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

Data Integrity, Data Privacy and Data Confidentiality Issues in Multi-User Cloud

K Priyadharshini, R Aroul Canessane

Abstract*: Cloud computing was one of the most significant computational models that help to handle the vast amount of data in a flexible and secure environment. In the current scenario, the amount of data being shared and the number of users or group in the cloud has been continuously increasing. The rise in the usage of the clouds had instigated the need to provide the security to the data that were transmitted among the user and owner through a cloud server. The data in the cloud most commonly endure in issues related to the integrity, privacy, and confidentiality (IPC). This paper was the accumulation of extensive research works to resist the issues in the clouds. Many researchers had indulged in the process of enhancing the security of the cloud data by generating the keys, performing the cryptic mechanisms, auditing, de-duplication techniques, enhancement in handling the queries and many more approaches. The outcomes from the some works are discussed with other approaches to understand the objective accomplished by each work over the other. The general IPC issue and challenges exist in the cloud environment were listed and it was identified that there is a necessity for the better methodology to accomplish the robust cloud environment.

***Keywords*: Cloud Computing, Data Security, Data Integrity, Data Privacy, Data Confidentiality.**

I. INTRODUCTION

The clouds were classified as the public cloud that was reckoned to be untrusted, the private cloud that was deliberated as the semi-trusted or fully trusted and the hybrid cloud which was the combination of both the private and public clouds. Hence more data were being transmitted or processed or shared between the various clouds to respond to the user requirement. During this process, the data from the user were outsourced. Thus there was a necessity to protect for its privacy and against duplications [1].

The cloud computing offers numerous users benefits and perform characterization of challenges in certain areas, issues on security is a significant concern. In general, security is disturbed with the issue on confidentiality, availability, and integrity of data [2].

Privacy was other users might neglect the capability of a specific or group to isolate themselves or data about themselves and thus reveal them selectively [3] User data. Reduplication knowledge has been extensively employed in the cloud storage, which refers that the similar data frequently were deposited once but shared multiple instances by unlike users. This would decrease the space for storage and simplify the cloud service providers (CSP) cost, but attackers could breach the data by knowing the hash code. Then, it was likely to disclose the sensitive data of the cloud [4].

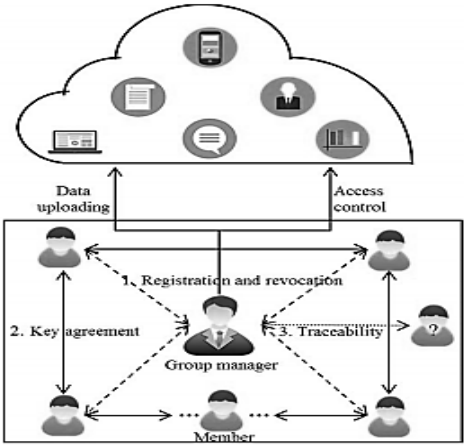


Fig.1 System Model for Secure Cloud Computing

II. RELATED WORKS

Since we know that the data that present in the cloud face many threats concerning its integrity, privacy, and confidentiality, many scholars generate the novel algorithms to secure the data. Some of the most recent works were collected for study, and the deliberations were segmented and detailed in the form of Data integrity, Data privacy, and Data confidentiality.

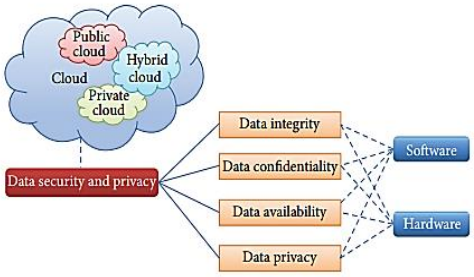


Fig.2 Cloud Computing Process Flow

2.1 Data integration

Tian et al [5] have examined user in public cloud storage through the anonymity inspection systems and have presented the attribute-based concept for checking cloud data integrity with two practical constructions. The work showed the suggested constructions are secure in the model of random oracle.

