International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S3, September 2019

Integrity Verification Mechanisms Adopted in Cloud Environment

Shakti Arora, Surjeet Dalal

Abstract: ***Cloud computing has changed the shape of computing world. Now a-days users are not worried about the computational cost and infrastructure cost because of the maximum availability of all the resources are available on demand. The most widely used feature used by the users are storage as a service given by the cloud computing providers. Users can upload and access the data anywhere anytime time with the help of internet access. As with the usability of the storage as a service, is increasing the risk of security of the information are also increasing. Data security on the cloud is the prominent area for researchers and number of techniques and algorithms has been proposed to assure the integrity, consistency and data availability. In this paper a number of data auditing mechanism used by different cloud providers have been discussed and optimized integrity verification mechanism have been proposed to overcome the limitations of existing approaches. The communication overheads are compiled and calculated with different input data size. A comparative analysis is also prepared to justify the proposed approach.***

I. INTRODUCTION

Cloud computing is model of granting access of pool(shared) of resources to the users , these resources could be network, applications, storage, servers and services with the management of service providers. Cloud computing is not a newly invented technology but a modern way of incorporating new technologies. The advantages of cloud services are that technology and resources can be used more efficiently as per the demand. Clouds have few important characteristics that make it useful for consumers. First it can be accessed directly from anywhere at any location without intervention of human beings or any third entity (on demand service)[1]. It can be accessed and operated on any of the network like phone, laptop, desktop (called broad network access). A multi-tenant model is adopted by the cloud service provider to serve the request of cloud consumers (called Resource pooling). The cloud networks can be changes easily according to the requirements of the cloud consumer (called rapid elasticity). A transparent feedback system is maintained between cloud consumer and cloud service provider with metering capability of the cloud computing.

Manuscript published on 30 September 2019.
***** Correspondence Author (s)
Shakti Arora, Research Scholar, Department of Computer Science, SRM University, Sonepat, Haryana 131029, India. (Email: shakti.nagpal@gmail.com)
Dr. SurjeetDalal, Associate Professor, Department of Computer Science, SRM University, Sonepat, Haryana 131029, India. (Email: profsurjeetdalal@gmail.com)

In cloud computing all the resources, services and processing power is shared with number of users at the same time. Numbers of entities are accessing the same resources at a global level. So there should be a strong security mechanism which can maintain the privacy of all the users and their information at the same time. There is few security parameters that need to be considered are as follows: Privacy-The information should only be available and accessible to confidential entities or authentic entities. None of the un-authorized users can get the access to the private/ sensitive information of the users. Integrity-The state of the information is not allowed to be changed at any level without the permission of the owner. It provides the confirmation about the originality of the content stored on the server [1]. Accessibility/Availability-It assures that information will be available to the users at all the time. A number of users are accessing and sharing the resources at the same time so chances of unavailability of resources are very high.

II. RELATED STUDY

Aldossary and Allen (2016), in their research identified the various issues that are restricting the adaptation of cloud computing. In that research, they provided the solutions that are used to reduce the threats on the survey issues. For instance, the data should remain confidential, protect data integrity and should available round the clock. In addition to that, sharing the stored data in the cloud server is quite unsafe due to service providers are unreliable and very difficult to attain proper validation and authorization of the users. The authors prepared the list of issues associated with the stored data and provided the answers to these issues. Barla and Veladanda (2014) developed a technique to share data in N number of parties. This technique is used distribute these identity digit ranging from 1 to N and similarly put on encryption on private data. These projects are unidentified in that the characteristics received are unidentified to the other participants of the group. Private networks are used between other members to verify the information theoretic sense. This kind of sequential figures assignment permits additional multifarious information to be pooled and has applications to other complications in privacy. Al-Saiyd and Nada (2013), studied the various security threats in the cloud computing, they developed a cloud computing life cycle model to ensure safety and allow the consumers take benefits of the cloud. A data reliability check algorithms, which ensures the third party to data safeguard the static and dynamic data from illegal surveillance, alteration, or intervention.

