DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4377

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY: CLOUD COMPUTING SECURITY ISSUES AND TECHNIQUES

Mrs.R.Ahila, Dr.S.Sivakumari
Assistant Professor, Dept of Information Technology,
Professor&Head, Dept of Computer Science and Engineering,
Avinashilingam Institute for Home Science and Higher Education for Women,India

***Abstract*:** Cloud computing is an emerging technology with promising future is becoming more and more popular nowadays. It allows users with unlimited resource. Nowadays, outsourcing computation has attracted much attention and been researched widely. Cloud storage is one of the most significant services of cloud computing. Though cloud computing has various advantages to users, it brings new security challenging problems. One of the important security problems is how to effectively check the integrity of the cloud data stored in the cloud. In the recent years, auditing protocols for cloud storages has been proposed to deal the integrity problem of cloud data. This paper deals with different auditing protocols. Literature survey shows that the protocols are focused on different aspects such as dynamic data operations, privacy protection of the data, the high efficiency, the privacy protection of the identities and the data sharing. These protocols achieve the assurance of cloud data integrity and availability and enforce the quality of cloud storage service and also enable on demand data correctness verification on behalf of the cloud users.

***Keywords*:** Cloud computing, auditing protocols, cloud service, cloud data security.

1. INTRODUCTION

Cloud storage is one of the important services in cloud computing [1]. In the cloud storage service [2], data owner stored their data on cloud. But this process introduces new challenges for data owners to provide security for that data. In some cases the cloud providers may not be honest. In order to, save the cloud storage space the cloud providers could reject the data that have not been accessed or rarely accessed and state that the data are still correctly stored in the cloud. Therefore, owners need to be induced that the data are correctly stored in the cloud. Conventional owner can check the integrity of data based on two-party auditing [3] where the data owner and cloud service provider are involved. But this is not a proper way to do auditing because both of data owner and cloud service provider are not able to give unbiased result. So an alternative auditing method called as third party auditing [4] was used. A third party auditor which has enterprises and capabilities can do more efficient and convince both owners and cloud service providers.

Third Party Audit performs tests of the subject matter to form a report or an opinion on the matter of assertions. This report discloses whether the cloud service provider security safeguards meet the security standards and also to access the effectiveness of its control over the retention, use collection and disclosure of personally identifiable information. The work flow of the third party auditing system is depicted in figure 1.

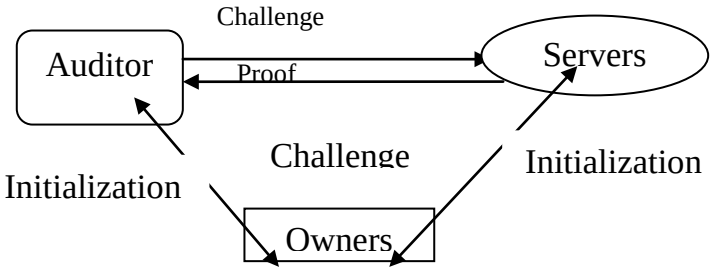

Figure 1. Third Party Auditing system

In this paper, different auditing techniques to effectively check the integrity of the data are discussed based on their advantages, disadvantages and metrics.

2. RELATED WORK

A privacy preserving public auditing system was proposed [5] for data storage security in cloud computing. In their work the privacy preserving auditing system utilized the homomorphic authenticator and random masking which guaranteed that Third Party Authenticator (TPA) cannot learn any knowledge about the data content stored on the cloud server during the auditing process. It was achieved by combining the public key based public key authenticator with the random masking to obtain a privacy preserving data auditing system. TPA can handle multiple audit sessions from different users for their outsourced data. The privacy preserving auditing system can ensured the privacy data stored in the cloud. This process not only eliminated the burden of the cloud from possibly expensive and tedious auditing task.

In flexible distributed storage integrity auditing mechanism [6] provided a secure and dependable services in cloud computing. In their work they utilized distributed erasure-coded data and homomorphic token to ensure the strong

© 2015-19, IJARCS All Rights Reserved

cloud storage correctness guarantee. This mechanism was flexible distributed along with explicit dynamic data support including the block append, delete and update. The erasure-coded is fully relied on the file distribution preparation which guaranteed the data dependability and provided redundancy parity vectors. The integration of data error localization and storage correctness insurance was achieved by using the homomorphic token with distributed verification of erasure-coded data.

