ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 3, Issue 2, February 2018

De-duplication and Security Using 3D AES over Cloud

[1] Renuka C. Deshpande, [2] S. S. Ponde
[1] Department of Computer Science and Engineering Marathwada Shikshan Prasark Mandal's Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2016-2017
[2] Associate Professor, Department of Computer Science and Engineering Marathwada Shikshan Prasark Mandal's Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2016-2017

Abstract: **De-duplication process is being mostly used in cloud server space to shrink the quantity of server space and reduce network bandwidth. To eradicate duplicate pieces of repeat data, Data de-duplication is exclusive data compression proposal used. To protect the confidentiality & isolation of receptive data while supporting de-duplication, the convergent encryption method has been proposed to encrypt data before outsourcing. For healthier data defense, this manuscript takes the primary effort to properly deal with the difficulty of certified data de-duplication. Apart from usual de-duplication structure, the differential rights concept for users has further measured in replica check moreover the records itself. There are numerous novel de-duplication constructions supporting certified replica check in fusion cloud architecture. Security investigations express that our proposal is secure in conditions of the characterization specified in the proposed security representation. As an evidence of conception, we implement a trial product of our future certified duplicate check scheme and conduct testbed experiments using our trial product. We include SHA-1 algorithm to de-duplicate data, IBE for the authentication of users. We also enhanced the security of cloud data by using symmetric algorithms i.e. Modified (3D) AES with least operating cost evaluate to previous research operations. The proposed results find that the storage, speed and security have been increased compared to previous research operations.**

Index Terms**: De-duplication, Confidentiality, Hybrid cloud, differential privileges, 3 DAES.**

I. INTRODUCTION

Cloud Computing offers high performance, shared resources, parallel supercomputing, effectively infinite size to users. Users can access cloud-based applications and services from anywhere. All he need is a device with an Internet connection. Simultaneously, cloud will provide the massive amount of storage and feasible resources within the low costs. Increasing extreme amount of data in military & research areas, financial portfolios, IT environments, needs large storage database, large network bandwidth & power sources creating the major challenge in future. Data de-duplication will be the only solution to this critical problem. Data de-duplication is the efficient technique to density technique for dropping duplicate replica of data. It reduces the extent of by sent over network and improves capacity to store data. Rather keeping many copies of data it saves only one. De-duplication has been done on various levels like file level, block level, byte level, bit level, document level, and piece level. Even though applying powerful algorithm data is susceptible to both in-house and outdoor attacks. A traditional encryption strategy requires special users toward encrypt their records with their personal keys. Convergent key is produced after computing hash price of the content of data. Convergent keys are used to encrypt/decrypt the data, but in several papers, separate encryption algorithms be used to encrypt/decrypt data like symmetric or asymmetric algorithms. To prevent unofficial attackers to get to up to sensitive data (POW) evidence of ownership protocol is needed to check authority of users. If the identical files found in S-CSP then pointer will provide to the user to that file and only data owners can decrypt that file using decryption keys. Convergent keys play the role of de-duplication. The every file is having particular rights to specify different category of users & data owners are having differential privileges access. In subsequent systems they cannot hold up differential authorization replica check. The only user is capable to perform duplicate check which has found matching privileges and copy of same file in cloud storage.

II. LITERATURE SURVEY

In the Existing systems there are some disadvantages like Lack of user privacy, Lack of data confidentiality, Lack of data integrity, Unsecured data duplication mechanism performed, Redundant data avoidance systems cannot support differential authorization duplicate check, Traditional encryption requires different users to encrypt their data with their own keys. Thus, identical data copies of different users will lead to different cipher texts, making de-duplication impossible. Data de-duplication performed at service

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 3, Issue 2, February 2018

provider level without considering user privileges, data get stored at cloud server level with related privileges keys.

AES Algorithm

AES is also a block cipher algorithm based on Feistel network, which uses 128 bits block size and varying key length of 128, 192 and 256 bits. Depend on the key length the number of rounds performed for encryption varies between 10, 12, or 14 rounds. Each AES round performs Key expansion, Sub-byte generation, Column-mix and Add-round key. AES provides a high security level since uses variable length key bits. Today most of the attackers are capable of breaking AES algorithm. The first cryptanalysis of 6-round AES was provided by its designers, who have shown how to break six rounds of AES-128 using a multi-set attack. Some related key attacks can go up to 10 rounds on AES-192 and AES-256. square attacks break 7 rounds, meet in the middle attack break 7 rounds, impossible differential attack break 7 rounds, new key related & open key attack break full AES 192 and AES 256, so best of these attacks reached 7 rounds for AES 128,10 rounds AES 192,AES 256. We need to make modification or improve complexity of operations of AES algorithm.

Mathematical Module for 3DAES

In 3DAES the four steps of AES are same i. e shift row, sub byte substitution, Column-mix and Add-round key. But that revolves around six sides of the cube 4*4 matrixes.

