ANALYSIS ON PUBLIC AUDIT IN CLOUD STORAGE DATA

Akheel Mohammed

Research Scholar, Department of Computer Science and Engineering,

JNTUH - Jawaharlal Nehru Technological University Hyderabad - College of Engineering, Kukatpally, Hyderabad, Telangana. India

D. Vasumathi

Professor, Department of Computer Science and Engineering,

JNTUH - Jawaharlal Nehru Technological University Hyderabad - College of Engineering, Kukatpally, Hyderabad, Telangana. India

ABSTRACT

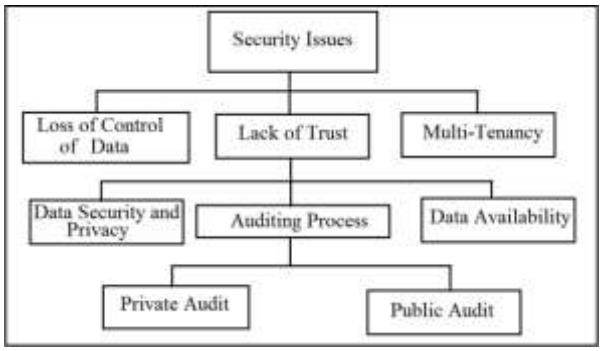
The cloud computing in its numerous forms allow users to store information at faraway region and reduce load at neighborhood machine. even though it is an advantage nevertheless disadvantage exists along with far off storage. The principal security troubles in cloud computing including loss of facts control, lack of agree with and multi-tenancy are reviewed. The cloud computing and its service and deployment models are discussed by ways which the existing protection troubles in cloud computing are averted. ensuring cloud facts integrity and privacy seems to be the major difficulty. to conquer unauthorized access of information via cloud provider providers and records customers, verification is done thru depended on 0.33-party auditor. The cloud auditing needs to be executed and data safety also needs to be ensured with out the know-how of the actual data shops at cloud. Researcher suggests eager hobby to offer a cloud framework, which preserves the privateness and ensures the integrity of cloud information. The paper critiques privateness maintaining public audit schemes in cloud computing environment.

Keywords: Cloud environment, cloud computing, audit, trust, security.

1.INTROUCTION

wide variety of technologies are coming in the cloud computing, which affords net-primarily based carrier and use of pc technology. storing statistics into the cloud garage off ers top notch help to users considering they do not need to care about the troubles of hardware problems. As a end result, users are at the hobby of their cloud service providers for the provision and integrity in their information. On the only hand, although the cloud offerings are a lot greater powerful and reliable than personal computing devices and large variety of each internal and external threats for information integrity nonetheless exist [1]. the entirety is hosted inside the cloud a nebulous assemblage of computers and servers accessed thru the internet. Cloud computing offers consumer to access all packages and files from anywhere inside the international, liberating you from the confines of the laptop and making it less complicated for organization participants in different places to collaborate. Cloud computing is imparting developers and organizations

with the ability to focus on what subjects' maximum and avoids un-differentiated work like procurement, renovation, and potential plans. Cloud carrier carriers have joined to build cloud environments and offer offerings to the person.



. **Figure 1 shows tree structure of protection issues concerning cloud facts.**

2.RELATED WORKS

Cloud computing faces many issues on integrity and privateness of user's facts saved inside the cloud. consequently, it calls for a few relaxed and efficient methods which could make certain the integrity and privacy of records stored within the cloud.

2.1 SECURITY ISSUE IN CLOUD COMPUTING

The data processed in different clouds inclusive of non-public and public clouds are issue to different protection exposures. therefore, it's miles vital to understand the diverse challenges related to cloud computing [3]. these issues may be studied in terms of the following factors:

1. loss of control of statistics
2. Accept as true with issues

The customers can loss of control of statistics over information in cloud computing because of the third-party fashions of the cloud. The records, packages, and sources are positioned with the company; the consumer identity control is handled by way of the cloud; and the user-access manage rules, security regulations, and enforcement are managed by the cloud provider [8]. The consumer has to rely on the cloud company for facts safety and privacy, and availability, and monitoring and repairing of offerings or sources. The cloud computing system is related to positive risks due to loss of control in passing sensitive facts to other corporations. In cloud computing, multi-tenancy refers to sharing of assets and services to run software program times that serve a couple of customers [15]. the main reason for cloud providers to have multi-tenancy is to reduce the fees by means of sharing and reusing resources among tenants. here, the bodily assets and offerings, as well as administrative capability and support, can also be shared.