Geeta et al. (2018) did the detailed survey of data security and auditing techniques and gave forthcoming future directions in data auditing and security. Sivakumar et al. (2018), presented a survey of various cloud Encryption Algorithms. Encryption is the technique to covert the data/information into codes so that the personal is authorized can see it with the help of key and the unauthorized users cannot use that data. Encryption protects the data and if the unauthorized users try to use that data he cannot decrypt the data in the useable form. Wahid et al. (2018) also defined the Encryption process is encoding information that will prevent unapproved access of information. They applied many cryptographic algorithms and the results obtained from the analysis were discussed. DES, 3DES, AES, RSA and blowfish cryptographic algorithms performance were compared in relation to their merits and demerits. Goubin and Martinelli (2011), performed the security analysis to equate it's to Boolean masking. The result of the study provided that the first order Boolean masking provides the equal safety as of 3rd up to 4th order. The growth of the cloud computed is obstructed by the security issues. Most of the researcher and industries are not willing to trust on the cloud computing (Fernandes et al. 2014). The security rules and regulation framed by the cloud providers are commonly clear to all the clients. Due to large number of users that are present in the system makes the cloud computing more unsecure[2]. Jouini and Rabai (2019), addressed the security problem in in could security and give the solution to these security problem by means of quantitative security threat measurement model. This model is named as Multi-dimensional Mean Failure Cost (M2FC). The stress is also given on various security issues pertaining to cloud computing and proposed a generic framework to assess the cloud security and gave suitable technique to resolve these security related issues. According to CSA (2013), Cloud Security Alliance (CSA) out of total nine threats data loss as well data breaches are main security issues on the cloud computers. These security threats are due to different kind of complication on cloud server. Samarati and Vimercati (2016) studied the various security related fears and issues increasing in the present scenario specially in processing the data and storage and management of stored data. Coppolino [4] et al. (2016), gave new guideline to cloud security research, in their research they summarized the key research directions and most popular research. They analyzed three different attacking vectors and provided the list of possible attacks at the same time they give the solutions to these attacks. They also suggested the novel security tools and techniques that can be developed by the researchers and industries. Ali et al. (2015) the topographical range of cloud computing gives rise to many illegal issues related to consumers assets and the rules and legislation under which they are operated[5]. The management of individual and their regulations by the service provider on the resources also play a major role in cloud security. This results in lack of control of the proprietor institute. Lu et al. (2010) research provided novel security application to protect the data in the cloud computing. As per their application the researchers proposed to classify the data and this classification can protect the data or secret files by providing them confidentiality and safety[6]. Confidentiality and safety can be maintained by offering secure verification mechanism. This will lead to protect the data on the cloud by restricting illegal operator to access. A track mechanism can be devised to resolve the dispute of the data.

III. AUDITING MECHANISM

To verify the honesty of information stored on the server or on the remote locations, a number of techniques POR, RIC, PDP are available. Client/information owner stores the data on the storage and with the help of challenge response protocol client is able to check the consistency of the data. Public auditing, dynamic auditing, collaborative auditing and batch auditing can be used to audit the data stored on the cloud.

IV. PUBLIC AUDITING MECHANISM

In the public auditing mechanism an outsider or third party is used to verify the consistency and originality of the data stored on the cloud storage. In public auditing the information owner interact with the third party and exchange the credentials. The owner of the information delegates the data auditing privileges. Third party sends the challenge to the cloud storage for generating the proof of data possessions and transfers the report of proofs to the information owner.

