IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303270 |

Secure Data Storage and Sharing Techniques in Cloud Computing

M. Brindha, Akash G, Rahul A, Mohamed Ali K, Manoj P

Assistant Professor, Department of Computer Science and Engineering, Mahendra Institute of Technology, Namakkal, Tamilnadu, India

Department of Computer Science and Engineering, Mahendra Institute of Technology, Namakkal, Tamilnadu, India

ABSTRACT: The cloud computing plays the prominent role in many organizations and researchers were focus on securing the cloud computing. The privacy preserving is the major challenge that grows exponentially with increases in user. In this paper, the depth survey is conducted on the recent methodologies of the cloud storage security related with the cloud computing. The overview of the cloud computing and security issues is analyzed in this paper. The key security requirements such as data integrity, availability and confidentiality. Security issues in the recent methodologies of cloud security is analyzed. The challenges in the cloud security is analyzed and possible future scope of the method is discussed. The paper involves in analyzing the state-of-art method to investigate the advantages and limitations.

KEYWORDS: Cloud Computing, Privacy Preserving, Cloud Storage Security, Data Integrity, and Confidentiality.

I. INTRODUCTION

Cloud storage provides the user to access the data flexibly and allow to store the more data in the system. However, this tends to develop security challenges in the cloud storage and users are concerns about the intact of the data integrity. In this scenario, cloud security has been developed and user has been provided with two secret keys. The secret key is developed based on the random numbers with some procedures. The algebraic property of the encryption method makes it suitable for the cloud security [1]. Cloud auditing services is developed to provide the proof of data integrity for the data stored in the cloud. Cloud auditing also suffers from weak security method. Cloud security performance has been measured in terms of three important metrics such as Integrity (I), Availability (A) and Confidentiality (C). Some techniques such as Secure Socket Layer (SSI) with 128 bit has been used for data integrity check and also supports for searchable encryption and divide the data into three section. Cloud storage technologies offers the user to provide the large space to store the data and process it without requiring much local resources in the system [2].

Enable the public auditing method for the cloud storage is important that is made easy with Third Party auditing (TPA) to analyze the integrity of the cloud data. The TPA reduces the burden for the user to check the integrity for cloud data. The users require the efficient and convincible auditing method for check the integrity. Batch auditing is used in the TPA to process multiple user data and supports the multiple cloud in the integrity check without the need of trusted organizer. The cloud storage provides the elastic scalability and offer the resources per pay option [3]. The security risk of data highly affects the relationship between the Cloud Service Provider (CSP) and customer. The cloud security method considers the three kinds of participators such as user, hacker and cloud manager.

Cloud computing is the computing model that provides the on-demand services for accessing the sharing the computing resources. In the verification phase, an active adversary can arbitrarily change the cloud data without detected by the auditor. The cloud may involve in deleting, replacing or re-constructing the deleted data blocks from the corresponding tags in the integrity checking process [4]. Therefore, the cloud auditing is the important process in checking cloud reliability based on RSA method.

The cloud storage security issues are of three categories, such as confidentiality, Integrity and authentication. The user doesn't possess the data storage, traditional security protecting doesn't able to adopt. Hence, from the analysis of this research provides the analysis of the latest techniques in the cloud storage services. From the analysis, it shows there is still needs to develop the technique with the greater flexibility [5].
The organization of this research papers is as follows, Section.2, presented the overview of cloud storage security. Section.3 is organize a review of issues faced in cloud storage services such as confidentiality, Integrity and

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303270 |

authentication. Section.3, presents comparative analysis of various existing techniques. Section.4 presents challenges faced in the secure cloud storage. And the conclusion is provided in the section.5.

II. SECURE CLOUD DATA STORAGE

The cloud security methods will vary with the different cloud deployment model. Four types of Cloud computing models are present such as private cloud, public cloud, community cloud and hybrid cloud. Organization maintains the private cloud to exclusively store their data in their environment. Public cloud offers the storage space and resources for the users. Hybrid cloud is the combination of any two above mentioned cloud types. The price of cloud deployment is changes from private cloud to public cloud based on the security measures. The cloud storage security is the challenging process regardless of deployment model. The basic architecture of cloud consists of resources, Service Level Agreement (SLA), and service interfaces. The three?layer model of the cloud with the logical functional boundaries is shown in Figure1.