2.2 AUDITING

Mainly Cloud environment is used to store big amount of information and allow the customers to get admission to the statistics from everywhere and at any time. in the latest trend of garage technology, rather than storing the information in difficult drives like pen drives, compact discs, the facts proprietors shop their statistics in cloud for future references and access [2]. In case of information loss, the backup may be restored from cloud. Separate backup servers also are maintained by the cloud with the aid of thinking about any bodily disasters in future [6] for the reason that statistics is stored remotely, the consumer needs to check the statistics periodically, whether it's been altered or no longer. The auditing process can be completed via two ways:

a) private audit: The integrity of the information is verified by using data owner.
b) Public audit: The integrity of the information is verified by means of the TTPA

The consumer does no longer have the time, feasibility or assets to carry out the garage correctness verification, he can optionally delegate this assignment to an independent 0.33 birthday party auditor, making the cloud garage publicly verifiin a position [4]. to securely introduce an eff ective TPA, the auditing system should deliver in no new vulnerabilities in the direction of person statistics privateness. particularly, TPA need to no longer examine person's statistics content through the delegated information auditing [5]. this is why, the usage of TPA services is a fee eff ective way for customers to benefit the accept as true with within the cloud. The TPA has professional authenticate expertise and audit talents.

2.3 COMPARISON OF AUDITING TECHNIQUES.

Yua et al in [9] the active adversary assaults for 2 identification privacy-keeping auditing mechanisms particularly Oruta and Knox, and a allotted storage integrity auditing mechanism. the writer indicates that these schemes are insecure when energetic adversaries are worried in the cloud garage and also can modify the facts within the cloud, without understanding to the auditor in the cloud [7]. approach of auditing extra comfy but Adversaries can Alters the statistics without understanding to auditor.

within the Yang et Al in [10] proposed scheme, every and each institution consists of the group contributors and the organization supervisor, maintained by using the area supervisor. Many unauthorized customers may alter the information saved in cloud without any identity. so as to triumph over this difficulty, proposed an efficient public auditing answer that preserves the identification privateness and the identification traceability for institution contributors simultaneously. Blind Signature technique of auditing is greater comfy however having extra computation cost.

virtual signature auditing method having less computation cost, but it calls for impartial auditing service. Scheme proposed through Navajothi et al in[13] which specializes in efficient and secure cloud storage device and dynamic privateness- retaining audit carrier (TTPA) for verifying the integrity of outsourced garage. It achieves both public audit-potential and dynamic records operations.

to conquer the difficulty of dynamic management of outsourced information, records confidentiality and integrity, Kim et al in [11] proposed a public auditing protocol for educational multimedia facts saved within the cloud using random values and a homomorphic hash feature [14]. even though cloud storage offerings provide a at ease and dependable get admission to to the outsourced instructional multimedia facts for users, it brings tough safety troubles in phrases of information confidentiality and integrity, and the some of the schemes also suffer from dynamic control of outsourced facts.

Cloud garage affords the data garage in secured and effective way; the records gets affected due to the unauthorized get right of entry to or some hardware/software program failures. Yuchuan et al in [12] designed an auditing framework for cloud storage and proposed an algebraic signature based totally faraway information ownership checking protocol, which lets in a third-birthday party to auditing the integrity of the outsourced records on behalf of the users and helps limitless wide variety of verifications.

Author Name	**Auditing Technique**	**Advantages**	**Disadvantages**
Yua et al[9]	Qrta andknox	More Secure	Adversaries alters the data without knowing to author
Yang et al[10]	Blind Signature	More Secure	Heavy computation Cost
Navjajothiet al [13]	Homo- morphic Hash function	Secure Supports full dynamic data	Additional computation cost
Kim et al[11]	Digital Signature	Less consumptioncost	Requires unbiased auditing services
Yuchuan etal [12]	AlgebricSignature	Efficient	More computationcost

Table 1: Comparison of Audit Techniques for Cloud Computing

The Table 1 shows comparison of auditing techniques. Trusted authority provides a unique global identification parameter to entities in the system. Data owners send request to third party auditors to perform auditing of data. Third party auditor launches the public auditing task by sending a challenge message to the Cloud Service Provider. The Cloud Service Provider will generate a response and send it to the TPA.

