IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 6, June 2018

Auditing Techniques for the Maintenance of Data Integrity in Cloud: The Review

Misbah U.Mulla[1], Prabhu R.Bevinamarad[2]

PG Scholar, Department of Computer Science and Engineering, B.L.D.E.A's Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka, India[1]

Assistant Professor, Department of Computer Science and Engineering, B.L.D.E.A's Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka,India[2]

Abstract: The cloud computing allows the data owners to store their data remotely so that data users can access the data more easily and efficiently, the data owners are relieved of the task of holding the huge amount of data on their local storage but due to which the control of the data is transferred from the data owner to the cloud server where the security of the data is at risk. The cloud servers and the services offered by them cannot be trusted completely and there are chances that the cloud server may not store the data honestly so to check the data integrity and to maintain its privacy is an important task as well as a challenge .This paper focuses on different techniques that are applied to check the accuracy of the outsourced information and keeps up the uprightness of the information on cloud. The aim of this survey is to understand the research work executed in this specific field.

Keywords: Cloud computing, data integrity.

I. INTRODUCTION

Cloud computing is one of the important and widely growing field due its numerous advantages. Here the resources are shared among the users and it supports centralisation of the data due to which the cloud users can access the data quickly using a network without having to be restricted to a single system for data access, the user is relieved of the burden of maintaining the data and by using the cloud storage the overall hardware and software cost is reduced to great extent as users pay for only those services which they use. The data privacy and security is the main concern of the data owners as they want their data to be stored correctly and honestly on the cloud server and they need some control over their outsourced data. The cloud storage has three main participating entities the cloud server, third party auditor and data owner [1] as shown in fig 1 ,the data owners store their data remotely on the servers with the goal that the clients can get to their information from those servers, the cloud server provide a huge amount of space for the storage as well as resources for the computation, third party auditor is an expertise and performs the tasks of data integrity checking whenever the owners of the data request them to verify the correctness of their outsourced data, the auditor communicates with the server and requests them to send the proof of the data which they are storing on the server this will ensures the maintenance of the data integrity on the cloud server.

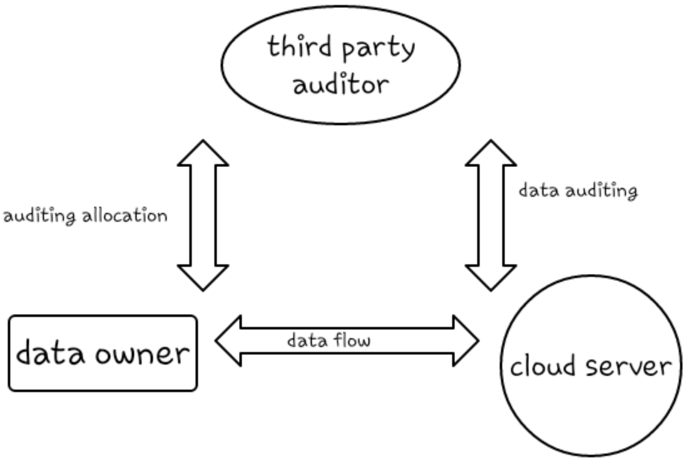

Fig. 1 The structural design of cloud data storage service

DOI 10.17148/IJARCCE.2018.7632

The different types of attacks by the server are replace attack, replay attack and forge attack.

1. Replace attack: The server selects different valid block of data and replaces it with the challenged pair of data tag and its block, this type of attack is executed by the server when it has already removed the actual block of data.

2. Replay attack: In this the actual data accumulated on the cloud is not retrieved and the proof is generated randomly either by using other information of different file or from the previously generated proof.

3. Forge attack: In this attack the server tampers the block of the data and its tag and cheats the auditor here the secret keys of the tags belonging to the owner are reused.