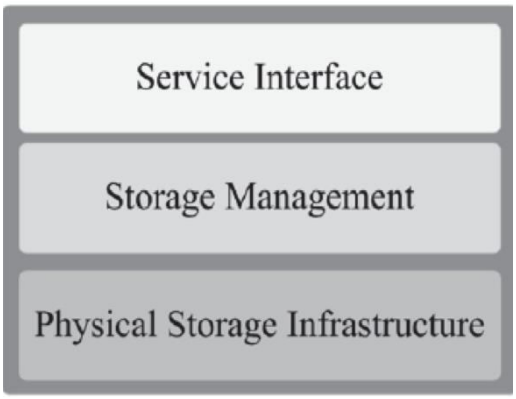

Fig. 1. Cloud Storage Architecture

A.Review on Authentication in Secure Cloud Data Storage

Cong Wang et al. [6] developed key aggregation method for securing cloud storage and this method generate the key in constant size. The developed method provides the flexible delegation of decryption rights. The key size is independent of the number of key is need to be encrypted. The stability of the method is high regardless of number of times user upload to the cloud server.

Debiao He et al. [7] developed the privacy aware authentication method for mobile cloud computing. The developed method is able to adopt to exponential increases of the number of users. The developed method has the advantages of mobile storage, communication and computation. The developed method supports the various cloud computing services with mobility. The security and privacy protection is low in this method due to the insecure transmission of the data. The flexibility of the developed method is high and satisfy the on-demand cloud applications with local infrastructure limitations. The developed method improves the privacy with more data sharing.

Sushmita Ruj et al. [8] proposed decentralized access control with anonymous authentication in the cloud. The cloud verifies the authenticity while storing the data without the user identity. Access control has been presented in the process that provides authentication for valid users. The method also supports the editing of the data and has the ability to prevent the replay attacks. The user revocation and prevention of the replay attack is based on the access control and anonymous authentication process. The user can able to check the integrity based on this method. The performance analysis of the developed method shows that the security of the method is high and also has high efficiency.

B. Review on confidentiality in Secure Cloud Data Storage

Sherman et al. [9] developed a method to support dynamic users and data provenance for building secure cloud storage system. The dynamic cipher texts are used for the broadcast encryption and provides the security for the text decryption and attacks. The cryptographic defense mechanisms is compared and analysis the research direction and methods for protecting the data in cloud. The developed secure authorized de-duplication method in the hybrid cloud. Data de-

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303270 |

duplication is one of the important process in cloud to eliminate the repeating data and this is used to save bandwidth and storage space. The developed method provides the minimum overhead compared to normal operations.

Qin Liu et al. [10] developed privacy preserving keyword search method for the cloud storage services. The developed method allows the CPS to handle the decipherment and returns the files that only contains the given keywords. The developed method reduces the computation and communication overheads. The developed method is efficient in provide the integrity and privacy to the data stored in the cloud. The developed method supports the TPA method to reduce the computational time.

C. Review on Integrity in Secure Cloud Data Storage

Yong Yu et al. [11] developed identity based privacy preserving method for remote data integrity for cloud storage. The developed method shows that the data is secure and can be used in the real-time system. The developed method effectively checks the data integrity without downloading the actual data. The complexity of the method is high and need to be reduced. The developed data integrity method for public verification of the cloud storage. The dynamic data process such as editing the data and updating is supported in the method. The overhead of the bath verification method is independent of the number of verification tasks. The homomorphic token is used in the flexible distributed storage and distributed erasure-coded data. This supports the secure and dynamic operations on outsourced data including block modification attack and server colluding attacks. The privacy method has the third party verifiers and client data are not accessible. The data is secured in the cloud and integrity has been verified.

The Remote Data Integrity Checking (RDIC) [12] protocols audit the cloud data for checking the integrity. The RDIC protocols verify for the TPA method that has the expertise and capabilities for the verification process. The ID-based RDIC architecture is shown in Figure 2.

