ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

# A Review on Achieving Security by Fragmentation and Replication of Data (Drop)

Jyoti Bansode, Anjana Ghule[2]

PG Scholar, Dept. of Computer Science and Engineering, Government College of Engineering, Dr.Babasaheb Ambedkar Marathwada University, Aurangabad, India.[1]

Asst. Professor, Dept. of Computer Science and Engineering, Government College of Engineering, Dr.BabasahebAmbedkar Marathwada University, Aurangabad, India.[2]

**ABSTRACT:** Distributed computing (CC) is a rising pattern that offers number of essential focal points. One of the key preferences of CC is pay according to utilize, where clients will pay just as indicated by their use of the administrations. At present information era is enhancing clients stockpiling accessibility. There is have to outsource such enormous measure of information. There are numerous Cloud Service Providers (CSP). CSP is developing pattern for quantities of clients and associations lessen the weight of nearby information stockpiling and upkeep. The information trade off might happen because of assaults by different clients and hubs inside of the cloud. In this manner, high efforts to establish safety are required to ensure information inside of the cloud. In any case, the utilized security system should likewise consider the enhancement of the information recovery time. In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that all in all methodologies the security and execution issues. In the DROPS philosophy, we separate a document into parts, and repeat the divided information over the cloud hubs. Each of the hubs stores just a solitary piece of a specific information record that guarantees that even if there should arise an occurrence of a fruitful assault, no significant data is uncovered to the aggressor. Besides, the hubs putting away the sections are isolated with certain separation by method for diagram T-shading to preclude an aggressor of speculating the areas of the parts. Besides, the DROPS approach does not depend on the customary cryptographic strategies for the information security; along these lines alleviating the arrangement of computationally costly techniques. We demonstrate that the likelihood to find and trade off the greater part of the hubs putting away the pieces of a solitary document is to a great degree low. We likewise look at the execution of the DROPS procedure with ten different plans. The larger amount of security with slight execution overhead was watched.

**KEYWORDS**: Centrality, cloud security, fragmentation, replication, performance, T-coloring.

## I. INTRODUCTION

The utilized security procedure should likewise consider the improvement of the information recovery time. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that aggregately approaches the security and execution issues. In the DROPS approach, we separate a document into sections, and duplicate the divided information over the cloud hubs. Each of the hubs stores just a solitary section of a specific information record that guarantees that even in the event of a fruitful assault, no significant data is uncovered to the aggressor. [6]Additionally, the hubs putting away the parts are isolated with certain separation by method for diagram T-shading to restrict an aggressor of speculating the areas of the pieces. Information replicationis a standout amongst the most critical system utilized for evacuating the indistinguishable duplicates of rehashing information and it is utilized as a part of the distributed storage with the end goal of diminish the storage room. Be that as it may, there is one and only duplicate for every record put away in cloud regardless of the fact that such document is claimed by immense number of clients. Keeping the numerous information duplicates with comparative substance replication

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

wipes out repetitive information by keeping stand out physical duplicate and allude other excess information to that duplicate. [1]Information replicationcan be record level or square level. The copy duplicates of indistinguishable document dispenses with by record level de-duplication. Furthermore, square level replication dispenses with copy pieces of information that happen in non-indistinguishable records. [5]This framework allots the document pieces utilizing T-shading diagram system. To keep up respectability we are giving the Third Party Auditor plan which makes the review of document put away at cloud and tells the information proprietor about record status put away at cloud server. This framework bolsters security difficulties, for example, approved copy check, respectability, information privacy and dependability.

## II. RELATED WORK

The utilized security technique should likewise consider the advancement of the information recovery time. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that all in all methodologies the security and execution issues. The DROPS techniques separate a record into pieces, and recreate the divided information over the cloud hubs. Each of the hubs stores just a solitary section of a specific information record that guarantees that even if there should arise an occurrence of a fruitful assault, no important data is uncovered to the assailant. Additionally, the hubs putting away the parts are isolated with certain separation by method for chart T-shading to preclude an assailant of speculating the areas of the sections.

