Enabling Multi-level Integrity Verification Scheme for Secure Cloud Data Storage

[1]Mrs. L.B.Lisha, [2]Ms. Jeslymole James

[1]Assistant Professor, [2]PG Scholar
Department of Computer Science and Engineering,
Marthandam College of Engineering and Technology, Kuttakuzhi, India

***Abstract*: Cloud Computing enables the remote users to access data, services, and applications in on-demand from the shared pool of configurable computing resources, without the consideration of storage, hardware and software management. On the other hand, it is not easy for cloud users to identify whether Cloud Service Provider's (CSP) tag along with the data security legal expectations. User data privacy is essential in the cloud storage for protecting the user data in the cloud server. Register the user's data and accessing their respective data from the cloud server is an active area in the research community. Due to the data validation conditions, hardware, and operational complexity constraints, it is a challenging issue for the user to verify the integrity of data. Hence, the proposed system is a new approach named Multi-level integrity verification scheme is proposed to ensure the data integrity of the user. The main focus is to protect the user data privacy, and to forward the user signature and the files from the user to the Cloud Server Provider (CSP) and Third Party Auditor (TPA). The user files are verified based on the dual control mechanism and the file signature is verified by the Cloud Server Provider. The privacy of the signature information and the cloud storage space utilization is effectively enhanced.**

***Keywords*: Csp, Cloud Data Privacy, Multi-Level Integrity Verification**

1. INTRODUCTION

Nowadays, it has become a common practice for education, healthcare, and other sectors to utilize the cloud environment for storing and processing the business data, for acting as a backup repository to personal data such as photographs, mail archives, contact details, and so on. Cloud services provide a massive amount of computing resources and storage space, which makes the users eliminate the accountability of maintaining data at local machines. So, users completely depend on the cloud services for their data storage, availability, and integrity. Even though cloud computing infrastructures and service providers are much reliable and powerful, a wide range of threats for data integrity exists. When the integrity verification is performed with data retrieval, overutilization of network bandwidth and communication cost overhead problems occur. Blockless verification has been proposed, where the metadata has been utilized to audit the outsourced data. The idea leads to problems such as Metadata maintenance, interpreting or obtaining the original data by the third party entities, communication and computation overhead. Addressing the gaps of the research work, the auditing of actual data blocks or replicas of data blocks seems to be lack, but these replica data blocks were only provided to various users who access the data in the servers that are geographically located near to the users. In order to ensure data reliability and availability, storing various replicas is a common approach followed in the cloud. For dynamic updates, single block update will lead to update various replicas of the concerned block. With existing schemes, verifying the integrity of the replicas seems to be communication and computation overhead. Considering the large files stored in CSP and resource constraints of DO, it is significant to develop a secure framework with efficient data auditing techniques for periodical data integrity verification. The contribution extends to provide the support of dynamic updates, error localization, data correctness, blockless verification and replica data auditing.

II. RELATED WORKS

Mehul A. Shah et al., proposed that the thirdparty auditing is important in creating an online service oriented economy, because it allows customers to evaluate risks, and it increases the efficiency of insurance based risk mitigation. We describe approaches and system hooks that support both internal and external auditing of online storage services, describe motivations for service providers and auditors to adopt these approaches, and list challenges that need to be resolved for such audi tingto become a reality. A.P.Mohana Priya et al., introduces that every data stored in the cloud will be generated with a Hash value using Merkle Hash Tree technique. So modification in cont…,ent will make changes in the Hash value of the document as well. Proxy also perform signature delegation work by generating private and public key for every user using OEAP Algorithm so that the security will be maintained. Boyang Wang et al., exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file. Cong Wang et al., proposes that users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Yang, K. et al., design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. Chang Liu et al., Big data and its applications are attracting more and more research interests in recent years. As the new generation distributed computing platform, cloud computing is believed to be the most potent platform. With the data no longer under users'

direct control, data security in cloud computing is becoming one of the most obstacles of the proliferation of cloud. In order to improve service reliability and availability, storing multiple replicas along with original datasets is a common strategy for cloud service providers. Public data auditing schemes allow users to verify their outsourced data storage without having to retrieve the whole dataset. H. Wang. et al., Cloud computing has become an important thing in computer field. Cloud computing takes information processing as a service, such as storage and computing. Data integrity is important thing in cloud storage. In certain situations, clients should store their data such as image or text in multi cloud. When the client stores his/her data on multi-cloud servers, the distributed storage and integrity checking is very important. Here we propose an Identity Based Distributed Provable Data Possession (ID-DPDP) protocol for multi-cloud storage.