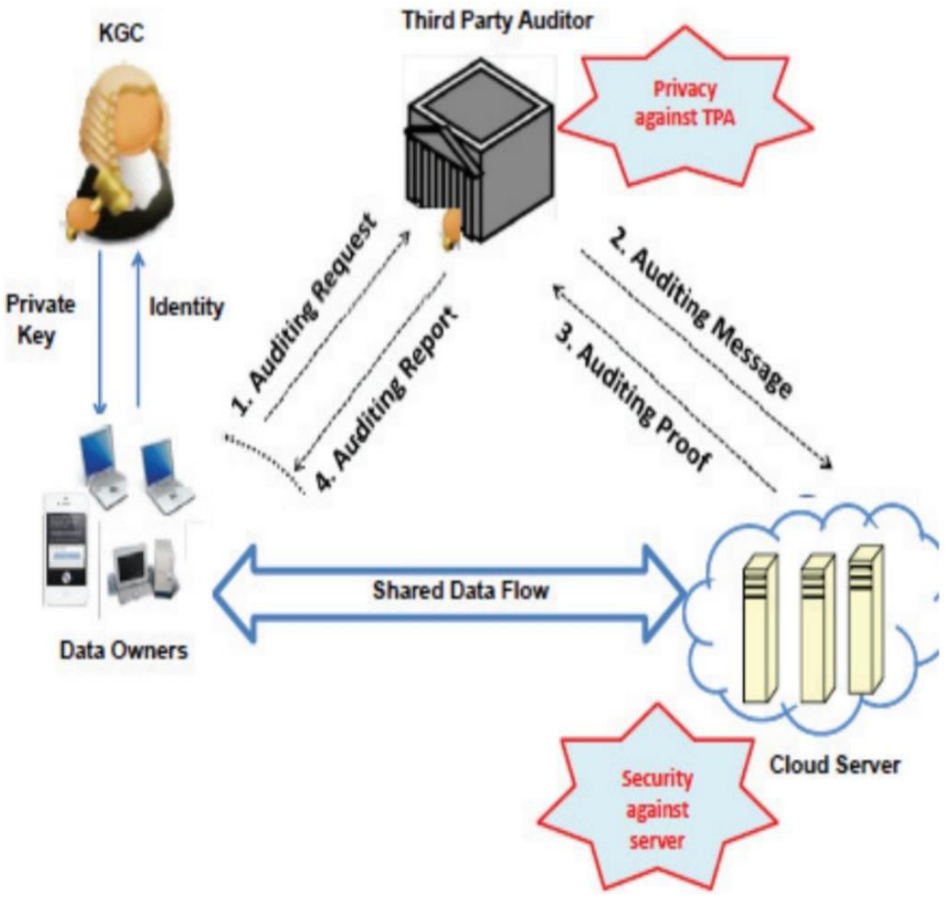

Fig. 2. The system model for Identity based Remote Data Integrity Checking

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303270 |

III. COMPARATIVE ANALYSIS OF SECURE CLOUD STORAGE

After the general explanation of cloud storage with its security problems by focusing on the comparative analysis on the data integrity, data confidentiality and authentication issues. The latest research involves in the secure cloud storage, which are analyzed with advantages and limitations in the table. (1).

TABLE I. ANALYSIS ON SECURE CLOUD STORAGE

Author	Methodology	Advantage	Limitation	Performance Evaluation
Henry C.H et al. [13]	Regeneration coding based method.	The method is feasible in analysis of the random subsets for the data integrity check.	Efficiency in terms of computation overhead and running time degrades over the increase of security key and block size	Probability and Time taken
Jingwei et al. [14]	Deduplication and auditing process.	Data tags are generated to easily check the data integrity	Encryption of data from user end and de-duplication at cloud server increases the execution time.	Number of blocks, time block
Chang Liu et al. [15]	Fine-grained updates are used for the public auditing.	Communication overheads is less for small data.	Data security in terms of confidentiality and availability should be improvised from server side with better quality of service	Storage taken, proof size, less data retrieved percentage
Jianbing Ni et al. [16]	Dynamic auditing protocol.	Communication overheads is less for small data.	Data Auditing in modification of encrypted data validation has complexity to recover original data.	The communication overhead is similar to the original method.
Rizwana Shaikh et al. [17]	Data classification method is developed for improving cloud security.	Security of the data is improved based on requirement	Encryption, integrity and access control mechanism has to improve security strength substantially	Quality and strength of method is increased.
Sandeep K. Sood et al. [18]	Combined method is used to improve the security.	Flexibility of the method is high and able to handle the complex structures.	Retrieving files from cloud over searching of encrypted data is more complex due to its data leakage	Security and Value of data (in Tera bytes)

IV. CHALLENGES IN SECURE CLOUD STORAGE

In cloud storage adoption, there are lot of benefits to deal with some issues to security that could affects the data. Some of the challenges is mentioned below that must be met in order to keep our information safe in cloud to avoid intruders.

Data Leakage: The cloud provides resources to the client that can be shared. The stored user data can be hacked or modified. These kinds of issues can be overcome by storing the encrypted data using robust encryption method.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303270 |

Access Credentials: Main challenge is to protect the data from own cloud credentials. The unique credentials can be used to separate of the data from other clients. Access control can be used to prevent the data from accessing and modifying files. Credentials were used to protect the data in the cloud.