### 1. A HybridCloud Approach for Secure Authorized Replication [1]

**From This Paper we Referred-**

In the proposed framework we are providing so as to accomplish the information replication the confirmation of information by the information proprietor. This confirmation is utilized at the season of transferring of the document. Every document transferred to the cloud is additionally limited by an arrangement of benefits to determine which sort of clients is permitted to perform the copy check and get to the records. New replication developments supporting approved copy check in half breed cloud design in which the copy check tokens of documents are produced by the private cloud server with private keys. Proposed framework incorporates verification of information proprietor so it will actualize better security issues in distributed computing.

### 2. Secured Authorized De-duplication Based Hybrid Cloud Approach[2]

**From This Paper we Referred-**

United encryption gives information privacy in de-duplication. A client gets a united key from every unique information duplicate and encodes the information duplicate with the concurrent key. What's more, the client likewise infers a tag for the information duplicate, such that the tag will be utilized to distinguish copies. To recognize copies, the client first sends the tag to the server side to check if the indistinguishable duplicate has been now put away. Both the focalized key and the tag are autonomously inferred, and the tag can't be utilized to find the joined key and trade off information secrecy. Approved information replication was proposed to ensure the information security by including differential benefits of clients in the copy check a few new de-duplication developments that backing in approved copy check in cross breed cloud design.

### 3. Implementation Replication System with Authorized Users[3]

**From This Paper we Referred-**

This paper speaks to that, numerous systems are utilizing for the end of copy duplicates of rehashing information, from those procedures, one of the imperative information pressure method is information duplication. Numerous focal points with this information duplication, for the most part it will diminish the measure of storage room and spare the transfer speed when utilizing as a part of distributed storage. To secure privacy of the touchy information while supporting replication information is encoded by the proposed joined encryption procedure before out

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

sourcing. Issues approved information duplication formally tended to by the principal endeavour of this paper for better assurance of information security. This is not the same as the conventional duplication frameworks. The differential benefits of clients are further considered in copy check other than the information itself. In half and half cloud engineering approved copy check bolstered by a few new duplication developments. In light of the definitions indicated in the proposed security demonstrate, our plan is secure. Evidence of the idea executed in this paper by leading proving ground tests. A Client project is utilized to display the information clients to do the record transfer process. A Private Server project is utilized to show the private cloud which deals with the private key and handles the document token calculation. A Storage Server program issued to store and de-copies documents. The Client gives the capacity calls to bolster token era and replication along the record transfer process. We watched that the data to Check replication and transfer the records, Fetching the Signs utilizing Hashing Algorithm, Checking for Duplication, document transferring, document downloading and aggressor attempting to attack(block) the cloud.

**4. Location-aware type ahead search on spatial databases: emetics and efficiency[4]**

**From This Paper we Referred-**

Clients regularly look spatial databases like yellow page information utilizing catchphrases to and organizations close to their present area. Such pursuits are progressively being performed from cell phones. Writing the whole question is lumbering and inclined to mistakes, particularly from cellular telephones. We address this issue by presenting sort ahead hunt usefulness on spatial databases. Like watchword inquiry on spatial information, sort ahead pursuit should be area mindful, i.e., with each letter being written, it needs to return spatial items whose names (or depictions) are substantial fruitions of the question string wrote in this way, and which rank most noteworthy as far as closeness to the client's area and other static scores. Existing answers for sort ahead inquiry can't be utilized straightforwardly as they are not area mindful. We demonstrate that a straight-forward mix of existing systems for performing sort ahead quest with those for performing vicinity seek perform inadequately. We propose a formal model for question preparing cost and create novel methods that enhance that cost. Our exact assessments on genuine and engineered datasets exhibit the adequacy of our systems. To the best of our insight, this is the RST take a shot at area mindful sort ahead pursuit.

