Trust and Reliability Ccontrol by Ccontinuous Auditing: Ensuring Cloud Security

Miss. Priyanka.S.Lahase.
M.E.(final yr) Student, Department of Computer Engineering, Shri Sant Gajanan Maharaj Collge of Engineering, Shegaon,Maharashtra, India.
Dr.N.M.Kandoi.
Professor, Department of Computer Engineering, Shri Sant Gajanan Maharaj Collge of Engineering, Shegaon, Maharashtra, India.

Abstract— Cloud computing, an emerging technology is being widely used for outsourcing the data into the cloud instead of storing it in the local physical storage. It can be accessed by either individual user or group of users. Cloud service providers must concern about the privacy, security and data auditing of the outsourced data. Service availability failure and the data loss is possible is due to the malicious intruders in the cloud environment. As the clients no longer have physical possession of data, the integrity and security of data become the major concern in the cloud computing. One of the important security concerns is to verify the integrity of data stored on cloud. This is paper proposed that various criteria should be continuously audited. Yet, reveal that most of existing methodologies are not applicable for third party auditing purposes. Therefore, propose a conceptual continuous auditing architecture, and highlight important components and processes that have to be implemented. Finally, discuss benefits and challenges that have to be tackled to diffuse the concept of continuous cloud service auditing. Also contribute to knowledge and practice by providing applicable internal and third party auditing methodologies for auditors and providers.

Keywords- cloud computing, continuous auditing, security, encryption.

I. INTRODUCTION

Cloud computing is a style of computing where anyone can easily obtain and access the computing resources anytime. It is cheaper and simple to use and work with it. Cloud computing permits global, expedient, on-demand service network access to a shared pool of configurable computing services (e.g. networks, servers, storage, applications, and services) which can be quickly delivered with nominal managing efforts or service provider collaboration. Making use of the cloud saves both users time and money. The term cloud is widely used as a metaphor on the Internet, so it is the type of Internet based computing, where different amenities such as servers, storage and applications are distributed to an organization's computers and devices connected to the Internet.

Cloud computing is a highly capable for the Information Technology (IT) applications; yet, there is some difficulties to be resolved for individual users and enterprises to store data on cloud. Most significant barriers to acceptance of data security, which is accompanied by problems including compliance, privacy, faith, and legal staples. Hence, vital goals are to preserve the security and integrity of data stored on cloud.

The primary matters in cloud is data security which consist of data confidentiality, data protection, data availability, data location, and secure communication. The security tasks in the cloud contains threats, data damage, service interruption, external malicious attacks, and multitenancy problems. Data integrity of cloud computing means that preserving information from alteration. Data should not be misplaced or altered via any illegal users. Cloud service providers are trusted to preserve a data integrity and accuracy. Data privacy is as well a significant to users who used to accumulate their important or private information in cloud. Verification and access control methods are performed to confirm data secrecy. The secrecy, verification, and access control security problems in cloud computing due to increasing the cloud reliability and trustworthiness needs to be addressed. To deal with secure data storage, the auditing for stored data in cloud is one of the new concept introduced in Cloud computing. Auditing is a method

of verifying the user's data which can be accepted either by the user itself (data owner) or by TPA. It benefits to preserve the honesty of data stored on cloud.

II. Related Work

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.

"In this section, we briefly review the related work on Auditing system and their different techniques.

Ateniese et al. [1] to accomplish public auditing is designed to check the correctness of data stored in an untrusted server, without downloading the whole data. In these mechanisms, data is separated into number of blocks, where individual block has individually signed by the data owner; and a casual grouping of all the blocks in its place of the entire data is recovered through integrity examination. A public verifier might be a data user (e.g. investigator) who may like to verify the owner's data.

Wang et al. [2] has proposed a public auditing mechanism for cloud data. Through public auditing on cloud data, the content of remote data belonging to an individual user is not revealed to any community verifiers. Inappropriately, current public auditing solutions revealed above only emphasis on private data in the cloud. Allotment of data between several users is possibly one of the most attractive feature that inspire cloud storage. Therefore, it is also crucial to confirm the honesty of public data in the cloud is precise.

Wang et al. [3] has planned a system where they utilized ring signature concept to construct homomorphic authenticators named as Oruta. A public verifier is validating the honesty of shared data without downloading the entire data. The individuality of the signer on every block in shared data is reserved private from the public verifier. So, TPA and Cloud service provider has no knowledge about the user's data.