An auditing framework was designed called as privacy and integrity preserving dynamic auditing protocol [7] for cloud storage system and proposed a privacy preserving and dynamic auditing protocol. The privacy preserving and dynamic auditing protocol didn't using any mask technique and it didn't require any trusted organizer to support batch auditing for multiple clouds. It solved the data auditing problem by saving an encrypted data in cloud by using encryption techniques. Thereby using encryption techniques, the auditor cannot decrypt the data in the cloud storage and it can verify the correctness of the data. It prevented data privacy against the third party auditor through cryptographic techniques. TPA plays an important role in privacy preserving process this ensured that TPA maintained the correctness of the cloud data with a great demand that the user's data contents of the collected information during auditing process cannot be derived by TPA.

In efficient Remote Data Auditing techniques [5] they implemented an algebraic signature properties to secure big data storage in cloud computing. These techniques incurred minimum communication and computation costs. In addition to that, a new data structure called as Divide and Conquer Table (DCT) was presented to support effective operations are delete, modify, insert and append. This data structure can be applied for large scale data storage and it incurred minimum computational cost. It verified the integrity of the cloud data by employing algebraic properties of the outsourced data blocks. It remotely checked the integrity of the files and minimized the computational overhead on the server side and server side of the cloud. In DCT data structure, the data owners modify, append, insert or delete the files at the block level.

A cloud computing auditing scheme was implemented [9] for light weight and privacy preserving secure cloud computing process for group users. In this scheme, a Third Party Medium was introduced to perform time consuming operations on behalf of users. It was generated a number of authenticators for users along with that it verified data integrity on behalf of users. The data privacy against the TPM was protected by blinding the data through the simple operations in the phase of data auditing and data uploading. By using this scheme, the users does not need to time consuming decryption operation which can be handled by cloud computing auditing scheme while using cloud data.

An optimized public auditing and data dynamics [10] for data storage security in cloud computing. In their work, the data integrity verification problem by the third party auditor for the client's data residing on cloud storage was focused. The optimized method make the third party auditing resistant to replay, replace and forge attacks launched by malicious insiders at cloud storage server. Furthermore, a protocol was suggested for efficient fine grained dynamic data and block level update operation on the cloud storage data utilizing a modified Chameleon Authentication Tree (mCAT) which perform hash computation during dynamic update data operations.

The public auditing system of data storage security in cloud computing they implemented an efficient construction for the seamless integration of public auditability and data dynamics protocol [11] that supported for fully dynamic data operations including support block insertion. This scheme was extended to support scalable and efficient public auditing in cloud computing and it achieved batch auditing where multiple delegated auditing tasks from different multiple users was performed consecutively by Third Party Auditor. The efficient data dynamics was achieved by improved the conventional proof of storage model by manipulating Merkle Hash Tree construction for block tag authentication and for efficient handling of multiple auditing tasks the technique of bilinear aggregate signature was explored to provide multi user setting where TPA performed multiple auditing tasks simultaneously.

In efficient and privacy preserving data auditing protocol they suggested [12] for data storage in cloud computing. The data auditing protocol was extended that support the data dynamic operations. It was efficient and provably secure in the random oracle model. The auditing protocol was further extended to support batch auditing for both multiple clouds and multiple users without using any trusted organizers. This protocol ensured the data privacy by using bilinear property of the bilinear pairing and cryptography method instead of using mask techniques. It reduced the computing loads of the auditor by moving it into the server. The multi cloud batch auditing system and multi owner batch auditing in privacy preserving data auditing protocol does not required additional trusted organizers and improved the auditing performance respectively.

An ID based auditing protocol was proposed [13] for outsourced data in the cloud. The ID based is a combination of ID based cryptography technique with homomorphic auditor technique, it is provably secure in the random oracle model and has high security reduction in the cloud computing. Initially based on homomorphic ID based signature process a ID based auditing protocol was designed of data integrity for cloud storage system. This protocol simplified the key management and alleviates the burden of the data users and auditors. The more important thing in this protocol was the computation cost of the auditor was independent of the number of the challenged data blocks. It needed a constant computation overhead for data integrity checking.

A dynamic outsourced data auditing scheme was suggested [14] to protect against dishonest entity and collision and to support verifiable dynamic updates to outsourced data. This scheme was based on batch leaves authenticated Merkle Hash Tree (BLA-MHT) for batch verify multiple leaf nodes and their own indexes all together that was more appropriate for the dynamic outsourced auditing system. Based on the proposed BLA-MHT and its algorithm, Dynamic Outsourced Auditing (DOA) was proposed that protected against any dishonest entity and collision. In addition to that,

© 2015-19, IJARCS All Rights Reserved

it concurrently avoided the resource intensive design of downloading entire outsourced data from Cloud service Provider (CSP) to Third Party Auditor (TPA). Furthermore by means of above algorithm, the proposed scheme was extended to support dynamic data operations of block level under the outsourced auditing environment.