**5.A Secured and Authorized Data Replication with Public Auditing [5]**

**From This Paper we Referred-**

This paper concentrates on private information replication method for cloud stockpiles. Instinctively, a private information replication convention permits a customer who holds private information demonstrates to a server who holds an outline string of the information that he/she is the proprietor of that information without uncovering additional data to the server. The proposed private information replication convention is provably secure in the recreation based structure accepting that the hidden hash capacity is crash flexible ,the discrete logarithm is hard and the deletion coding calculation E can eradication up to part of the bits in the vicinity of vindictive foes.

## III.GOALS AND OBJECTIVE

**Goals:**

1. This paper concentrates on private information replication method for cloud stockpiles.

2. Instinctively, a private information replication convention permits a customer who holds private information demonstrates to a server who holds an outline string of the information that he/she is the proprietor of that information without uncovering additional data to the server.

3. The proposed private information replication convention is provably secure in the recreation based structure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

accepting that the hidden hash capacity is crash flexible ,the discrete logarithm is hard and the deletion coding calculation E can eradication up to part of the bits in the vicinity of vindictive foes.

**Scope:**

1. The information proprietors lose the control over their delicate information once the last is outsourced to a remote CSP which may not be reliable.

2. This absence of control raises new impressive and testing errands identified with information secrecy and integrity assurance in distributed computing.

3. Customers require that their information stay secure over the CSP. Likewise, they need a solid confirmation that the cloud servers still 2 have the information and it is not being messed with or halfway erased after some time, particularly in light of the fact that the interior operation points of interest of the CSP may not be known not clients.

4. Encrypting delicate information before outsourcing to remote servers can deal with. The utilized security methodology should likewise consider the improvement of the information recovery time. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that all things considered methodologies the security and execution issues.

5. The DROPS strategy isolates a document into parts, and imitates the divided information over the cloud hubs. Each of the hubs stores just a solitary section of a specific information record that guarantees that even if there should arise an occurrence of a fruitful assault, no significant data is uncovered to the aggressor.

6. Moreover, the hubs putting away the sections are isolated with certain separation by method for chart T-shading to restrict an assailant of speculating the areas of the pieces.

## IV.PROPOSED ALGORITHM

**1. ALGORITHMFORFRAGMENTPLACEMENT**

O = {O1;O2;....;ON}
O = {SIZEOF(O1); SIZEOF(O2);.....; SIZEOF(ON)}
COL = {OPEN COLOR; CLOSE COLOR}
CEN = {CEN1; CEN2; .....;CENM}
COL ← OPEN COLOR FOR ALL I
CEN ←CENI| I

COMPUTE:
FOR EACHOK € O DO
SELECT SI | SI ← INDEXOF(MAX(CENI))
IF COLSI = OPEN COLOR AND SI>= OK THEN
SI← OK
SI ← SI − OK
COLSI ← CLOSE COLOR
SI'←DISTANCE(SI; T) P /*RETURNS ALL NODES AT
DISTANCE T FROM SI AND STORES IN TEMPORARY SET SI'*/

COLSI. ← CLOSE COLOR
END IF
END FOR

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

## V. AUDITING MECHANISM

**AUDITING STEPS**

1) Start
2) When user upload file fragments the hash value of these fragments is created using SHA-256 algorithm.
3) This value along with original fragment is sent to TPA. And fragments are stored at cloud server.
4) TPA generates a random set like public key pk, private key sk and signature σ on each block (Verification metadata).
5) TPA at the time of auditing computes the hash value of fragments stored at cloud with hash value they have.
6) If the hash value matches then TPA sends the status as safe to data owner.
7) If the hash value does not match then TPA sends the modified fragment id and original fragment to Proxy Agent.
8) Proxy agent search for that id at cloud and replaces the modified fragment with original fragment.
9) End.