II. LITERATURE SURVEY

The literature survey has been done to study in detail and to analyse the various methods that are applied to solve the issues related to the cloud security and which can be used to verify the correctness of the outsourced data on the cloud. In [2] the authors have proposed an data integrity verification protocol based on identity from lattices its main intention is to provide security against the quantum computer attacks and the attacks such as tamper, lost and replace attack from cloud service provider, in this protocol the management process of the certificates is eliminated, this protocol provides enhanced security based on small integer solution assumption hardness, in this scheme no information is leaked related to the outsourced data to the verifier, the results shows that this protocol is secure and flexible.

In[3] the authors have worked on the hybrid identity based technique to provide security in cloud ,this method is combination of Identity Based Encryption(IBE) and Attribute Based Encryption (ABE) techniques the main aim of this method is to provide enhanced revocation and security against various kind of attacks. The process of revocation, encryption uses the attributes like type of subscription, country etc along with the specific identity of the user ,the issues of effective identity revocation are addressed by representing the computation on outsourced data into hybrid identity based encryption at server side, the results of this method have shown that the efficiency of the revocation is improved up to 40% compared to other methods which are existing.

In [4] the authors have presented a novel model in public key cryptography, the concrete ID based proxy-oriented data integrity checking protocol it is designed using the bilinear pairings and the security is provided by using the computational diffie –hellman problem hardness. This protocol constitutes of four main steps , the set up is performed and the procedure begins first based upon the identity of the user the key generation centre provides the users private key, next warrant is created by client and using this the proxy key is generated by the proxy ,than the tags are generated for the file blocks and these pair of tag and block are uploaded by the proxy on the public cloud server finally the client request for the proof to the public cloud server and based upon the proof verifies the integrity of the uploaded data. This identity based PUIC protocol performs public, private and delegated integrity checking of the remotely stored data.

In [5] the authors have proposed an private provable data possession (PDP) scheme which can detect the forgery attack on the data stored on cloud storage by using the computational diffie hellman (CDH) and Discrete Logarithm (DL) assumptions, in this scheme the tag and the proofs are generated at very low computation cost and it is more reliable and good in performance, this improved provable data possession scheme provides security against the forgery attack.

In[6] the authors have introduced an remote data auditing protocol that provides bidirectional auditing and statistical analysis in this the central authority generates the credentials for all the involved entities and the new entity called the common platform is introduced in this protocol which authorizes the auditor ,collects the results of validation and supervises the verifier , this protocol also supports the dynamic operations performed on the files stored on the cloud and this method is efficient and also provides security in random oracle model. Here the load is distributed accordingly and the client is relieved of the computation overhead, this method handles errors efficiently by locating them accurately with low expenses compared to other methods.

In[7] the authors have presented auditing scheme based on fuzzy identity it was developed to address the issues related to complex key management in cloud ,here the identity of the user is used as a group of attributes describing the user and this protocol is built by using biometrics as the fuzzy identity ,this method offers a good system and security model , the details of this protocol are as follows first the fuzzy identity is send to the key generation centre by the cloud user ,the key generation centre provides the secret key based on identity of the user, by using this key the user generates the meta data of the file and uploads the file with its metadata on the cloud server, finally the challenge response protocol is executed by generating a challenge by the auditor and cloud server to find whether the data is valid and intact ,the new scheme detects the errors more efficiently within no time and provides strong security.

In[8] the author have introduced a protocol called distributed provable data possession in cloud based on identity, to design this protocol the specific bilinear paring is applied, this protocol is flexible and quite efficient as in this the task of certificate management is been eliminated and if the user is authentic based upon its authorization ,this ID-DPDP

DOI 10.17148/IJARCCE.2018.7632

protocol performs delegated verification, public verification and the private verification, in this key generation centre generates the secret key for the client, next the file is converted into blocks and the tags for the blocks are generated and both of these are uploaded to combiner and the combiner circulates this pair of block and tag to the different servers, next the auditor sends the challenge to the combiner and it is further forwarded to all the servers, than the responses from the servers are combined and send to the verifier, auditor verifies the combination of responses and checks whether it is invalid or valid. This protocol is both flexible and efficient in the process of data integrity verification.