A better data integrity data verification approach [15] for cloud computing. This approach was used for multiple Third Party Auditors, Combinatorial Batch Codes (CBC), Paillier Homomorphic Cryptography (PHC) and homomorphic tags for data integrity verification. The building blocks of proposed technique were variants of the PHC system with homomorphic tags and CBC. The homomorphic encryption on the data blocks was obtained by using PHC system. Homomorphic tags with the Paillier Cryptography system assigned a special verifiable value to each data block that helped to unleash data operations on this block. The integral data was assigned and stored into different distributed cloud server by using CBC.

An efficient public audition solution was implemented [16] which can preserve the identity privacy and the identity traceability for group members simultaneously. A new framework was designed for data sharing in the cloud and formalized the description of the public auditing scheme for shared cloud data. It supported the privacy identity and traceability of the cloud data. Then a scheme was constructed where group members were introduced they help to generate group authenticators to protect identity privacy. There are two lists were employed to record the members perform the modification on each block to achieve the identity traceability. Through blind signature technique data privacy during authenticator generation was achieved.

A novel integrity auditing scheme [17] for cloud data sharing services. This can be characterized by multi user modification, efficient user revocation, communication and computational auditing and high rate detection probability performance. The novel integrity scheme can resist user impersonation attack, which was not focused in conventional techniques which support multi user modification. In addition to that batch auditing of multiple tasks was effectively supported in this scheme. This scheme was featured by salient properties of public integrity auditing and constant computational cost on the user side. It was achieved through an innovative design on polynomial based authentication tags that allowed aggregation of tags of different data blocks. In order to provide system scalability, the cloud was empowered with the ability to aggregate authentication tags from multiple writers into one which leads to constant size of integrity proof information. Moreover secure delegation of user revocation was allowed and aggregation of integrity auditing operations for multiple tasks (files) through batch integrity auditing technique with enhanced reliability.

An Identity based Cloud data integrity checking protocol [18] was suggested to eliminate the complex certificate management in traditional cloud data integrity checking protocols. The proposed protocol in this paper was concrete construction from RSA signature that support public auditing and variable sized file blocks. Moreover, a formal security model was proposed and proved that the security of this model under construction of RSA has highly secured model to protect the data in cloud environment.

A cloud storage auditing protocol was proposed [19] with verifiable outsourcing of cloud data storage. In this protocol, the key updates were safely outsourced to some authority party and it reduced burden on the client side of key update. In this proposed protocol, the Third Party Auditor (TPA) only needed to keep an encrypted version of the client's secret key during the burdensome operations on behalf of the client. When the client wants to upload a data in the cloud, they only need to download the encrypted version of the secret key from the TPA. This protocol also equipped the client with the capability to verify the validity of the encrypted secret key provided by TPA.

The secure delegation of auditing [20] in this paper it allows the data stored in the cloud environment to delegate the auditing task with potentially secure way by the un trusted third party verification. In this proposed technique the data owner verify the TPA performs the specified audit task and also verified the TPA perform audit task while right time by the owner of the data. The data is protected with confidentially besides TPA. Additionally the proposed method allows the TPA perform the re outsource the task of the auditing.

The H-one auditing mechanism [21] suggested for the information flow tracking techniques to implement complete and efficient privacy logs for the cloud environment. The proposed technique enables the auditing the cloud infrastructure and improving the customer trust in the services of the cloud and provides the secure auditing which is recorded by any unauthorized administrator privileges. Initially the audit log produced then the recordings of the audit should be efficient and finally the audit logs should be available.

The inter cloud audit schema [22] improve the request and response of the audit which is exchanged between the federated clouds. This technique used for cross cloud communication and improve the security awareness in the invocation chain and overcome the security issue. This technique implement in the nimbus cloud and by using the filtering techniques and composition techniques to find the security anomalies. The detection techniques used for the return audit assets and develop within the cloud.

The aggregatable signature based broadcast encryption scheme [23] suggested for improving the zero knowledge privacy preserving with efficient cloud auditing scheme. In this technique it remove the burden of the cloud user from the deadly and complicating task also eliminates the outsourced data leakage. The storage cost and the communication cost iteratively decreased. Additionally improve the privacy preserving in the cloud environment.