**SHA-256**

1. Step 0: Initialize some variables
2. There are five variables that need to be initialized.
3. h0 = 01100111010001010010001100000001
4. h1 = 11101111110011011010101110001001
5. h2 = 10011000101110101101110011111110
6. h3 = 00010000001100100101010001110110
7. h4 = 11000011110100101110000111110000
8. Pick a string
9. Break it into characters Note that spaces count as characters.
10. Convert characters to ASCII codes
11. Convert numbers into binary
12. Put the numbers together:
13. Add the number '1' to the end:
14. Append '0's' to the end.
15. In this step you add zeros to the end until the length of the message is congruent to 448 mod 512.
16. Append original message length
17. 'Chunk' the message
18. Break the 'Chunk' into 'Words'
19. Break each chunk up into sixteen 32-bit words
20. 'Extend' into 80 words
21. XOR (We begin by selecting four of the current words. The ones we want are: [i-3], [i-8], [i-14] and [i-16].)
22. Left rotate
23. The main loop (This loop will be run once for each word in succession.)
24. Finally the variables are converted into base 16 (hex) and joined together.

**AES**

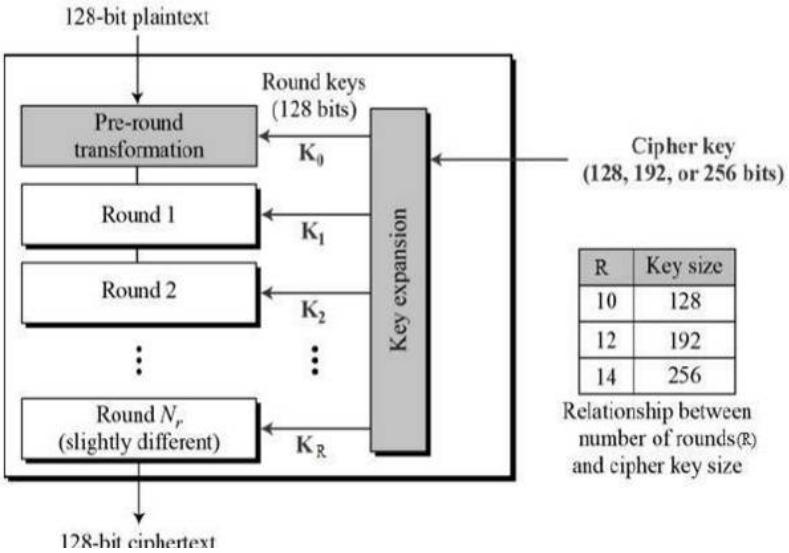
AES is a block cipher with a block length of 128 bits.
AES allows for three different key lengths: 128, 192, or 256 bits.
Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.
Except for the last round in each case, all other rounds are identical.
Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

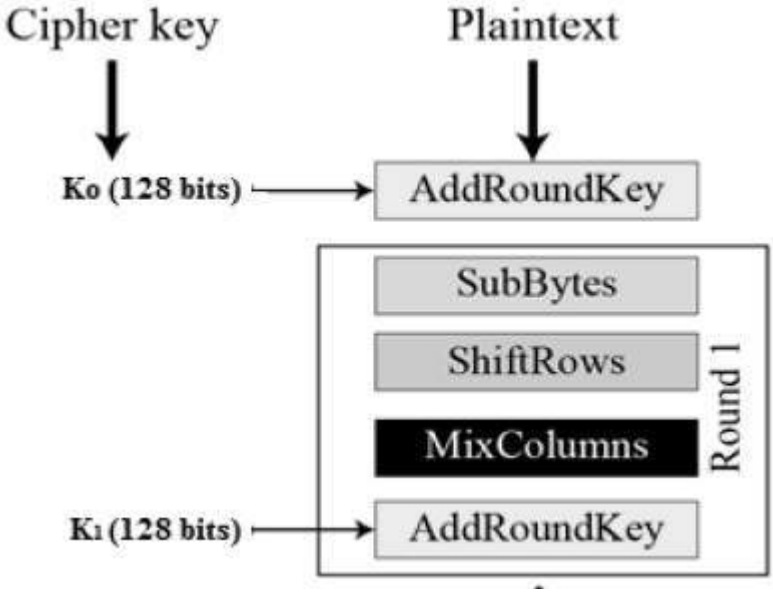



| R | Key size |
|---|---|
| 10 | 128 |
| 12 | 192 |
| 14 | 256 |

Relationship between number of rounds(R) and cipher key size

## VI. ENCRYPTION PROCESS

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −




**1) Byte Substitution (Sub Bytes)**

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2) **Shift rows**

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

**3) MixColumns**

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

**4) Addroundkey**

The 16 bytes of the matrix are now considered as 128 bits and are XOR to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

**Decryption Process**

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a cipher, the encryption and decryption algorithms need to be separately implemented, although they are very closely related.