3.PROPOSED WORK

The technique utilized in proposed machine is comfortable records in cloud storage. Cloud computing platforms offer clean get admission to to a agency excessive overall performance computing and garage infrastructure via internet services.

3.1 PROBLEM DECLARATION

Maximum statistics garage middle enables the customers to remotely keep and access the facts. human beings have didn't word, but dynamic auditing cannot manage over encrypted statistics in cloud. by rethinking the approach to dynamic auditing process. Proposed machine can restoration the security challenges in auditing of encrypted records garage. To provide higher solution, proposed public auditing protocols which aid encrypted information and information dynamics. Proposed auditing protocol that is secured cloud garage auditing protocol correctly handles encrypted information and acting auditing on encrypted facts stored in cloud facts.

3.2 OBJECTIVES

A relaxed and green privateness maintaining public auditing scheme is to be proposed to reap following goals. It achieves privateness maintaining and public auditing for cloud through using a TPA (third birthday party Auditor), which does the auditing without retrieving the facts copy, subsequently privacy is preserved.

1) Storage Correctness

2) Privateness Upkeep

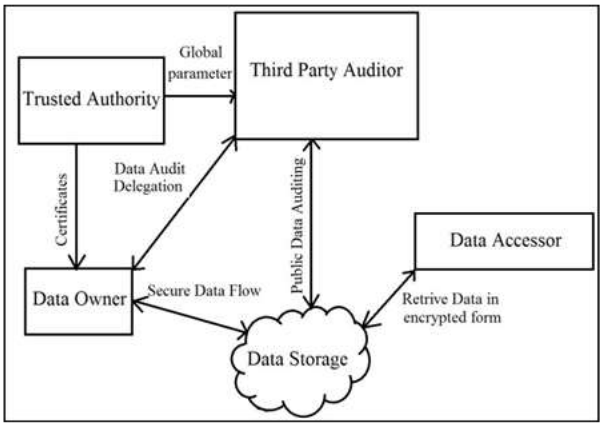
3) Searching Over Encrypted Facts

4) Auditing Of Cloud Statistics

3.3 SYSTEM MODEL

The main goal of proposed system is to secure and protect the data which come under the property of users.

Figure 2 shows architecture of proposed system.



]

Data Accessor: An individual consumer or organization has a lot of data les and needs to store in the cloud. It depends on the cloud to manage data and computation, so it can reduce storage cost.

Data Storage: A cloud service provider has huge storage space and computation resource to provide the clients data.

Third Party Auditor: A trusted organization has expertise and capabilities that the clients do not have. It is responsible for assessing the client's data on cloud storage service.

Trusted Authority: Trusted authority provides certificates to data owner for identification purpose. Also provides global parameters to third party auditors.

Data Owner: Data owner upload data on cloud. Send request for checking integrity of data.

4.PROPOSED ALGORITHM

The data owner stores the data in the cloud initially. Instead of storing the entire data, the owner divides the data into multiple blocks and sends to the remote cloud storage [6]. If the data owner wants to check the integrity of content stored in cloud, initially a request message is made by the data owner to the TPA. The TPA receives the request message from data owner and sends a challenge message to the CSP, in order to verify the data. Once the CSP receives the challenge message from the TPA, it will send a response to TPA. Here the verification process is done by the TPA without having the knowledge of the original data. The TPA checks the data; it will provide the result to the data owner.

The general framework given as follow:

CertGen: The TA generates certificates and assign to data owners

AssignPar: The TA assigns global parameters to TPAs.

Setup: The data owner stores the data in cloud by dividing it into multiple numbers of blocks.zKeyGen: The data owner generates a key using the large prime numbers. Using the large prime number, the public and the secret keys are generated by the data owner.

SigGen: The data owner after generating the keys, will provides its own identity that it is by the true data owner, who stored it in cloud.

Challenge: Once the keys are signed by the data owner, TPA wants to verify the data. So data owner sends a request to TPA regarding this. The TPA in turn will send a challenge message to the CSP.ProofGen: Once the CSP receives the challenge message from TPA, the CSP generates the proof and responds to TPA.

ProofVerify: On receiving the proof the TPA verify the proof and finally it provides result to the data owner.

The proposed algorithm not only provides secure audit of cloud data but also prevents access to unauthorized users.