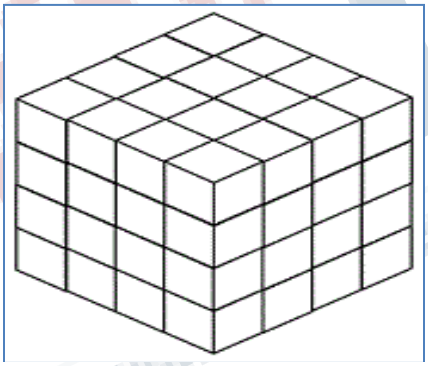

Figure 3.1: Cube Structure

- 4*4=16 bytes Matrix
- 16*6= 96 blocks
- 6 Rounds of operation

Operation formula

- Add_ round_ key (mix_ column(shift_row(byte_sub(state))))
- Add_ round_ key ((shift_row(byte_sub(state)))).

Attacks which are failed on 3DAES

Known-Plaintext Attack, Chosen-Plaintext Attack, chosen chipher text attack, Meet in the middle attack, man in the middle attack, brute force attack, dictionary attack, birthday attack, pre computation attack, denial of service attack, Side channel attack, Sql injection.

IV. PERFORMANCE ANALYSIS

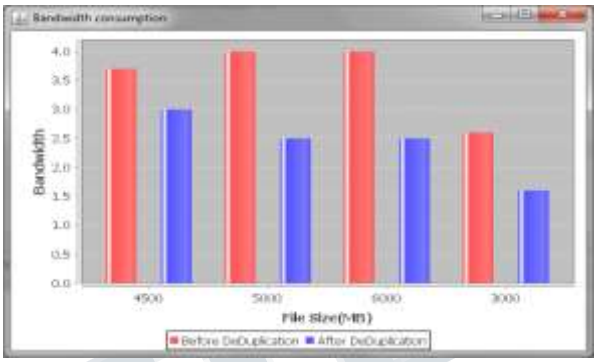

Figure 4.1 Bandwidth

Sr. no.	File Size(Mb)	Bandwidth Before deduplication	Bandwidth After deduplication
1	1000(mb)	0.2ms	0.1ms
2	1500(mb)	0.4ms	0.2ms
3	2000(mb)	0.5ms	0.3ms
4	2500(mb)	1ms	0.5ms
5	2700(mb)	1.5ms	1ms
6	2900(mb)	2ms	1.5ms
7	3000(mb)	2.5ms	1.5ms
8	3500(mb)	3ms	2.5ms
9	4000(mb)	3.7ms	3ms
10	500(mb)	4ms	2.5ms
11	6000(mb)	4ms	2.5ms
12	6500(mb)	5ms	3ms
13	7000(mb)	7ms	4ms

Table 4.1 Bandwidth

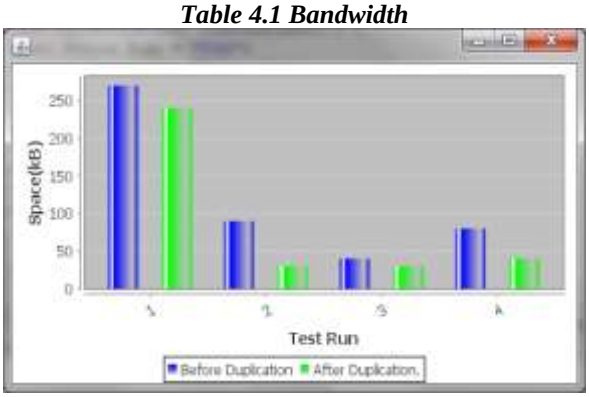

Figure 4.2 Storage

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 3, Issue 2, February 2018

Sr no.	No. of files	Before Deduplication	After Deduplication
1	3	50(mb)	25(mb)
2	4	100(mb)	50(mb)
3	5	150(mb)	75(mb)
4	8	200(mb)	100(mb)
5	10	270 (mb)	150(mb)
6	15	300(mb)	150(mb)
7	18	350(mb)	175(mb)
8	20	190(mb)	30(mb)
9	22	220(mb)	110(mb)
10	24	250(mb)	125(mb)
11	30	160(mb)	30(mb)
12	35	200(mb)	100(mb)
13	40	40(mb)	40(mb)
14	50	300(mb)	150(mb)

Table 4.2 Storage

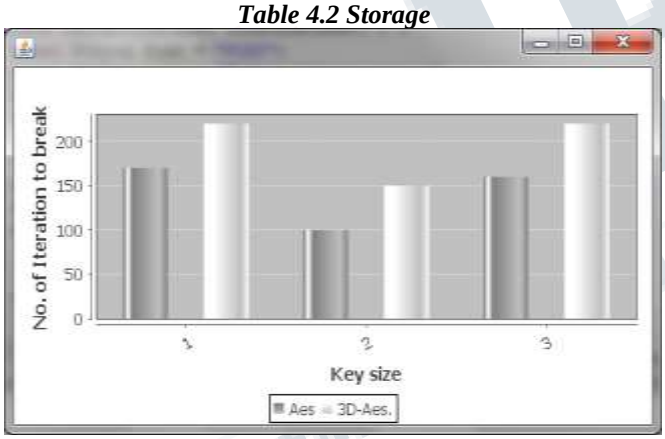

Figure 4.3 Security

Key size	Possible combinations (AES)	Possible combinations (3D AES)
128 bit	$3.4*10^{38}$	$3.4*10^{6*38}$
192 bit	$6.2*10^{57}$	$6.2*10^{6*57}$
256 bit	$1.1*10^{77}$	$1.1*10^{6*77}$