## VII. ANALYSIS CHART

Comparative execution times (in seconds) of encryption algorithms

| Input Size (bytes) | DES | 3DES | AES | BF |
|---|---|---|---|---|
| 20,527 | 2 | 7 | 4 | 2 |
| 36,002 | 4 | 13 | 6 | 3 |
| 45,911 | 5 | 17 | 8 | 4 |
| 59,852 | 7 | 23 | 11 | 6 |
| 69,545 | 9 | 26 | 13 | 7 |
| 137,325 | 17 | 51 | 26 | 14 |
| 158,959 | 20 | 60 | 30 | 16 |
| 166,364 | 21 | 62 | 31 | 17 |
| 191,383 | 24 | 72 | 36 | 19 |
| 232,398 | 30 | 87 | 44 | 24 |
| Average Time | 14 | 42 | 21 | 11 |
| Bytes/sec | 7,988 | 2,663 | 5,320 | 10,167 |

Above table shows the time required to encrypt file with different encryption algorithm.
So the algorithm we are using is AES. This table shows that the AES requires less time as compared to DES.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

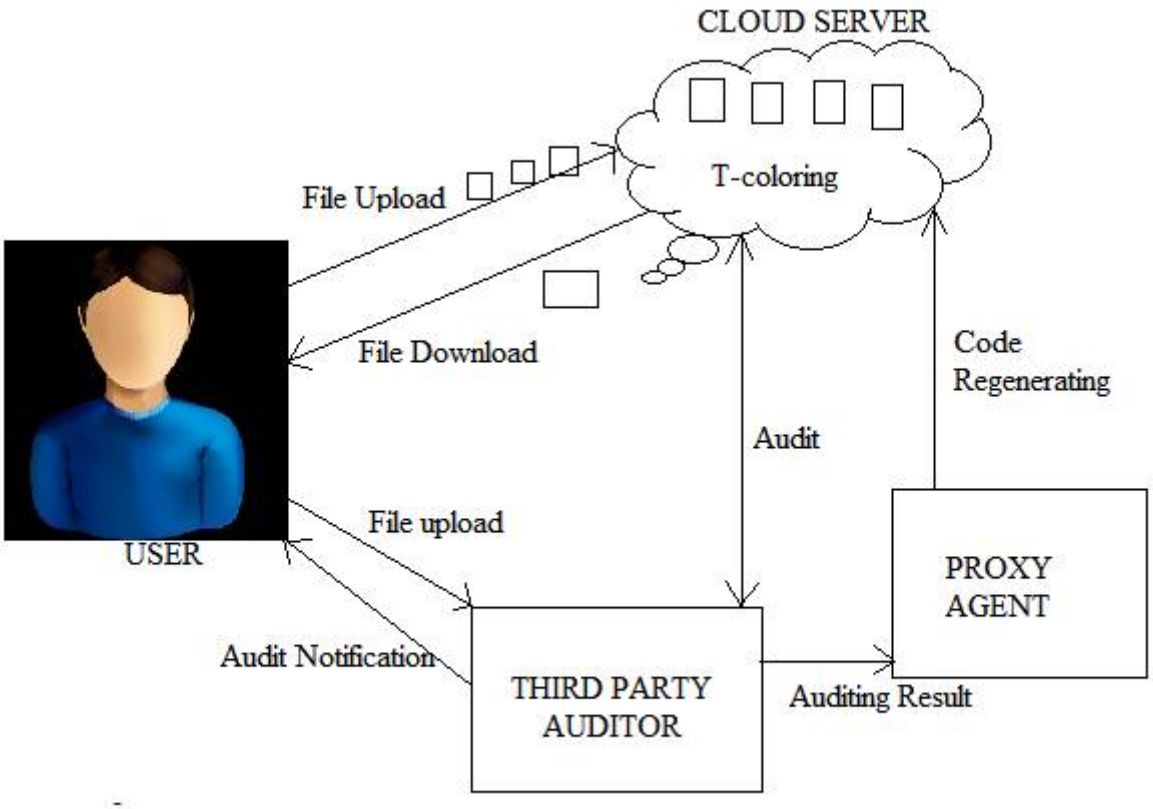
*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