Revised Manuscript Received on August 30, 2019.
* Correspondence Author
K Priyadharshini*, Research Scholar, Sathyabama Institute of Science and Technology (Deemed to be university), Chennai, India.
R Aroul Canessane, Professor, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology (Deemed to be university), Chennai, India.

The method was recommended for cloud storage systems in real-world. The scheme to verify the dynamic integrity of the data stored in the cloud was explored by Yan et al. [6]. The bloom and lattice filters were employed for the attacks of quantum computers by sending the file and signature of a user to the service provider of cloud and TPA correspondingly. Under this approach, the verification by TPA could be challenging with the increased number of users. Li et al. [7] had developed the remote data possession checking (RDPC) algorithm to confirm the cloud data integrity. The RDPC had involved the key verification with other details in employing a unique user ID. The approach was effective and feasible in the cloud, but they mostly depend on the discrete logarithms and computational Diffie Hellman. An effective and straightforward scheme for auditing the integrity of the data was proposed by Balasubramanian et al. [8]. The algorithm was established on the fundamentals of the network coding and bilinear pairing. Codes generated for Functional minimum storage (FMSR) minimized the cost to repair the loss or corruption in data in the cloud

Ferretti et al. [9] had recommended a scheme established on the encrypted bloom filters which detect the unauthorized data modification in the cloud. The scheme reduced both the network and storage overhead relied on the workload and structure of the database. The approach was validated on the network and storage cost. There was not a proper mechanism to verify the freshness and completion of data.

2.2 Data Privacy

Li et al. [10] proposed an embryonic tool for key updating and authenticating zero-knowledge privacy of cloud data auditing. The presented approach had reduced the computation cost and the cost of communication along with the required security. The prototypes were constructed to verify the performance on the soundness zero-knowledge privacy. The real-time verification was not carried out to understand the practical problems. Jiang et al. [11] proposed the PP query scheme along with the LSH approach to permitting the storage of the data in the system that was distributed heterogeneously. The searching time was reduced without compromising the search quality and efficiency. The scheme was to be fine-tuned after implementation in the real world applications.

2.3 Data Confidentiality

Two schemes of Reversible Data Hiding over Encrypted Image (RDHEI) were revealed in the form of homomorphic encryption and encryption domain by Xiong et al. [12]. These two methods were combined to ensure the confidentiality of the data within the cloud and also in transmission. The major concern was the storage of ciphertext data in the cloud.

An attribute-based scheme was employed to verify the set of chosen attributes and ciphertexts under online/offline mode at the time of encryption and decryption with security in the assumption of weak Decisional Bilinear Diffie-Hellman (wDBDH) by Li et al. [13]. The suggested scheme was found to be proper under the restricted resource. The limitation was that the recommended scheme did not support the direct revocation of attributes in data sharing under the limited cloud computing resource.

III. RESEARCH METHODOLOGY AND ITS RESULTS DISCUSSION

3.1 Data Integrity: Yan et al. [6] had implemented the bloom filters similar to that of Ferrettiet al. [7], but he had bridged the gap of data verification by implementing the additional lattice filter. Even though both the Gaetaniet al. [14] had implemented the blockchain system for ensuring the data security, the former had a double layer approach that overcomes the applied brute force.

Yan et al. [6] analysed the characteristics and efficiency of the proposed scheme and tabulated the results as below.

Table.1 Characteristics of Proposed System

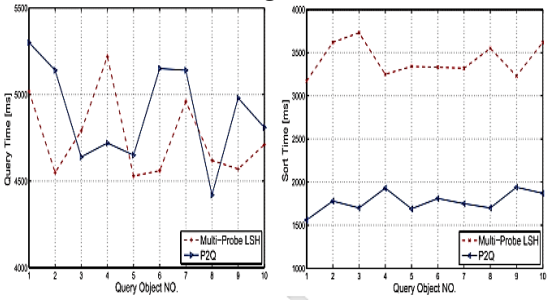
Sl. No	Characteristics	Proposed scheme
1	Integrity verification	Yes
2	Third party audit	Yes
3	Dynamic update	Yes
4	Whether the third party can obtain user files	No
5	Whether the signature algorithm can resist quantum computer attacks	Yes