Table 4.3 Key size versus possible Combination Required, brute force Attack to crack AES and 3DAES

Figure 4.4 Time

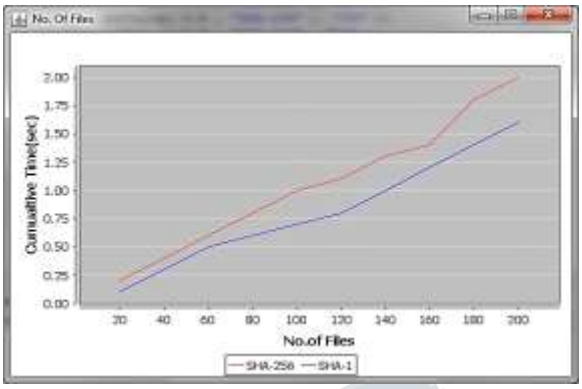

Figure 4.6 Time

Sr.no	No. of files	Time to upload For SHA1	Time to upload For SHA1
1	10	0.125s	0.20 s
2	20	0.75s	0.3 s
3	30	0.65s	0.5 s
4	40	0.9s	0.65 s
5	50	1.00s	0.9s
6	60	1.15s	1.00 s
7	70	1.35s	1.15s
8	80	1.60s	1.35 s
9	90	1.85s	1.60s
10	100	1.00s	1.85s
11	120	1.15s	1.00s
12	140	1.35s	1.15s
13	160	1.65s	1.35s
14	180	1.85s	1.6s
15	200	2s	1.85s
16	220	3s	2s

Table 4.4 Cumulative Time

V. CONCLUSION

In the proposed work de-duplication strategy reduces space of the cloud, bandwidth of the network. 3DAES gives new encryption technique in advance to AES i. e more security over the private cloud in future.

VI. FUTURE SCOPE

Another Encryption Algorithms could be modified for security in future. It will include experiments on Video and

audio data & de-duplicated, that will save storage of the cloud much greater. Focus will be to improve encryption time and decryption time.

REFERENCES

[1] Guljar P. Shaikh1, S. D. Chaudhary, Priyanka Paygude, Debnath Bhattacharyya "Achieving secure deduplication by using private cloud and public cloud"-International Journal of Security and Its Applications Vol. 10, No. 5 (2016) pp.17-26 2016

[2] B. Aparna, Prof K. S. M. V Kumar "Privacy preserving and Authorized data Deduplication in public cloud framework,"- International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 10, October-2015.

[3] Prof. N.B. Kadu, Mr. Amit Tickoo, Mr.Saurabh I. Patil, Mr. Nilesh B. Bhagat, Mr. Ganesh B. Divte "A hybrid Cloud approach for secure Authorized deduplication"- International Journal of Scientific and Research Publications, Volume 5, Issue 4, April 2015.

[4] Sumedha A. Telkar (S. A. Maindakar) 1, Dr M Z Shaikh "secured and efficient cloud storage data deduplication system"- International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016.

[5] Rushikesh Naiknaware, Omkar Deshpande, Abhishek Kangle, Himalay Koli, Dipmala Salunke "A hybrid approach for secure authorised deduplication"- International Journal of Innovative Research in Science, Engineering and Technology Vol. 5, Issue 5, May 2016.

[6] Jin Li, jingwei Li,Xiaofeng Chen,Chunfu jia and wenjing Lou "identity-based Encryption with outsourced revocation in Cloud Computing"- IEEE TRANSACTIONS ON COMPUTERS.

[7] paritosh S. patil "New Encryption technique For Secure SMS Transmission"- International Journal of advanced computer Technology,3(11),nov-2014(volume-3,issue-11).

[8] zheng yan, mingjun wang,athanasios vasilakos "Encrypted data management with deduplication in cloud computing"-researchgate,IEEE cloud computing ,March 2016.

[9] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," in Proc. IEEE Trans. Parallel Distrib. Syst., http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.284, 2013.

[10] P. Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-duplication," in Proc. 24th Int. Conf. Large Installation Syst. Admin., 2010, pp. 29–40.

[11] Cryptography and Network Security – by Atul Kahate – TMH.

[12] "Deduplication Using SHA-1 and IBE with Modified AES" Renuka C. Deshpande1, S. S. Ponde2 , International Journal of Science and Research (IJSR).