In[9] the authors have introduced a regenerating code based auditing scheme for cloud storage where the verification task is delegated from the data owner to the auditor ,as the owner of the data cannot be online all the time to perform the verification process so here an entity called proxy which is semi trusted is introduced into the system model and the proxy manages the reparation of the authenticators and coded blocks ,to make the process of regenerating code efficient the BLS signature is used to design the authenticator ,the authenticator is provided by the owner of the data along with the procedure of encoding, the technique is highly efficient and provides good security.

In[10] the authors have proposed a scheme that supports the integrity verification of the outsourced data on the cloud, in this method cryptographic hash function and double block transportation is applied to provide the security to the data against attacks and to prevent the outflow of information in cloud, to secure the data against the third party auditor the double block transportation is used so that the verifier should not learn or reveal the contents of the stored files ,the cryptographic hash function and the XOR are used to check the data integrity during the verification process, it supports verifying batch files, dynamic data operations and auditing with the technique of key chain. By using this method the burden of expensive auditing by the cloud user is eliminated the data is kept highly secured from the verifier.

In [11] the authors have presented a cloud storage with security features here the elgamal partial homomorphic encryption is used to provide privacy for the data against the auditor during the verification process, verifier has computation resources and performs auditing on behalf of the data owner ,in this the verifier can further perform multiple verifications.

In [12] the authors have introduced a probabilistic approach for the verification of correctness of the data and it is done by making use of metadata in tiny sizes whose size does not depend on the original file's size ,the metadata is constructed by making use some bytes from each block ,the file when stored on the cloud server it is partitioned into fixed sized blocks and if data is tampered it may effect this size of the block to detect this modification the metadata is added to each block which helps in checking the correctness of the stored data, this technique also support the dynamic data operations ,in this method the computation time is reduced to the greater extent as when compared to other methods .

In [13] the authors have presented an secure and efficient dynamic verification scheme. It preserves the privacy of the data in case of auditor by collaborating the bilinearity property related to the bilinear pairing with the cryptography method it eliminates the use of masking ,by using this protocol the batch auditing can be done for more than one owners and here no additional management and organising is needed ,here the verification is done at server side due to which the computation and communication cost is reduced to greater extent this results in efficient auditing and is applicable to storages in cloud on large scale.

In [14] the authors have introduced a verifying service to check the honesty of the outsourced information on the cloud this service is based on various methods such as index hash table, random sampling and fragment structure it detects the anomalies in timely manner this method also uses the probabilistic query to make the auditing service more better and efficient, the auditing service includes tag generation, periodic sampling auditing and auditing of dynamic operations ,the experimental results proves that this technique checks the data integrity on the cloud with good accuracy and carry out auditing with less computation cost and storage space.

In [15] the authors have presented a scheme for checking the information trustworthiness on cloud , in this the auditor holds one cryptographic key and a pre-computed value with it and makes use of this pair during verification process which is independent of file size it also supports files with dynamic attributes, this basic method is further extended to detect the modifications in batch files and hence helps in protection of the information and furthermore the information proprietor can be given authentic proofs of their data that it is maintained and stored honestly on cloud.

In [16] the authors have presented a technique for providing security to the data in cloud computing for that the random masking and homomorphic authenticator are used to guarantee that the verifier should not have any knowledge about the information which is outsourced on the cloud during the verification process and even the data owner is relieved of the burden of doing the task of auditing and this auditing is further extended to multiple user setting where the auditor performs the auditing in the batch format in a parallel way ,the experimental results shows that this method provides sufficient security.

III. CONCLUSION

In this paper we conclude that the integrity checking process of the outsourced data on the cloud is one of the important and growing field and it is seeking more and more attention from researchers these days and in future more contribution can be done in this field, overall the researcher have proposed strong security models and algorithms to improve the performance of the data integrity checking process but the existing techniques have some benefits and on the other hand few drawbacks , some methods can verify the integrity of static data but cannot handle the dynamic operations and some implementations provide efficient security to the outsourced data but unable to prevent the data leakage against the verifier during the verification process. Hence, few methods are flexible but time consuming and expensive, moreover the results from the existing research are satisfactory but as it is the era of big data and eventually the applications and the data accumulation will be increasing tremendously so to handle the future consequences it is necessary to design and develop robust and efficient auditing schemes and protocols to face the upcoming challenges.