| Algorithm | Output Size (Bits) | Internal State Size | Block Size | Length Size | Word Size | Rounds |
|---|---|---|---|---|---|---|
| SHA-0 | 160 | 160 | 512 | 64 | 32 | 80 |
| SHA-1 | 160 | 160 | 512 | 64 | 32 | 80 |
| SHA-224, SHA-256 | 224/256 | 256 | 512 | 64 | 32 | 64 |

Above table shows hash algorithms comparison. From the above algorithms we are using SHA-256 which requires less rounds. So for this we required less execution time.

## VIII. ARCHITECTURE




Suppose a graph G=(V;E) and a set T containing non-negative integers including 0. The Colouring is a mapping function f from the vertices of V to these to f non-negative integers, such that |f(x)- f(y)|≠ T, where (x;y) E. The mapping function f assigns a color to a vertex. In simple words, the distance between the colors of the adjacent vertices must not belong to T. Formulated by Hale, the T-colouring problem for channel assignment assigns channels to the nodes, such tha th e channels are separated by a distance to avoid interference.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

## IX. CONCLUSIONS

Outsourcing information to remote servers has turned into a developing pattern for some associations since it uproots the weight of nearby information stockpiling and support. In this work comprises the issue of making numerous duplicates of element information record and confirming those duplicates put away on untrusted cloud servers. The DROPS approach, a distributed storage security plot that all things considered manages the security and execution as far as recovery time. The information document was divided and the parts are scattered over different hubs. The hubs were isolated by method for T-shading. The fracture and dispersal guaranteed that no noteworthy data was realistic by an enemy if there should be an occurrence of a fruitful assault. No hub in the cloud, put away more than a solitary part of the same record. The execution of the DROPS procedure was contrasted and full-scale replication methods. The consequences of the recreations uncovered that the synchronous spotlight on the security and execution brought about expanded security level of information joined by a slight execution drop.

## REFERENCES

[1] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani,N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, "Quantitative comparisons of the state of the art data
Center architectures," Concurrency and Computation: Practice and Experience, Vol. 25, No. 12, 2013, pp. 1771-1783.
[2] K. Bilal, M. Manzano, S. U. Khan, E. Calle, K. Li, and A. Zomaya, "On the characterization of the structural robustness of data center networks," IEEE Transactions on Cloud Computing, Vol. 1, No. 1, 2013, pp. 64-77.
[3] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, "Energy-efficient data replication in cloud computing datacenters,"In IEEE Globecom Workshops, 2013, pp. 446-451. .
[4] Y. Deswarte, L. Blain, and J-C. Fabre, "Intrusion tolerance in distributed computing systems," In Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, Oakland CA, pp. 110-121, 1991.
[5] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
[6] W. K. Hale, "Frequency assignment: Theory and applications,"Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
[7] K. Hashizume, D. G. Rosado, E. Fernndez-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing,"Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.
[8] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.
[9] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.
[10] A. Juels and A. Opera, "New approaches to security and availability for cloud data," Communications of the ACM, Vol. 56, No. 2, 2013, pp. 64-73.
[11] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, "Dike: Virtualization-aware Access Control for Multitenant Filesystems,"University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.
[12] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.
[13] S. U. Khan, and I. Ahmad, "Comparison and analysis of ten static heuristics-based Internet data replication techniques,"Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008, pp. 113-136.
[14] A. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards Secure Mobile Cloud Computing: A Survey," Future Generation Computer Systems, Vol. 29, No. 5, 2013, pp. 1278-1299.
[15] A. N. Khan, M.L. M. Kiah, S. A. Madani, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing, The Journal ofSupercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706 .