Algorithm stores data in cloud storage is as:

A. *Start*
B. *Trusted authority generates global parameters for TPA and provides certificates to data owners.*
C. *Data owner select file an split it into number of blocks*
D. *Encrypt the blocks of file*
E. *Generate hash value for each block of file*
F. *Generate signature*
G. *Store encrypted file at cloud storage*
H. *End*

Algorithm to perform audit operation is as:

A. *Start*
B. *If data owner requires to perform audit*
C. *Send the signature to TPA*
D. *TPA requests for data to CSP*
E. *The TPA send challenge message to CSP*
F. *TPA verifies data integrity*
G. *CSP generates proof and responds to TPA*
H. *TPA sends verified proof to data owner*
I. *End*

Algorithm to search over encrypted data is as:

A. *Start*
B. *Data Accessor sends relevant query in encrypted form*
C. *Encrypted query evaluated at CSP*
D. *Results are generated in encrypted form*
E. *Results in encrypted form are send to data accessor*
F. *Data Accessor decrypts results*
G. *End*

Execution flow of secure system model is shown in algorithm. Steps of algorithm are essential to prevent from unauthenticated users and impartial auditing by data owners into the cloud. Behalf of the two

categories either public or private auditing, the public auditing is chosen by most of the researchers to provide a secured transaction and a secured integrity checking.

4.1 BASIC AUDITING PROTOCOL

The basic auditing protocol by using all the semantics of a cloud storage auditing protocol. Figure 3 shows Framework of basic auditing protocol. TPA=(KeyGen,Outsource,Audit,Prove,Verify)

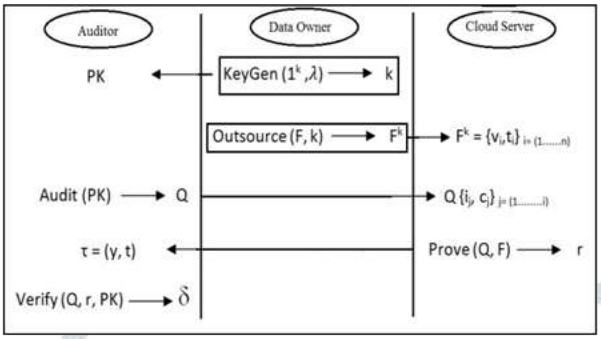


Figure 3 Framework of Basic Auditing Protocol

KeyGen(1k, λ) → K: The Data owner generates two random (safe) primes p, q of length k/2 each and then sets N = pq. In addition to k, assume an additional security parameter λ to generate the file identifier e, a prime number of (exactly) λ + 1 bits, greater than 2λ. Then the data owner determines the block length n and the total number of blocks m. The client also chooses g,g1,...,gn,h1,...,hm at random (in Z∗ N). The public key is PK = (N,e,g,g1,...,gn,h1,...,hm) and the secret key is SK = (p,q). Denote the key by K = (SK,PK).Outsource (**F; K) → F∗**: On input the data F to be outsourced, the client divides F into a collection of vectors **{vi = [vi1,...,vin]}i=1,2,...,m .** For each vi, compute its signature as follows. First, generate a random integer **si ∈ Ze** uniformly. Use the Chinese remainder theorem to calculate **xi ∈ZN** by solving as given in equation 1.

$$x_i^e = g^{s_i} \cdot (\prod_{j=1}^{n} g_j^{v_j}) \cdot h_i \bmod N. \qquad (1)$$

Then the signature for **vi is ti = (si,xi**). The client then outsources the processed data

F∗ = {vi,ti}i=1,2,...,m to the cloud server. Audit (PK) → Q: Based on the public key PK provided by the client, the auditor runs this algorithm to generate a collection of indices and coefficients {ij,cj}j=1,2,...,l where 1 ≤ ij ≤ m, cj ∈ N and l is the number of blocks the auditor queries. The auditor sends the queryQ =

$$x = \frac{\prod_{j=1}^{l} x_{i_j}^{c_j}}{g^{s'} \prod_{j=1}^{n} g_j^{w'_j} \prod_{j=1}^{m} h_j^{w'_{n+j}}}. \qquad (2)$$

