. Res. J. Engineer. Technol.*,vol. 06, pp. 231-236, 2019.

[20] R. Singh and S. Prakash, "Privacy preserving in TPA for secure cloud by using encryption technique," in *IEEE Int. Conf. Innovat. Inf., Embedded Comm. Sys. (ICIIECS),* March 2017, pp. 1-5.

[21] A.S. Kalyana Kumar, K. Abdul Razak, "A Secure Crypto-Based Data Outsourcing Model for Monitoring the Smart Environment in Cloud," *Int. J. Scient. Technol. Res.,* vol. 8, pp. 7-12, 2019.

[22] N. Shimbre and P. Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm," in *IEEE Int. Conf. Comput. Comm. Cont. Automat.,* Feb. 2015, pp. 35-39.

[23] S. Hiremath and S. Kunte, "A novel data auditing approach to achieve data privacy and data integrity in cloud computing," in *IEEE Int. Conf. Electrical, Electronics, Comm., Comp., Optimizat. Techniq. (ICEECCOT),* Dec. 2017, pp. 306-310.

[24] B. L. Adokshaja and S. J. Saritha, "Third party public auditing on cloud storage using the cryptographic algorithm," in *IEEE Int. Conf. Energy, Comm., Data Analyt. Soft Comput. (ICECDS)*, Aug. 2017, pp. 3635-3638.

[25] S. Shaikh and D. Vora, "Secure cloud auditing over encrypted data," in *IEEE Int. Conf. Comm. Electron. Sys. (ICCES),* Oct. 2016, pp. 1-5.

[26] S. Hiremath and S. R. Kunte, "Ensuring Cloud Data Security using Public Auditing with Privacy Preserving," in *IEEE 3rd Int. Conf. Comm. Electron. Sys. (ICCES),* Oct. 2018, pp. 1100-1104.

[27] R. Suryawanshi and S. Shelke, "Improving data storage security in cloud environment using public auditing and threshold cryptography scheme," in *IEEE Int. Conf. Comput. Comm. Cont. Automat. (ICCUBEA)*, Aug. 2016, pp. 1-6.

[28] S. Patii and N. Rai, "An effectual information probity with two TPAS in cloud storage system," in *IEEE 3rd Int. Conf. Sci. Technol. Engineer. Manage. (ICONSTEM)*, March 2017, pp. 432-434.

[29] S. H. Abbdal, H. Jin, A. A. Yassin, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien and D. Zou, "An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage," in *IEEE 2nd Int. Conf. Big Data Sec. Cloud (BigDataSecurity), IEEE Int. Conf. High Perf. Smart Comput. (HPSC),* and *IEEE Int. Conf. Intellig. Data Sec. (IDS),* April 2016, pp. 412-417.

.