X. Jia et al. [4] claimed that the public auditing protocol can resistant against several known attacks. But, this protocol is susceptible to existential imitations known as message attack from a malicious cloud server and an outdoor attacker. The cloud server can alter the outsourced data as needed when possessed. Besides, the spiteful cloud server can permit the auditing from TPA once it drops the outsourced data. In addition, the attacks done through the malicious codes on cloud server, this protocol is susceptible to occurrences from an outdoor attacker. Even if the cloud server is trusted, the external attacker can intrude for data directed by the user to the cloud server in Tag Block step and adjust it arbitrarily. Additionally, the outdoor attacker can just eavesdrop on that data and forge with deal of data. Thus, it is indirectly affecting the secrecy and integrity of data.

Srijanya et al. [5] performs public auditing by introducing a TPA. It provides auditing service which is achieved by making use of Merkle Hash Tree. Users generate public and private key using KeyGen. It computes signature on each block and generates a root R then signs the root R using the private key and sends it to server. User and TPA might validate the honesty of outsourced data by challenging the cloud server. Thus, it provides assurance of public auditability for storage accuracy of data. But the root key generation process used is time consuming whereas the confidentiality of data is not maintained. It does not even support batch auditing.

Tejaswani et al. [6] has proposed a privacy preserving public verifiability for integrity of data storage in cloud using Merkle hash tree whereas the confidentiality of data is achieved using RSA based cryptography algorithm. In this proposed method, user first generates public and private key and then encrypt the file along with computing signature over the encrypted file. User sent the signature and public key to TPA. After that TPA creates a task and sent to the server. Server computes comeback and provides it to TPA. Later TPA checks the integrity of data comparing response with signature. The proposed approach is secure. Also, integrity and confidentiality of data is achieved. It does not support data dynamics along with batch auditing.

Yuan et al. [7], a single cloud node is used to keep track of validation tag which was last updated by the rescinded users. In this situation, if the cloud node answerable for tag update is negotiated due to some inside faults or outdoor attacks, the revoked user will be able to produce legal validation tags gain.

Wang et al. [8] has also proposed a design that permits the users to examine the data stored in the cloud storage. This technique may useful to detect the modified blocks simply using homomorphic token pre-computation technique and then erasure coded method is used to get the chosen blocks from multiple servers. To accomplish data storage correctness and data error localization at the same time, it makes use of precompiled verification tokens.

He et al. [9] proposed a scheme in which data owner encrypts the information file first by using renewing code and then coded file will get stored transversely on multiple cloud servers. Multiple cloud servers may suggest similar service provider or different service providers. Data owner may perform a block-level dynamic operation on the outsourced data as block modification, insertion, and deletion. Auditor could cleverly authenticate integrity of data stored on multiple cloud servers; again, data file is frequently modernized by data owner. The secrecy and honesty of data stored in cloud are the reputation perceptions in cloud computing.

More et al. [10] has proposed a mechanism using a MHT and RSA algorithm. In their system, she has implemented a system which provides a public auditability for static data only. If the owner makes some changes in original file then TPA fails to give the appropriate result. Again, it fails to provide batch auditing.

III. PROPOSED APPROACH:-

Cloud computing is a modern technology which is growing rapidly throughout the world. The users make use of cloud storage to save the data on cloud and that can be accessed from anywhere and anytime. But at the same time, user is mostly concerned about the validation of data which stored in the cloud. Therefore, to check the validation of data (auditing), an entity called Third Party Auditor (TPA) is used. There are various privacy preserving data auditing schemes which have their own benefits and limitations. Therefore, there is a need to develop auditing scheme which overcomes all these limitations of existing approaches. A new privacy preserving and dynamic public audit service for secure cloud storage is proposed which is secure and efficient to use. It consists of three key units: data owner, TPA, and cloud server. Data owner does several actions as piercing a file into blocks, encoding it, producing a hash value for each block, merging it, creating a signature on it and does dynamic data processes such as adding, modifying, deletion of data. TPA does validation of data while performing various activities such as producing hash value for encrypted blocks which is acknowledged from cloud server, merged them then generating new signature on this. After words, it matches both the signatures to check the correctness of information. Validation of data done either periodically or on user's demand. Cloud server saves the encoded blocks of file. The main objective is to develop an audit service which holds the abilities as privacy preserving, public auditing, and data integrity along with privacy.