Table.2 Efficiency of Proposed System

Sl. No	Efficiency	Proposed Scheme
1	Whether it is a random oracle model	Yes
2	Whether it is sampled	No
3	Public key length	mlog (12σ)
4	Private key length	mklog (1 + 2d)
5	Signature length	mlog (12σ)

By limiting the access to obtain the data in the cloud by the TPA, the data integrity was established by this technique and small size of the key had enhanced the efficiency of the scheme. By avoiding the sampling process, the scheme was free from the Gaussian sampling which was very expensive. In [7] valid verification and completion of data are not done. This limitation is overcome by the subsequent works [8]. For the present work, problems due to the existence of a single cloud server are taken as research gap which in turn makes more efficient

3.2 Data Privacy: Many researchers had implemented novel techniques to preserve the data from privacy, and they mainly concentrated on the computation time and cost for the searching keyword. The major concern was that most of the works were not performed on the real-time application. From the results obtained from Jiang et al [11].



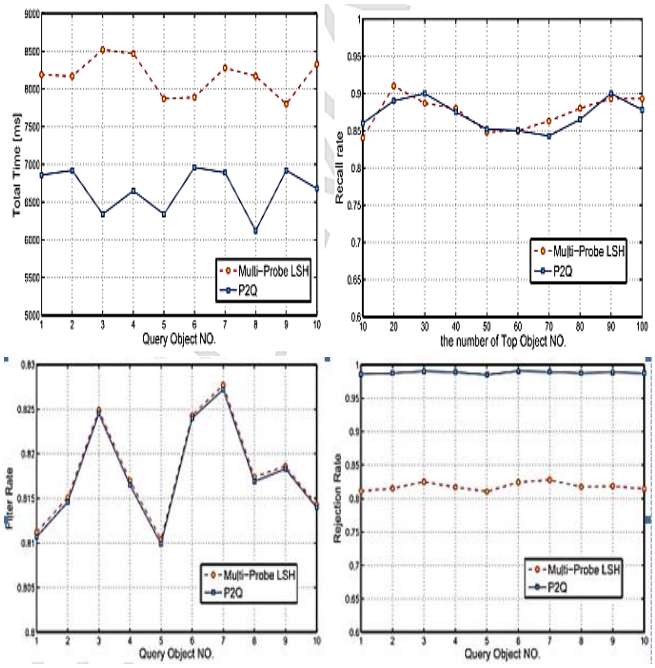


Fig.3 PP Performance of MPLSH

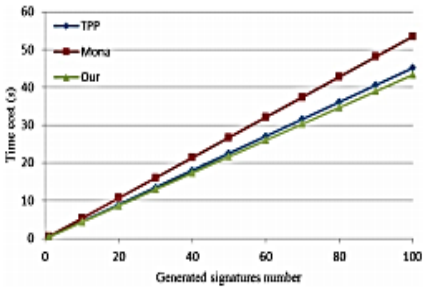
Table.4 Comparison between MPLSH and P2Q

Schemes	MPLSH	P2Q
Query time (ms)	4753	4895
sort time (ms)	3416	1773
Total time (ms)	8169	6668
average recall	0.8744	0.8713
Filter rate	0.8181	0.8177
Rejection rate	0.8181	0.998

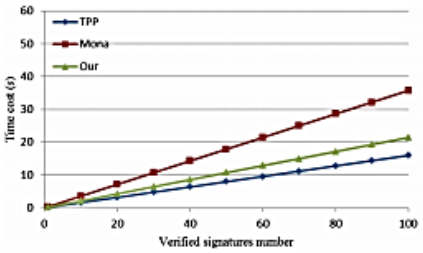
The method proposed by Jiang et al [11] had the response time and the average search efficiency which was 22.5% lesser and 20.8% more than the MPLSH. It was stated that the proposed P2Q was efficient for ensuring the data privacy.

In [10], verification in real-time was not carried out. Then in the subsequent works, the drawback is fine-tuned for real-world applications with trade-off between the effectiveness and security of the data. The practicality of the proposed techniques has not been validated which remains as the research gap for data privacy.