REFERENCES

[1] Mrs. Rupali SharmaSawan V. Baghel and Deepti P. Theng,“A Survey for Secure Communication of Cloud Third Party Authenticator”,in ieee sponsored 2’nd international conference on electronics and communication systems,pp.51-54, 2015.

[2] Zhangyun Liu, Yongjian Liao, Xiaowei Yang, Yichuan He and Kun Zhao, “Identity-Based Remote Data Integrity Checking of Cloud Storage From Lattices”,in IEEE 3rd International Conference on Big Data Computing and Communications,pp.128-135,2017.

[3] Mrs. Rupali Sharma and Dr. Bharti Joshi,“ H-IBE: Hybrid-Identity based Encryption Approach for Cloud Security with Outsourced Revocation”,in IEEE International conference on Signal Processing, Communication, Power and Embedded System (SCOPES),pp.1192-1196, 2016.

[4] Huaqun Wang, Debiao He and Shaohua Tang ,“Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud”,in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, june 2016. pp.1165-1176, 2016.

[5] Tung-Tso Tsai, Yuh-Min Tseng, Ying-Hao Hung and Sen-Shan Huang, “Cryptanalysis and Improvement of a Provable Data Possession Scheme in Public Cloud Storage”,in IEEE Third International Conference on Computing Measurement Control and Sensor Network,pp.56-59,2016.

[6] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, and Tie Qiu, “An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing”,in special section on emerging trends, issues and challenges in energy-efficient cloud computing,pp.7899-7911,2016.

[7] Yannan Li, Yong Yu_, Geyong Min, Willy Susilo, Jianbing Ni and Kim-Kwang Raymond Choo “ Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems”, in Journal of Latex Class Files, vol. 14, pp.1-12, 2015.

[8] H. Wang, “Identity-based distributed provable data possession in multicloud storage”, in IEEE Trans. Service Computing, vol. 8, pp. 328–340, 2015.

[9] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, “Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage”,in IEEE Transactions on Information Forensics and Security, vol 10,pp.1513-1528, 2015.

[10] Zaid Alaa Hussien, Hai Jin, Zaid Ameen Abduljabbar, Ali A. Yassin,Mohammed Abdulridha Hussain, Salah H. Abbdal and Deqing Zou, “ Public Auditing for Secure Data Storage in Cloud through a Third Party Auditor Using Modern Ciphertext”,in 11th International Conference on Information Assurance and Security,pp.73-78, 2015.

[11] D. N. Rewadkar and Suchita Y. Ghatage, “Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit”,in IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies,pp.695-699, 2014.

[12] Thanh Cuong Nguyen, Wenfeng Shen, Zhou Lei, Weimin Xu, Wencong Yuan and Chenwei Song, “A Probabilistic Integrity Checking Approach for Dynamic Data in Untrusted Storage”,in IEEE 2013.

[13] Kan Yang and Xiaohua Jia, “An efficient and secure dynamic auditing protocol for data storage in cloud computing,” IEEE Trans. on Parallel and Distributed. Systems, vol. 24, pp. 1717–1726, Sep. 2013.

[14]Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.J. Hu, “Dynamic audit services for outsourced storages in clouds”,in IEEE Trans.on Services Computing, vol. 6, pp. 227–238, 2013.

[15] Xiangtao Yan and Yifa Li, “A Wew Remote Data Integrity Checking Scheme for Cloud storage with Privacy Preserving”,in IEEE ,pp.704-708, 2012.

[16] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Proc. IEEE INFOCOM, pp. 1–9, 2010.

DOI 10.17148/IJARCCE.2018.7632