Storage Cost			Computation Cost		
DO	TPA	Server	DO	TPA	Server
O(1)	O(1)	O(2n)	O(n)	O(1)	O(1)

Table 2:Storage and computation cost of our proposed scheme

We compared our scheme with the existing remote integrity checking methods. The comparison analysis of our proposed methods with the existing methods are illustrated in the Table 1. It shows that our scheme is the one which offers the highest probability of corruption detection. And also if there are corruptions like appending, deletion, and insertion of malicious data in the data stored in cloud , our scheme detects the corruptions with the highest probability of 1.

File Size (KB)	Encryption Time (milliseconds)	Decryption Time (milliseconds)
1	15	20
2	25	27
3	32	35
4	35	47
5	40	50
6	44	46
7	50	48
8	51	48
9	59	54
10	64	65

Table 3:Time of encryption and decryption of different files

Probability of detection of data replacement corruption is illustated in Fig.8. From this it is inferred that, the probability of detection of data replacement corruptions is higher in our proposed sytem and in the papers[2][3][4][8]. But for the other data corruptions like data deletion, data insertion and data appending, our proposed system has the highest probability detection of 1, that was not achieved through the previous integrity checking methods.

7 Conclusion

In this paper, we have analyzed various security challenges in cloud environment and proposed a suitable solution for confidentiality and integrity assurance by designing an efficient block cipher, 2-keys symmetric encryption technique. This proposed scheme can be applied for the secure storage of bulk data . After the detailed study, it is analyzed that it is the first method that detects the data corruptions with the probability of 1. This method is appropriate for the data that is dynamically changing. Our scheme requires less computation and communication cost ,and can be used for large-scale cloud storage systems. Our encryption scheme can also be applied for encrypting image and video files.

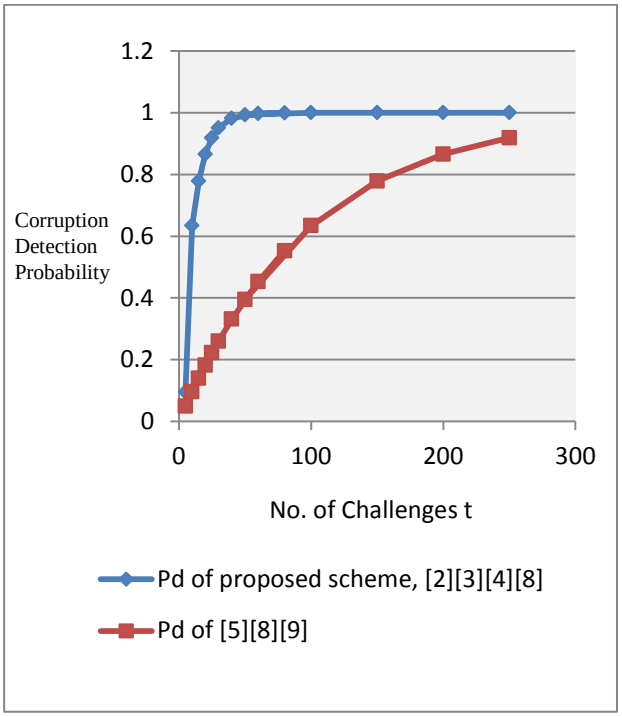

Fig.8: Probability of detection Pd of data replacement corruptions for 100 blocks, 10 sectors in a block and 1corrupted block

References

[1] Veeralakshmi Ponnuramu, and Latha Tamilselvan., (2014), 'Encryption for Massive Storage in Cloud' *in Computational intelligence in Data Mining, Volume 2,pp 27-38, Smart Innovation, Systems ,and Technologies(Springer), volume 32*.

[2] C.Wang , Q.Wang, S.S.M.Chow, K.Ren,W.Lou, (2013) , 'Privacy-Preserving Public Auditing for Secure Cloud Storage' , *IEEE Transactions on Computers* , Vol 62, No.2,.

[3] Ponnuramu Veeralakshmi. and Latha Tamilselvan, (2012).' Data integrity proof and secure computation in cloud computing'. *J. Comput. Sci., 8: 1987-1995*.

[4] Kan Yang, Xiaohua (2013) ' An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing', *IEEE Transactions On Parallel and Distributed systems*,VOL 24, NO. pp.1717-1726.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, (2012),'Toward Secure and Dependable Storage Services in Cloud Computing', *IEEE Transactions On Services Computing*,VOL. 5, NO. 2, pp.220-232.

[6] Pearson,(2009), 'Taking Account of Privacy when Designing Cloud Computing Services', in *Proceedings of ICSE-Cloud'09*, Vancouver.

[7] A.Juels and B. S. Kaliski, Jr.,(2007),'Pors: proofs of retrievability for large files,' in CCS .'07: *Proceedings of the 14th ACM conference on Computer and communications security*. New York, NY, USA: ACM, pp. 584–597.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song,(2007), 'Provable data possession at untrusted stores,' in CCS '07*: Proceedings of the 14th ACM conference on Computer and communications security. New York*, NY, USA: ACM, pp. 598– 609.

[9] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou,(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- 858.

[10] M. Jensen, et al.,(2009), 'On Technical Security Issues in Cloud Computing,' in *IEEE International Conference on Cloud Computing*, Bangalore, India, pp. 109-116.

[11] Lifei Wei , Haojin Zhu, Zhenfu Cao, Weiwei Jia,(2010), 'SecCloud: Bridging secure storage and computation in cloud', in ICDCS'10.

[12] C.Wang, Q. Wang, K. Ren, and W. Lou, (2009), 'Ensuring Data Storage Security in Cloud Computing,' *in Proc. of IWQoS'09*.

[13] H. Shacham and B. Waters,(2008), 'Compact Proofs of Retrievability,', *Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology* pp.90-107.

[14] E.-C. Chang and J. Xu,(2008), 'Remote integrity check with dishonest storage server,' *in Proc. Of ESORICS'08.Berlin, Heidelberg: Springer-Verlag*, pp. 223–237.

[15] C. Wang, Q. Wang, K. Ren, and W. Lou,(2010), 'Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing,'*Proc. IEEE INFOCOM*, pp. 525-533.

[16] Y. Zhu, H. Hu, G. Ahn, and M. Yu,(2012), 'Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage', *IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244.*

[17] Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, (2007), 'Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds,',*Proc. ACM Symp. Applied Computing*, pp. 1550-1557.

[18] W. Stallings, Cryptography and network security principles and practice, Fourth edition, Prentice hall, 2007