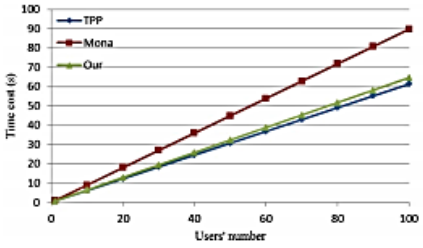
3.3 Data Confidentiality: Li et al. [13] and Huang et al. [15] had experimented the data confidentiality by implementing the attribute-based scheme. However, the former had used the limited resource environment compared to the latter. The outcomes obtained below:



(a)



(b)



(c)

Fig.4 Comparison on Efficiency in Access Control a) Cost for Access Generation, b) Cost for Access Verification, c) Total Time Cost for Access Control

It was clear that the proposed scheme was superior to Mona and TPP in both circumstances. This outcome was because TPP could only support key agreement among two entities, which requested for a huge amount of communication and computational costs for key generation between multiple users. Secure analysis scheme on encrypted cloud data with more realistic consideration, such as data synchronisation and protection of the data access patterns from CS is taken as research gap for the proposed work.

IV. CONCLUSION

The three major concerns in cloud computing concerning the integrity, privacy, and confidentiality of the data in the cloud environment were addressed. Many novels and innovative methods for solving security issues in cloud computing were enumerated mainly by its methodology, performance. From the study, it was clear that the threat for the clouds was changing from time to time and the approaches were being developed to ensure the security of data in the cloud. In most papers, the performance encompassed on the overheads or cost for computation and communication. Similarly, for data privacy and confidentiality were being handled by the keywords optimization for searching and innovative cryptic techniques respectively. As the outcome of the study, there was a need for enhancement of data security in the cloud although many already exist. The exploration of optimum technique or a combination of technology to resolve the data security issues had to be completed at the earliest to utilize the cloud service completely.

REFERENCES

1. Khan, Abdul & Khan, SiffatUllah&Ilyas, Muhammad &Azeem, Muhammad. (2012). A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing. *IOSR Journal of Computer Engineering. 1*. 2278-661.

2. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 12, pp. 1947–1960.
3. J. Krumm, "A survey of computational location privacy," Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399, 2009.
4. C. Cachin and M. Schunter, "A cloud you can trust," IEEE Spectrum, vol. 48, no. 12, pp. 28–51, 2011.
5. Tian, M., Wang, L., Zhong, H., & Chen, J. (2018). *Attribute-based Data Integrity Checking for Cloud Storage. Fundamental Informaticae, 163(4), 395–411*.
6. Yan, Y., Wu, L., Gao, G., Wang, H., &Xu, W. (2018). A dynamic integrity verification scheme of cloud storage data based on lattice and Bloom filter. Journal of Information Security and Applications, 39, 10–18.
7. Li, J., Yan, H., & Zhang, Y. (2018). Certificateless public integrity checking of the group shared data on cloud storage. IEEE Transactions on Services Computing, 1–1.
8. Balasubramanian, V., & Mala, T. (2018). Cloud data integrity checking using bilinear pairing and network coding. Cluster Computing. doi:10.1007/s10586-018-1805-z.
9. Ferretti, L., Marchetti, M., Andreolini, M., &Colajanni, M. (2017). A symmetric cryptographic scheme for data integrity verification in cloud databases. Information Sciences, 422, 497–515.
10. Li, Y., Yu, Y., Yang, B., Min, G., & Wu, H. (2018). Privacy-preserving cloud data auditing with an efficient key update. Future Generation Computer Systems, 78, 789–798.
11. Jiang, R., Lu, R., & Choo, K.-K. R. (2018). Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data. Future Generation Computer Systems, 78, 392–401.
12. Xiong, L & Shi, Y. (2018). On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing. Computers, Materials, and Continua. 55. 523-539.
13. Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security, 72, 1–12.
14. Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2017). Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage. IEEE Transactions on Information Forensics and Security, 12(4), 767–778.
15. Huang, Q., Yang, Y., &Shen, M. (2017). Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Future Generation Computer Systems, 72, 239–249.