{ij,cj}j=1,2,...,l to the cloud server. Prove (Q, F∗) → Γ: On receiving an audit query Q = {ij,cj}j=1,2,...,l, in which l is the period of the audit query. The cloud server first finds the signature (sij,xij) for every queried statistics block. like linear network coding operations, the server then computes x using equation 2. The server extracts the first n entries of w as a vector y ∈ Zn e and the signature of y is t = (s, x). The server sends back Γ = (y,t) as a evidence of the corresponding query confirm(Q, Γ; PK) → δ: On enter of an audit question Q = {ij,cj}j=1,2,...,l, The server's proof Γ = (y,t), the auditor constructs a vector w such that the

first n entries of w are the same as y, the (n + ij)-entry is cj, and all different entries are 0. If they're identical, the integrity of the file is verified as accurate and output δ = 1; else, the integrity of the file is verified as wrong and output δ = zero.

5 CONCLUSIONS

In cloud garage carrier, the statistics integrity of far-off verification is a critical issue. The concept of public audit solves data integrity problem via far off verification of shared statistics. look at unique consultant methods and analyze these processes. assessment desk certainly recognizes the advantages and disadvantages of every technique. Public auditing schemes want to ensure statistics privacy, offer clean accessibility, and save you from unauthenticated person. A relaxed and green privacy preserving public auditing scheme has been proposed. It achieves privateness preserving and public auditing for cloud by the usage of a 3rd birthday celebration Auditor, which does the auditing without retrieving the data copy, as a result privateness is preserved. The statistics integrity is tested by using TPA on request of the patron with the aid of verifying both the signatures. the public auditing is chosen via most of the researchers to provide a secured transaction and a secured integrity checking.

In destiny, the information security and privacy may be enhanced with modern-day auditing strategies for cloud computing and cozy cloud framework can be formed from un-legal users.

6.REFERENCES

[1] Xu, Y., Zhang, C., Wang, G., Qin, Z., & Zeng, Q. (2020). A Blockchain-enabled Deduplicatable Data Auditing Mechanism for Network Storage Services. IEEE Transactions on Emerging Topics in Computing, 1–1. doi:10.1109/tetc.2020.3005610

[2] Xu, R., & Joshi, J. (2020). Trustworthy and Transparent Third-party Authority. ACM Transactions on Internet Technology, 20(4), 1–23. https://doi.org/10.1145/3386262

[3] Mahdavi Hezavehi, S., & Rahmani, R. (2020). An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments. Cluster Computing. doi:10.1007/s10586-019-03031-y

[4] Okikiola, F. M., Mustapha, A. M., Akinsola, A. F., & Sokunbi, M. A. (2020). A New Framework for Detecting Insider Attacks in Cloud-Based E-Health Care System. 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS). doi:10.1109/icmcecs47690.2020.240889

[5] Sookhak, Mehdi, Abdullah Gani, Muhammad Khurram Khan, and Rajkumar Buyya. "Dynamic remote data auditing for securing big data storage in cloud computing." Information Sciences 380 (2017): 101-116

[6] Kim, Daeyeong, Hyunsoo Kwon, Changhee Hahn, and Junbeom Hur. "Privacy-preserving public auditing for educational multimedia data in cloud computing." Multimedia Tools and Applications 75, no. 21 (2016): 13077-13091

[7] Ateniese, Giuseppe, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik. "Scalable and efficient provable data possession." In Proceedings of the 4th international conference on Security and privacy in communication netowrks, p. 9. ACM, 2008

[8] Shimbre, Nivedita, and Priya Deshpande. "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm." In Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on, pp. 35-39. IEEE, 2015

[9] Cao, Ning, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." IEEE Transactions on parallel and distributed systems 25, no. 1 (2014): 222- 233

[6] Lordemann, David, Daniel Robinson, and Paul Scheibe. "Method and system for establishing an audit trail to protect objects distributed over a network." U.S. Patent Application 09/952,696, filed September 14, 2001

[7] 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

[8] Li, Ling, Lin Xu, Jing Li, and Changchun Zhang. "Study on the third-party audit in cloud storage service." In Cloud and Service Computing (CSC), 2011 International Conference on, pp. 220-227. IEEE, 2011

[9] Yu, Yong, Lei Niu, Guomin Yang, Yi Mu, and Willy Susilo. "On the security of auditing mechanisms for secure cloud storage." Future Generation Computer Systems 30 (2014): 127-132

[10] Yang, Guangyang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu, and Rong Hao. "Enabling public auditing for shared data in cloud storage supporting identity.