The security flows of the protocol [24] in their work it against the various attack by the malicious cloud server. The outsourced data can be modified by the malicious cloud server for the user purposes. Then the outside attacker also modify the data sometimes ask high cost for the cloud storage. This technique does not provide the secure data storage for the users.

© 2015-19, IJARCS All Rights Reserved

The secure cloud storage system [25] they suggested for the privacy preserving public auditing. In this method it can extent the TPA to perform the audits for the multiple users simultaneously and efficiently. Initially the proposed scheme support to the scalable and efficient privacy preserving public storage auditing in the cloud environment which achieves the batch auditing and the multiple delegated auditing tasks from the various users this leads to the TPA with the privacy preserving manner. The secure cloud storage system improves the cloud security.

The efficient public integrity auditing scheme [26] is to overcome the problem of the constructing public integrity auditing for shared dynamic data with the revocation of the group user. The proposed technique initially perform the secure and efficient shared data integrate auditing for the multi user operation then the efficient data auditing scheme proposed with the new features like tractability and count ability. Finally in this schemes it provide the security and efficient analysis for the cloud environment.

The dynamic proof of the irretrievability scheme [27] suggested for the public auditability and the encoded the data by the dynamic operations. The networking coding and the removal code are adopted for improving the data availability and the communication efficiency by the data recovery process. In their work they utilized to generate the meta tags of the encoded blocks to support the public auditability and support random sampling which is improve the security and the performances of the proposed technique.

The SecCloud and SecCloud^{+} [28] suggested to handle the problem of the data integrity and deduplication in cloud. The SecCloud used for the auditing entity with maintenance of the MapReduce cloud which generates the data tags before the uploading as well as the integrity of the auditing data stored in the cloud. The SecCloud^{+} used for encrypts the data before the uploading and also improves the integrity auditing and secure deduplication on the encrypted data.

The highly efficient data integrity auditing scheme [29] They suggested for the storage of the cloud in the mobile health applications. The proposed technique used in the tag generation in each block with minimal because of the hash function. Then cloud server receives and store the data blocks without tag in the data owner and the efficient authentication occur. Additionally the message locked encryption scheme used for encrypts and the auditing information are checked in the data blocks which provides the efficient verification. The proposed scheme detects the data blocks with errors and checked and ensures to utilized and recover the fault data.

Cloud Auditing in the Identity based data outsourcing [30] in their work they for the secure IBDO techniques. This allows the file owner to delegate the outsourcing capabilities to the outsourcing. The authorized proxy only allows the next process and outsources the file behalf of the file owner. The both file origin and the file integrity verified by the public auditor.

4. CONCLUSION &FUTURE SCOPE

In this paper, a detailed survey and further analysis on auditing methods for efficient cloud storage service were encountered. It is obvious that all the authors have developed different approached to obtain better results than the previous methods with suitable modifications. Even then, further improvement on auditing methods is required to secure the cloud storage data.

The further research focus will be based on developing a more efficient auditing protocol to reduce the communication cost, reduce the auditing time, to support for multi user setting and to provide multi auditing tasks.

5. REFERENCES

[1]. Faheem Zafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed, Adeel Anjum, Majid Iqbal Khan, Nadeem Javed, Masoom Alam, and Fuzel Jamil. "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends", Computers & Security 65 (2017), 29-49.

[2]. Glauber D. Gonçalves, Idilio Drago, Alex B. Vieira, Ana Paula Couto da Silva, Jussara M. Almeida, and Marco Mellia. "Workload models and performance evaluation of cloud storage services", Computer Networks 109 (2016): 183-199.

[3]. Md. Tajuddin and K. China Busi. "An enhanced dynamic auditing protocol in cloud computing." International Journal of Engineering Trends and Technology 4, no. 7 (2013): 3173.

[4]. Swapnali More and Sangita Chaudhari. "Third Party Public Auditing Scheme for Cloud Storage." Procedia Computer Science 79 (2016): 69-76.

[5]. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, 2010. “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, Infocom, 2010 proceedings ieee, pp. 1-9.

[6]. Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing Lou, 2012. “Toward secure and dependable storage services in cloud computing”, IEEE transactions on Services Computing, Vol. 5, No. 2, pp. 220-232.

[7]. Anuradha Appasaheb Jagadale, and Shilpa Gite**,** 2014. “Privacy Preserving Auditing Protocol Using Cryptography for Cloud Storage Systems”, IJSR, Vol. 3, No.12, pp. 144-148.

[8]. Mehdi Sookhak, 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.