III. PROPOSED SYSTEM

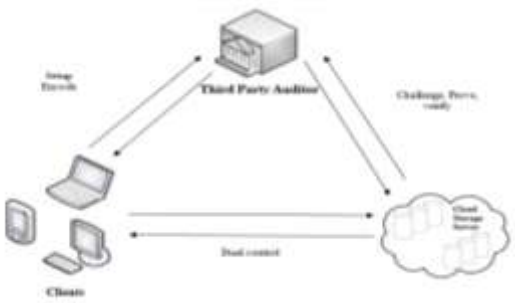

Fig 1: Block Diagram

Multi-level integrity verification approach is proposed to confirm and guarantee the information respectability of the client. The information honesty confirmation plot is basically utilized in the distributed storage to ensure the client information protection. In the distributed storage, the client needs to enroll their record and their own information to the cloud server. The general method of the proposed information honesty approach is performed utilizing six significant stages, for example, Setup (), Encode (), Dual control (), Challenge (), Prove () and Verify ().The username and the secret key of the client is confirmed and put away into the CSP of the distributed storage in the Setup stage. The bit sifting based check approach is utilized in the Encode stage to segment the client information document into the information squares. The client advances the review solicitation to the TPA for confirming the client record and along these lines, the TPA sends the test to the CSP in the Challenge stage. In the Verify stage, the TPA checks the client records dependent on the double control system, and the Dual control eliminate is conveyed inside the Prove stage. In light of these stages, the information trustworthiness confirmation plot utilizes three element members, to be specific CSP, User, and TPA. By pleasing these stages, another convention is created utilizing another numerical model, where various variables and parameters, for example, meeting passwords, Chebyshev polynomial, hashing activity, and ECC are utilized alongside the Kernel separating hypothesis.

IV. METHODOLOGY

In Cloud Storage Server (CS), information records in huge will be put away by DO. Since the information isn't put away locally, customers need to guarantee the rightness of the information put away and kept up in the cloud. It isn't plausible for DO to check all put away information occasionally with time and asset limitations. In this way, the undertaking can be depended to Third Party Auditor (TPA). TPA is unprejudiced when CS isn't trusted. DO will get to CS to store, recover, or update information documents. The information uprightness dangers making progress toward DO information records can be as inward and outer assaults in CS. The assaults might be bugs in either programming or equipment or system configuration, hacking, pernicious exercises, and so forth... Further, CS might act naturally focused. CS may even choose to shroud the imperfections or loss of information upkeep, so as to keep up a notoriety among DO's. To pick up trust in the cloud, TPA administration can be utilized to perform visit inspecting. In the proposed model, uncovering facilitated information to TPA or outer gatherings is in no utilization, since the information will be in scrambled structure and away request. CS and TPA even together can't recover the genuine information put away in the cloud, with the metadata data accessible. Since the proposed framework uses diverse square requesting for capacity and inspecting. DO can give TPA's open key to CS for approving the reviews performed by TPA.