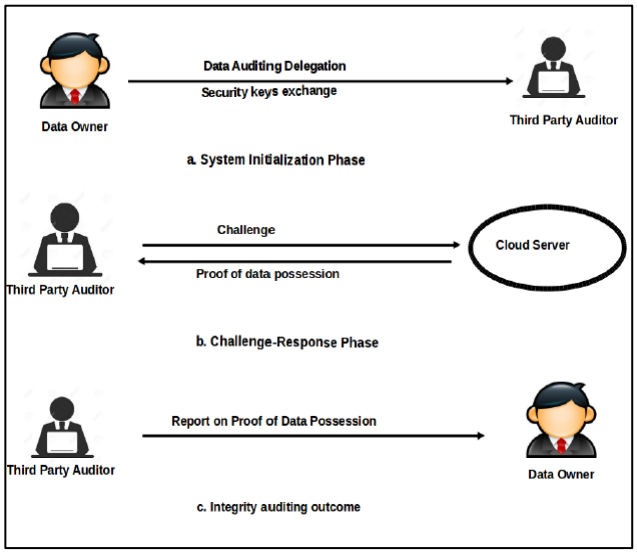

Figure 1 Public Auditing Mechanism of Data Verification

V. DYNAMIC AUDITING

The data stored on the cloud keeps on changing with the time, so the data auditing mechanism should work on the consistency of dynamic data. Data owners dynamically update their data on the cloud. The dynamic auditing protocols are designed in such manner that they can verify the appropriateness of the data updated by dynamic operations. A public homomorphic authenticator verification mechanism can be used for auditing. A chunk value is added by the data owner with the data as an authenticator to check the consistency of the data.

The authenticator value appended with each data assures the correctness of the data. Insertion and checking the authenticator with update information increases additional overheads. Replay attack and Forge attack are the two important issues that make the system insecure while dealing with dynamic updates on the storage data

VI. COLLABORATIVE AUDITING

In today's environment multi cloud architecture is adopted by the cloud users, a distribute framework with distributed database architecture for storage is provided which reduces the cost of storage and increases the availability of the data. The collaborative data auditing mechanism is required to audit the data at distant locations. In multi cloud environment TPA is responsible for data auditing and verification.

VII. BATCH AUDITING

Auditing of data storage helps the data owner to check the integrity of the data on the server. a number of data owners exist and generates a number of data auditing requests at the same time from multiple owners.in this case auditor combines all the request and perform a batch auditing for multiple data owners. The parameters initialized for tag generation are different for each owner.it becomes difficult for data auditor to combine tags from multiple owners to conduct batch auditing. In batch auditing cluster of same size of information is processed by the server in a sequence, it adds the additional complexity and transmission overheads to divide the information in same size.

VIII. METHODS OF INTEGRITY VERIFICATION& RESULTS

A number of integrity verification mechanisms are used by different researchers to verify and audit the data stored on the cloud storage. Some of the techniques are discussed below

Message authentication Code
Hash message authentication Code
Provable data possession
Pre-computed tokens
Checksum
Proof of Retrievability

Comparative analysis of integrity verification techniques

Concept	Algorithm	Advantages	Disadvantages
Strong public verification with group client repudiation	Vector commitment, asymmetric group key agreement, verifier-local revocation group signature	Avoids the collusion attack.	High computation cost.
Public verification for combined information with effective client repudiation.	Homomorphic authenticable proxy resignature scheme (HAPS), panda mechanism	Secure user revocation, public auditing.	Collusion of repudiated customer and cloud
Dynamically data sharing with security	Group initialization, batch regulation authority administration addition and elimination.	Low computational and communicational overheads.	The complexity of the security technique in communication is linear w.r.t the length of the file
Honesty examining for combined information with safe customer repudiation	Public auditing scheme, polynomial-based authentication tags	Total overhead is small	User revocation takes longer time
Protected and adaptable Information collaboration assistance in distributed computing	Collaboration service (SECO)	Secure against attacks	Data consistency is
Efficient chameleon hashing-based privacy preserving auditing	Identity based privacy-preserving public auditing protocol	Cipher text	Not achieved.
Privacy-preserving and secure data sharing in cloud	System initialization, encryption, key generation, decryption	Fragile information access control, safe against conspiracy attack	Scheme has to be implemented in real cloud platform
Short dynamic group signature supporting control label ink ability.	PS-OL scheme	Yields short signature, proves the security features.	Privacy is not preserved by global link ability

Public honesty Examining for vital information distribution with multi customer modification.	System setup, challenge, prove, validation, customer repudiation	Large error revelation probability, effective customer repudiation	Scheme does not Achieve reliability and error detection probability, achieve reliability and error detection Probability
Secrecy-conserving public inspecting convention for low-accomplishment	Secrecy-conserving public inspecting convention.	Light weight computation, supports batch auditing	Additional time cost as the number of chunks increases at the user side

IX. CONCLUSION

In this paper we studied and compared a number of auditing mechanism, with the advantages of all the techniques a number of gaps and limitations are identified. Data consistency is not assured for the outsourced data, as well as the communication cost and computation overheads are also increasing. While implementing in the real time collusion attacks and error detection probability is also very low.