Propose a new approach in the challenge of data ownership and cryptography to manage the storage of encrypted data with Data Auditing. We are motivated to save data in the cloud and to preserve the privacy of data owners by proposing a scheme to manage the storage of encrypted data with auditing. We test safety and evaluate the performance of the proposed scheme through analysis and simulation. The results show its efficiency, effectiveness and applicability.

System Diagram:

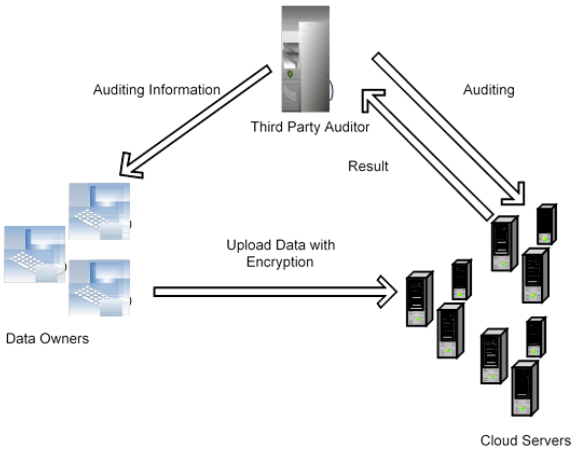

Fig 1. System Architecture

Proposed Methods

1. AES Algorithm for Encryption.

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input:

128_bit /192 bit/256 bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process:

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round:10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output:

cipher text(128 bit)

2. FRAGMENTATION ALGORITHM

Input: File

Output: Chunks

Step1: If file is to be split go to step 2 else merge the fragments of the file and go to step

Step2: Input source path, destination path

Step3: Size = size of source file

Step4: Fs = Fragment Size

Step5: NoF = number of fragments

Step6: Fs = Size/Nof

Step7: We get fragments with merge option

Step8: End

3. MD5 (Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Steps:

1. A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.

2. The output of a message digest is considered as a digital signature of the input data.

3. MD5 is a message digest algorithm producing 128 bits of data.

4. It uses constants derived to trigonometric Sine function.

5. It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.

6. Most modern programming languages provides MD5 algorithm as built-in functions

Conclusion

A new secure and privacy preserving public auditing service is proposed. Privacy preserving public auditing is accomplished with the help of TPA. TPA performs auditing without retrieving the data, therefore preserving the privacy of the data. In this scheme, the data are split into multiple blocks and then stored in the encrypted format at cloud server for storage, thus the secrecy of data is maintained. The modification of data is verified by TPA on request of the data owner by comparing both the signatures, one which is produced by data owner and the other generated by TPA. It only verifies whether the stored data is altered or not and notifies the result to the data owner.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable Data Possession at Untrusted Stores,‖ Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-610, 2007.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ―Privacypreserving public auditing for secure cloud storage,‖ IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, Feb. 2013.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, ―Toward secure and dependable storage services in cloud computing,‖ IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, Apr. 2012

[4] K. Yang and X. Jia, ―An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing,‖ IEEE Transactions on Parallel and Distributed Systems, 2012.

[5] Srijanya K and N. Kasiviswanath, ―Data Integrity Verification by Third Party Auditor in Remote Data Cloud,‖ International Journal of Soft Computing and Engineering, 3(5), 2013.

[6] V. Tejaswini, K. Sunitha, and S. K. Prashanth, ―Privacy preserving and public auditing service for data storage in cloud computing,‖ ParipexIndian Journal of Research, vol. 2, no. 2, pp. 131–133, Jan. 2012.

[7] J. Yuan and S. Yu, ―Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification,‖ IEEE Transactions on Information Forensics and Security 2015.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ―Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,‖ IEEE Transactions on Parallel and Distributed Systems, 22(5):847–859, 2011.

[9] K. He, C. Huang, J. Shi and J. Wang, ―Public Integrity Auditing for Dynamic Regenerating Code Based Cloud Storage,‖ IEEE Symposium on Computers and Communication (ISCC), 2016.

[10] S. More and S. Chaudhari, ―Third Party Public Auditing Scheme for Cloud Storage,‖ Procedia Computer Science, vol. 79, pp. 69–76, 2016.