Enhanced Cloud Performance and Security via Data Fragmentation Replication and Encryption

V.Nila #1, S.Manikandan #2
1 M.E Student, Department of Computer Science, Arasu Engineering College, Kumbakonam.
2 Assistant Professor, Department of Computer Science, Arasu Engineering College, Kumbakonam.
1.nilamahesh1@gmail.com
2.maniastra111@gmail.com

***Abstract*- Cloud security refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment. The data outsourced to public cloud must be unsecured give rise to security concerns. The security strategies must also use for data file or document etc. In this paper we propose these data fragmentation multiple encryption technique. In this technique must be provide high level security for document. This technique performed to common data is divided in to multiple fragment, the fragmented data are encrypted on the set of nodes. The fragmented data's are arranged based on distance node measure technique. We ensure controlled and fragmented data's are encrypted only for improve security. In this multiple encryption technique overcome the existing cryptography methodology.**

***Keywords*: Cloud computing, security, Distance node measure, File segmentation, Replication, Encryption.**

I.INTRODUCTION

Cloud security by identifying unique security requirements. Security enhance agility, scalability, availability, ability to adapt fluctuations according to demand accelerate development work and provide potential for cost reduction through optimized and efficient computing []. Secure overlay cloud storage with access control and assured deletion. Energy efficient data replication in cloud achieves minimizing network delay and bandwidth usage [].

Cloud computing is Symmetric (private) and Asymmetric (public) keys encryption. Symmetric key cryptography involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of one key for encryption and another different key for decryption[].To improve performance for using data retrieval time the nodes are selected based on resource graph technique, a cloud security ensures throughput, reliability and security[].

The data outsourced to a public cloud must be unsecured. Unauthorized data access by other users and processes must not be prevented. As discussed above, any weak entity can put the whole cloud at risk. Although an old problem, it still continues to receive significant attention from the database community due to its inherent difficulty, especially in the context of large datasets in the multi-nodes. Division and replicated data and to further improve the security we select the node in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by means of resource graph technique [6].

On the security of multiple encryption. The DFME technique based on two phase. In first phase nodes are selected based on resource graph. In second phase the nodes are selected initial placement of fragment based on between node measures [].On the other hand, multiple encryptions can bring favorable additional new features to a scheme. Combination of ordinary threshold encryptions may yield new threshold encryption with various access structures[].This paper proposes using a Data fragmentation and replication within a cloud and using cryptography to ensure the confidentiality, integrity, and authenticity of data and communications while attempting to address specific security vulnerability[].

The DFRE technique based on two phase. In first phase nodes are selected based on resource graph. In second phase the nodes are selected initial placement of fragment based on between node measures [].

II.RELATED WORK

Hashizume [7] Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form

[11].The authors in [10] approaches Cloud Computing focused in the so-called SPI model identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and ts environment. A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats. Our proposed scheme does not store whole file on a single node to avoid compromise of all of the data in case successful attack on the node. Software confidentiality is as important as data confidentiality to the overall system security. Software confidentiality refers to trusting that specific applications or processes will maintain and handle the user‟s personal data in a secure manner. In a cloud environment the user is required to delegate „„trust‟‟‟ to applications provided by the organization owning the infrastructure. Software applications interacting with the user‟s data must be certified not to introduce additional confidentiality and privacy risks.

III.PRELIMNARIES

A. Fragmentation Technique:

In cloud computing fragmentation is a phenomenon in which storage space is used inefficiently, reducing capacity or performance and often both. The exact consequences of fragmentation depend on the multiple cloud storage allocation for security purpose. The encrypted data are segmented into multiple packets, and each packet is individually sent to the cloud server for protected data. This process is to avoid the eaves dropping in the cloud and protect the data against hacking. The Cloud security of large scale system depends on the security of individual node. A successful intrusion in to a single node may have severe consequence not only for data and application on the victim node but also for other node[11].

B. Replication Technique:

Replication in computing involves sharing information so as to ensure consistency between redundant resources, such as software or hardware components, to improve reliability, fault tolerance, or accessibility. File-based replication is replicating files at a logical level rather than replicating at the storage block level. There are many different ways of performing this. Unlike with storage-level replication, the solutions almost exclusively rely on software. File level replication solution yield a few benefits. Firstly because data is captured at a file level it can make an informed decision on whether to replicate based on the location of the file and the type of file. Hence unlike block-level storage replication where a whole volume needs to be replicated, file replication products have the ability to exclude temporary files or parts of a file system. Moreover, if an attacker is uncertain about the locations of the ragments, the probability of finding fragments on all of the nodes is very low. Let us consider a cloud with M nodes and a file with z number of fragments.