REFERENCES

1. D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, (2014) Security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (2), pp.113–170.
2. Jouini, M., & Rabai, L. B. A. (2019). A security framework for secure cloud computing environments. In Cloud security: Concepts, methodologies, tools, and applications. IGI Global. pp. 249-263
3. Cloud Security Alliance – CSA, Top Threats Working Group (2013). The Notorious Nine - Cloud Computing Top Threats.
4. Samarati, P., di Vimercati, S. D. C., Murugesan, S., & Bojanova, I., (2016). Cloud security: Issues and concerns. Encyclopedia on cloud computing, pp.1-14.
5. Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L., (2017). Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering, 59, 126-140.
6. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383.
7. Lu, R., Lin, X., Liang, X., & Shen, X. S. (2010). Secure provenance: the essential of bread and butter of data forensics in cloud computing. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. pp. 282-292.
8. Somani, U., Lakhani, K., & Mundra, M. (2010). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. First International Conference On Parallel, Distributed and Grid Computing pp. 211-216).
9. Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A., (2009). Security guidance for critical areas of focus in cloud computing, v2.1. Cloud Security Alliance, pp. 25 -32.
10. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), pp.1-11.
11. Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3), pp.79-84.
12. Sato, H., Kanai, A., and Tanimoto, S. (2010). Acloud trust model in a security aware cloud. In IEEE/IPSJ International Symposium on Applications and the Internet. pp. 121-124.
13. Che, J., Duan, Y., Zhang, T., and Fan J. (2011). Study on the security models and strategies of cloud computing. Procedia Engineering, 23, pp.586-593.
14. Kuyoro, S. O., Ibikunle, F., and Awodele, O.(2011). Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), 3(5), pp. 247-255.
15. Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), pp.47-54.
16. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, pp. 88-115.
17. Morsy M. Al., Grundy J. and Müller I., (2010).An Analysis of the Cloud Computing Security Problem. Proc. APSEC Cloud Workshop, Sydney, Australia.
18. Karadsheh L. (2012).Applying security policies and service level agreement to IaaS service model to enhance security and transition. Computers & Security, 31(3), pp. 315-326.
19. Zhang, L., Y. Luo, F. Tao, B. Li, L. Ren, X. Zhang, H. Guo, Y. Cheng, A. Hu, and Y. Liu. (2012). Cloud Manufacturing: A New Manufacturing Paradigm. Enterprise Information Systems.
20. Tso, R. (2013). A new way to generate a ring: Universal ring signature. Computers & Mathematics with Applications, 65(9), 1350-1359.
21. Cheng F., and Lai W.,(2012). The impact of Cloud Computing Technology on Legal Infrastructure within Internet Focusing on the Protection of Information Privacy. Proceeding International Workshop on Information and Electronics Engineering. 29, pp.241-251,
22. Yu, Y. (2017). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), pp. 767–778.
23. Mahalakshmi B. and Suseendran, G., (2016). Effectuation of secure authorized deduplication in hybrid cloud. Indian Journal of Science and Technology, 9(25)
24. Ali, M., Khan, S. U. and Vasilakos, A. V., (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, .35, pp. 357–383.
25. Wang, B., Chow, S. S. M., Li, M., & Li, H. (2013). Storing shared data on the cloud via security-mediator. In Proceedings of International Conference on Distributed Computing Systems. pp. 124–133.
26. Karadsheh L. (2012). Applying security policies and service level agreement to IaaS service model to enhance security and transition.Computers & Security. 31(3) pp. 315-326.
27. Ramgovind, S., Eloff, M. M., and Smith, E. (2010). The management of security in cloud computing. In 2010 Information Security for South Africa (pp. 1-7).