Setup phase

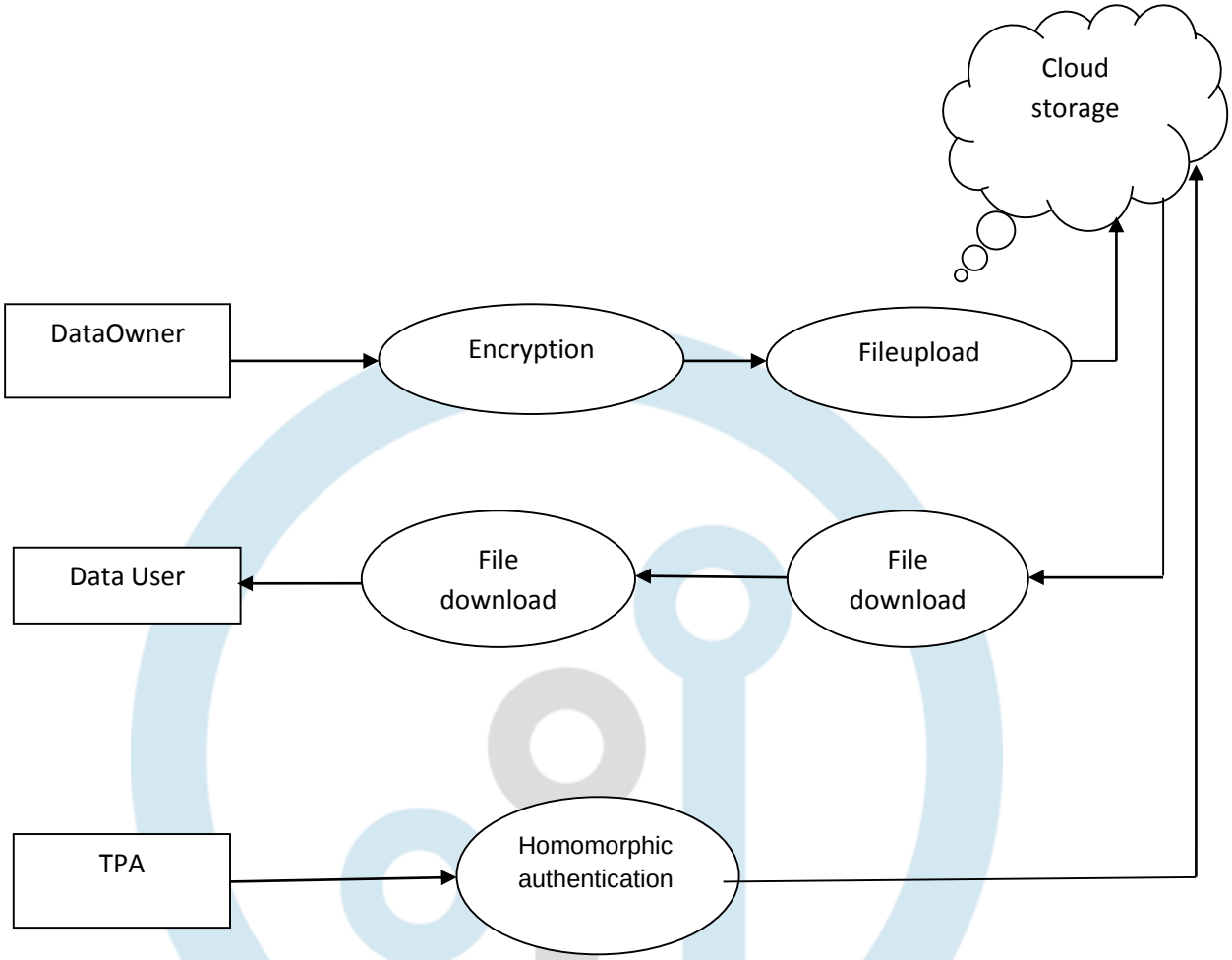

Fig 2: Process Flow

In the Setup stage, the username and secret word of the client is made and is traded among the CSP and the client element members. In like manner, the meeting secret word and the private key for client is additionally made and put away in the element members. Besides, the name, private key and the meeting secret word for TPA is made and confirmed by the TPA substance. At first,the client certifications, as username and the secret key are made by the client and sent it to the CSP substance. The CSP stores the username and secret word of the client and make a meeting secret phrase for the client and forward the client meeting secret word to the individual client. It exhibits the image depiction of the proposed trustworthiness check approach. The client meeting secret key is made by the CSP substance by playing out the Ex-OR activity with the ECC encryption and the hashing capacity, which is specified as,

$$U_{pwdses} = C\left[pb_{key} \,//\, S_{pvtkey}\right] \oplus h\left(cby_{pynl}^{user}\right)$$

The CSP creates the user private key by performing the Ex-or operation with the hashing of user password and the ECC encryption of the server private key, which is expressed as,

$$U_{pvtkey} = h\left(U_{pwd}^{*}\right) \bmod p_1 \oplus C\left(S_{pvtkey}\right)$$

Encode Phase

In the Encode stage, the client segments the information record *B* into *I* number of information squares. Let *I1*,*I2*,*I3*,… .In indicates the information squares and the marks, for example, *D1*,*D2*,*D3* and *D4* are processed dependent on the information obstructs in the Encode stage. The mark D1 is registered by adding the information squares and hashing the chebyshev polynomial of client with the username, which is represented as,

$$D_1 = \left(\sum_{k=1}^{l} I_k \oplus I_{k+1} \right) \oplus h\left(U_{name} // cby_{pyml}^{user*} \right)$$