C. Distance node measure:

The nodes are measured based on resource graph node selection. The DFRE methodology ensure integrity and consistency between each node selected. Moreover, the nodes storing the fragments are separated with certain distance by means of resource graph to prohibit an attacker of guessing the locations of the fragments. The nodes are measured using certain technique.

$$I_c(V) = \frac{1 - N}{\sum_{a \neq c} d(c, a)}$$

D. Multiple Encryption:

Encryption of data using multiple, independent encryption schemes (“multiple encryption”) has been suggested in a variety of contexts, and can be used, for example, to protect against partial key exposure or cryptanalysis, or to enforce threshold access to data. Most prior work on this subject has focused on the security of multiple encryption against chosen-plaintext attacks, and has shown constructions secure in this sense based on the chosen-plaintext security of the component schemesSubsequent work has sometimes assumed that these solutions are also secure against chosen-ciphertext attacks when component schemes with stronger security properties are used. Unfortunately, this intuition is false for all existing multiple encryption schemes.

Informally a multiple encryption is to encrypt a message by multiple cryptosystems. A multiple encryption scheme ME is generated by component ciphers. Specification Multiple encryption is a cryptosystem composed by separate component ciphers, each of which may be independent. Suppose {Ei}1≤i≤n is a set of compatible component ciphers, where for Ei, Enc-Geni a probabilistic key-generation algorithm, with the input (1k) and the internal coin flipping produces a public-secret key pair(pki, ski);
Enci an encryption algorithm, with an input message mi ∈Mi and the public key pki, with the internal coin flipping, outputs a ciphertext ci ∈Ci;

Deci a decryption algorithm, which is a deterministic algorithm, with the input ciphertext ci and the secret key ski, outputs a message mi or "⊥". A multiple encryption is a 3-tuple algorithm (MEnc-Gen,MEnc,MDec), where each algorithm may be combined from a number of public key cryptosystems with a unifilar connecting order. MEnc-Gen invokes every Enc-Geni, and writes their outputs to a key list with public keys PK = (pk1, ...,pkn) and secret keys SK = (sk1, ..., skn). MEnc with an input message M from message space M and PK, performs encryption MEnc on M by invoking a list of component encryption algorithms, eventually outputs a ciphertext C ∈ C. The decryption algorithm MDec takes (C, SK) as input and outputs M, or "⊥" if C is invalid. We also denote in brief the encryption algorithm as MEnc(M; COIN) (or MEnc(M)), and the decryption algorithm as MDec(C) in clear context, where COIN stands for the randomness used the multiple encryption. Essentially, we have two typical constructions: parallel construction, e.g., the generic construction given in [11],6 Rui Zhang et al.which the message is first split into shares by secret sharing then encrypted separately; sequential construction, e.g., the cascade cipher studied in [22], the message is encrypted by one component cipher then encrypted by another, and eventually forms the cipher text. By combining these two constructions, we get a hybrid construction, which we refer to hereafter as "natural" construction.

E. RESOURCE GRAPH INFORMATION:

In a graph theory resource graph coloring denoted by G = (V,E) given the set T of non-negative integers containing 0 is a function C:V(G) of node to the vertices of G such that replicate data. Moreover the node storing the fragmented data over cloud nodes stores only a single fragment of a particular data filethat ensures even in case of successful attack no meaningful information is revealed to the attacker.

Symbol	Meaning
A	Initiate Fragment data
G(V,E)	Distance between fragment data
R	Replication data
Wi	Nearest neighbor node calculated

IV. DFRE TECHNIQUE

The DFRE methodology consisting of N node each node consist of security and it provide performance. The Cloud user submits the input file into multiple segment and places each in a node then these segment are replicated on other set of nodes and the nodes are arranged based on resource graph colouring technique. If intruders attack in a node then do not guess which fragment in a node.

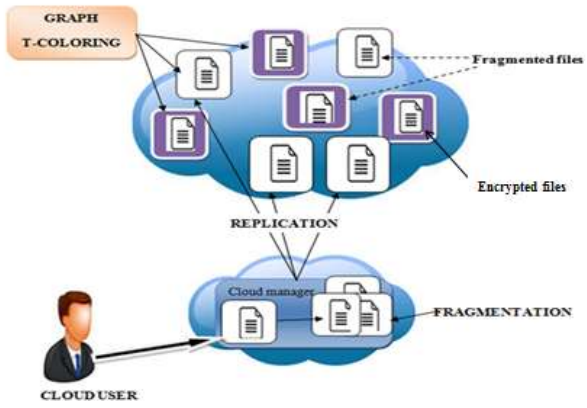

Fig. 1.DFRE Methodology

The System model of the DSR methodology N node, each with its own capacity of measure segment node Si. The total nodes of storage is Ri and Rj is the total time of all links within a selected path from Ri to Rj represented by R(i,j). We consider N number of file segment such that Sk denotes n segment of a file.