Performance of encryption and decryption: Applying strong encryption method should not affect the performance of the cloud. Both encryption and decryption process has to kept in low computational time and resources. The method requires high computational time and resources affects the user experiences.

Data Security during transmission: The data might be hacked during the transmission. The strong encryption method and credentials can be used to secure the data from the hackers. The secure transmission is need to establish to transfer the data. This is additional security measure to protect the data from intruder.

V. CONCLUSION

Recently, the cloud computing has witnessed the rapid development and secure method to protect the data is required. Security measures can be equipped in the cloud to improve the reliability and trustworthy. This paper analysis the existing method in cloud security to evaluate the three main parameters such as integrity, authentication and confidentiality. To improve each aspect various methods is need to incorporate that are different from traditional security system on data transfer or file storage system. The summarized the existing method progress up to data and provides future scope of the method. The cloud storage security system requires the effective method to overcome the issues such as data leakage, insecure transmission and access credentials.

REFERENCES

[1] Chen, L., 2013. Using algebraic signatures to check data possession in cloud storage. Future Generation Computer Systems, 29(7), pp.1709- 1715.
[2] Yu, J., Ren, K., Wang, C. and Varadharajan, V., 2015. Enabling cloud storage auditing with key-exposure resistance. IEEE Transactions on Information forensics and security, 10(6), pp.1167-1179.
[3] Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), pp.1831-1838.
[4] Wang, C., Wang, Q., Ren, K., Cao, N. and Lou, W., 2011. Toward secure and dependable storage services in cloud computing. IEEE transactions on Services Computing, 5(2), pp.220-232.
[5] Wang, C., Wang, Q., Ren, K. and Lou, W., 2010, March. Privacy?preserving public auditing for data storage security in cloud computing. In 2010 proceedings ieee infocom (pp. 1-9). Ieee.
[6] Guo, C., Luo, N., Bhuiyan, M.Z.A., Jie, Y., Chen, Y., Feng, B. and Alam, M., 2018. Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage. Future Generation Computer Systems, 84, pp.190-199.
[7] He, D., Kumar, N., Khan, M.K., Wang, L. and Shen, J., 2016. Efficient privacy-aware authentication scheme for mobile cloud computing services. IEEE Systems Journal, 12(2), pp.1621-1631.
[8] Ruj, S., Stojmenovic, M. and Nayak, A., 2013. Decentralized access control with anonymous authentication of data stored in clouds. IEEE transactions on parallel and distributed systems, 25(2), pp.384-394.
[9] Chow, S.S., Chu, C.K., Huang, X., Zhou, J. and Deng, R.H., 2012. Dynamic secure cloud storage with provenance. In Cryptography and security: From theory to applications (pp. 442-464). Springer, Berlin, Heidelberg.
[10] Liu, Q., Wang, G. and Wu, J., 2012. Secure and privacy preserving keyword searching for cloud storage services. Journal of network and computer applications, 35(3), pp.927-933.
[11] Yu, Y., Au, M.H., Ateniese, G., Huang, X., Susilo, W., Dai, Y. and Min, G., 2016. 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.
[12] Yu, Y., Au, M.H., Mu, Y., Tang, S., Ren, J., Susilo, W. and Dong, L., 2015. Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. International Journal of Information Security, 14(4), pp.307-318.
[13] Chen, H.C. and Lee, P.P., 2013. Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation. IEEE transactions on parallel and distributed systems, 25(2), pp.407- 416.
[14] Li, J., Li, J., Xie, D. and Cai, Z., 2015. Secure auditing and deduplicating data in cloud. IEEE Transactions on Computers, 65(8), pp.2386-2396.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303270 |

[15] Liu, C., Chen, J., Yang, L.T., Zhang, X., Yang, C., Ranjan, R. and Kotagiri, R., 2013. Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates. IEEE Transactions on Parallel and Distributed Systems, 25(9), pp.2234- 2244.
[16] Ni, J., Yu, Y., Mu, Y. and Xia, Q., 2013. On the security of an efficient dynamic auditing protocol in cloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(10), pp.2760- 2761.
[17] Shaikh, R. and Sasikumar, M., 2015. Data Classification for achieving Security in cloud computing. Procedia computer science, 45, pp.493-498.
[18] Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), pp.1831-1838. 337 Authorized licensed use limited to: Auckland University of Technology. Downloaded on December 21,2020 at 14:24:08 UTC from IEEE Xplore. Restric

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details