When the marks are send to the CSP element at that point, the Challenge () stage starts to process its capacities. In the Challenge () stage, the client communicate the Aud req to the TPA to play out the confirmation procedure. The TPA gets the Aud req and confirms it to validate the character of client. When the client personality is confirmed, the TPR communicate the Challreq to the CSP substance. The test is communicated by the TPR to the CSP element in the Challenge () stage. In the Prove stage, the CSP acknowledges the Chall req, which is send by the TPR through the validation. The CSP produces the document signature for the relating Chall req and communicate the record mark to the TPA element. The summation of the information squares and the complete got information squares are permitted to play out the EX-OR activity. The username put away in the CSP substance is linked with the chebyshev polynomial for client and the outcome is applied into the hashing capacity. The document marks are created by the CSA in the Prove stage and are communicated to the TPA. In the confirm stage, the TPA gets the record marks, which is send from the CSA and checks the information documents dependent on the double control component

Dual control phase

In the Dual control phase, the dual control mechanism is carried out for verifying the file signatures, which are generated by the CSP entity. The intermediate message X1 is computed using the below expression as,

$$X_1 = D_1 \oplus D_2$$

The intermediate message X2 is computed as,

$$X_2 = D_1^{-} \oplus D_2^{-}$$

The intermediate message X1 and X2 are compared, if X1 = X2 then, it is considered as verification-1. Moreover, the intermediate messages X3 and X4 are computed as,

$$X_3 = f\left(D_3 // D_4 \right)$$

$$X_4 = f\left(D_3^{-} // D_4^{-} \right)$$

The intermediate messages X3 and X4 are compared, if X3 = X4 then,verification-2 terminates. Hence, in the dual control mechanism, the verification is performed at two levels.

CONCLUSION

The proposed system is an acquisition and transmission in an IaaS cloud environment, a novel framework that allows forensic evidence to be acquired and transmitted between trusted platforms is presented. Forensic data are transmitted as streaming data, in which the data integrity information is generated as the fragile watermarks. The benefits of using the watermarks allow custodians to verify the data integrity, as well as detect and localize malicious modification at run time. To transmit forensic data as a data stream and verify its integrity at the same time, a unique watermark is embedded into the data stream without altering the data itself. While using the fragile watermarking it is crucial to restore the original image without any distortions. Reversible watermarking is designed so that it can be removed to completely restore the original image. The prototype of the system has been implemented in an IaaS cloud environment, whose security properties have been proven by formal security protocol verifiers.

REFERENCES

[1] S. T. King, P. M. Chen, Y.-M. Wang, C. Verbowski, H. J. Wang, and J. R. Lorch, "SubVirt: Implementing malware with virtual machines," in Proc. IEEE Symp. Secur. Privacy, May 2006, pp. 314–327.
[2] V. Ciancaglini, M. Balduzzi, R. McArdle, and M. Rösler. (2015). Below the Surface: Exploring the Deep Web. [Online].
[3] Symantec. Avoiding the Hidden Costs of the Cloud. Accessed: Aug. 1, 2018. [Online]. Available: https://www.symantec.com/content/ en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf [4] R. Samani and F. Paget. (2013).
[5] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS attacks and defenses," in Proc. Int. Conf. Inf. Soc., Jun. 2013, pp. 67–71.
[6] D. Goodin. ZeusBot Found Using Amazon's EC2 as C&C Server. [Online]. Available: ttp://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/
[7] M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," J. Syst. Softw., vol. 86, no. 9, pp. 2263–2268, Sep. 2013.
[8] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, Mar. 2012.
[9] NIST Information Technology Laboratory. (2013). NIST Cloud Computing Forensic Science Challenges. [Online]. Available: http://csrc.nist. gov/publications/drafts/nistir-8006/draft_nistir_8006.pdf
[10] U. S. Congress. (2018). Cloud Act. [Online]. Available: https://www. congress.gov/bill/115th-congress/house-bill/4943
[11] Forensics at the OJ Simpson Trial. [Online]. Available: https://www.crimemuseum.org/crime-library/famousmurders/forensicinvestigation-of-the-oj-simpson-trial
[12] Wang C., Wang Q., Ren K., Lou W., "Privacy-preserving public auditing for data storage security in cloud computing", IEEE proceedings in infocom, pp. 1–9, March 2010.

[13] Worku S.G., Xu C., Zhao J. and He X., "Secure and efficient privacy-preserving public auditing scheme for cloud storage", Computers & Electrical Engineering, vol. 40, no. 5, pp.1703-1713, 2014.
[14] Duan Qiang, Yuhong Yan, and Athanasios V. Vasilakos, "A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing," IEEE Transactions on Network and Service Management, vol. 9, no. 4, pp. 373-392, 2012.
[15] Rajak S and Verma A, "Secure Data Storage in the Cloud using Digital Signature Mechanism," International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, no. 4, 2012.