[9]. Wenting Shen, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu and Rong Hao, 2017. “Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium”, Journal of Network and Computer Applications, Vol. 82, pp. 56-64.

[10]. Anirudha Pratap Singh and Syam Kumar Pasupuleti, 2016. “Optimized Public Auditing and Data Dynamics for Data Storage Security in Cloud Computing”, Procedia Computer Science, Vol. 93, pp.751-759.

[11]. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, 2011. “Enabling public auditability and data dynamics for storage security in cloud computing”, IEEE transactions on parallel and distributed systems, Vol. 22, No. 5, pp. 847-859.

[12]. Kan Yang, and Xiaohua Jia, 2013. “An efficient and secure dynamic auditing protocol for data storage in cloud computing”, IEEE transactions on parallel and distributed systems, Vol. 24, No. 9, pp. 1717-1726.

[13]. Jianhong Zhang, Qiaocui Dong, 2016. “Efficient ID-based public auditing for the outsourced data in cloud storage”, Information Sciences, Vol. 343, pp. 1-14.

© 2015-19, IJARCS All Rights Reserved

[14]. Lu Rao, Hua Zhang, and Tengfei Tu, 2017. “Dynamic Outsourced Auditing Services for Cloud Storage Based on Batch-Leaves-Authenticated Merkle Hash Tree”, IEEE Transactions, pp. 1-14.

[15]. Rajat Saxena and Somnath Dey, 2016. “Cloud Audit: A Data Integrity Verification Approach for Cloud Computing”, Procedia Computer Science, Vol. 89, pp. 142-151.

[16]. Guangyang Yang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu, and Rong Hao. "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability." Journal of Systems and Software 113 (2016): 130-139.

[17]. Jiawei Yuan and Shucheng Yu, 2015. “Public integrity auditing for dynamic data sharing with multiuser modification”, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 8, pp. 1717-1726.

[18]. Yong Yu, Liang Xue, Man Ho Au, Willy Susilo, Jianbing Ni, Yafang Zhang, Athanasios V. Vasilakos, and Jian Shen. "Cloud data integrity checking with an identity-based auditing mechanism from RSA." Future Generation Computer Systems 62 (2016): 85-91.

[19]. Jia Yu, Kui Ren and Cong Wang, 2016. “Enabling cloud storage auditing with verifiable outsourcing of key updates”. IEEE Transactions on Information Forensics and Security, Vol. 11, No. 6, pp. 1362-1375.

[20]. Xu, J. (2011). Auditing the Auditor: Secure Delegation of Auditing Operation over Cloud Storage. IACR Cryptology EPrint Archive, 2011, 304.

[21]. Ganjali, A., & Lie, D. (2012, October). Auditing cloud management using information flow tracking. In Proceedings of the seventh ACM workshop on Scalable trusted computing (pp. 79-84). ACM.

[22]. Xie, R., & Gamble, R. (2013, January). An architecture for cross-cloud auditing. In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (p. 4). ACM.

[23]. Shao-hui, W., Su-qin, C., & Zhi-wei, W. (2012). Public auditing for ensuring cloud data storage security with zero knowledge Privacy. pp-1-12.

[24]. XU, C. X., HE, X. H., & Daniel, A. (2012). Cryptanalysis of Auditing protocol proposed by Wang et al. for data storage security in cloud computing.

[25]. Wang, C., Chow, S. S., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE transactions on computers, 62(2), 362-375.

[26]. Jiang, T., Chen, X., & Ma, J. (2016). Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Transactions on Computers, 65(8), 2363-2373.

[27]. Ren, Zhengwei, Lina Wang, Qian Wang, and Mingdi Xu. "Dynamic proofs of retrievability for coded cloud storage systems." IEEE Transactions on Services Computing (2015).

[28]. Li, J., Li, J., Xie, D., & Cai, Z. (2016). Secure auditing and deduplicating data in cloud. IEEE Transactions on Computers, 65(8), 2386-2396.

[29]. Ren, Y., Shen, J., Zheng, Y., Wang, J., & Chao, H. C. (2016). Efficient data integrity auditing for storage security in mobile health cloud. Peer-to-Peer Networking and Applications, 9(5), 854-863.

[30]. Wang, Y., Wu, Q., Qin, B., Shi, W., Deng, R. H., & Hu, J. (2017). Identity-based data outsourcing with comprehensive auditing in clouds. IEEE Transactions on Information Forensics and Security, 12(4), 940-952.

© 2015-19, IJARCS All Rights Reserved