IV. ALGORITHM & DESIGN

In cloud security file are fragmented over a single point of failure.

1. Algorithm for Distance node measure algorithm

Inputs and initialization:
O = {O1;O2; ON}
O = {sizeof(O1); sizeof(O2) ;sizeof(ON)}
cois = {dis1;dis2….disN}
col _ open color i
dis _ ceni i
Compute:
For each OK > O do
Select Si S Si _ index of(max(ceni))
ifcolSi = open color and Ri>= ok then
Si _ OK
Si _ Sj _ OK
Col Si _ Close color
Si_ distance (Sj; T) P /*return all node at
distance T from Si and stores in temporary set Si*/
ColSi _ close color
end if
endforl = {open color; close color}

2.Multiple Encryption

Enc(P) = S K I (S ~ [S m (P)]) , (6)

M1 = SIn(P), (7)

M2 = S ~ (M 1) (8)

= S KI(SKI(P)) (9)

S~I(C)M1 and M2 are intermediate values in the computation of C from P, as shown in Figure 1. motivate the method o f cryptanalysis with the following observations:

If we knew K1 and a P - C pair, then it would be possible to compute the intermediate values M I and M2 from (7) and (10). This would let us m o u n t a k n o w n plaintext attack on K2 using (8). There are 256 values of K1, s o / f we could quickly determine the right K2 once we found the right K1, then cryptanalysis would only take 256 operations to search over K1. However, determining K2 using a k n o w n plaintext attack requires 256 operations and would result in complexity 2112.

V. EXPERIMENTAL RESULT

The proposed work secure data service that outsources data and security management on cloud without disclosing any user information with the help of proxy re-encryption and identity based encryption schemes must be used to Segment data. The file is splitting over multiple node the attacker do not hack the information about cloud file. Three datacenter networks is categorized by a DSR technique such as (a) Two tier (b) DCN network (c) Tree based structure.

DCN is server centric network architecture, core layers of node connected in a processing network.

C. RESULTS AND DISCUSSION

The DFRE methodology compared to other technologies such that (a) impact increasing in a number of a replication node,(b) changing storage capacity. (a) impact increasing in a number of replication node

The DFRE methodology increasing the number of node selected by 500 and 1000 to 3000 increasing node values are 500.

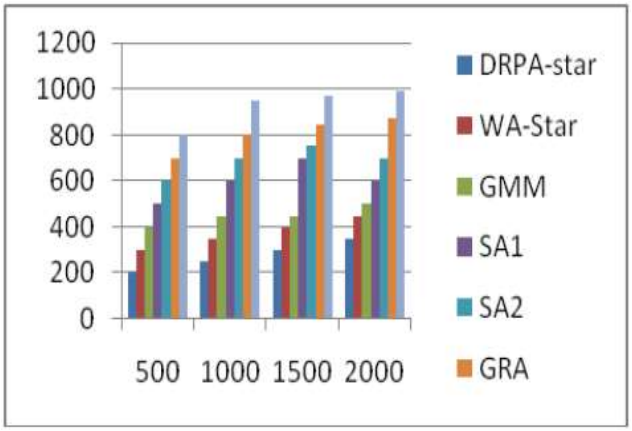

Fig 2: Fault tolerance level of DFRE technique

It is also important to mention that even higher read/write ratio values. The security and high performance are mentioned by DFRE fault tolerance. Replication cost and fragmentation cost is required for resource graph technique. Therefore the global replication perception of algorithm resulted in high performance SA1and SA2 due to the suffered search tree based selected for node. The DFRE methodology is proposed collectively approach the security and performance. To increase the security and performance level of data, the DSR methodology sacrifices the performance to certain extent.

CONCLUSION

We propose the DSR methodology, c cloud manager scheme that collectively deals with the security and high performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The node was separated by means of resource coloring technique. The result of the simulation focusing on simultaneous security and performance. In future work will save the time and provide high secured document in the cloud.

REFERENCES

[1] 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 Transaction on Cloud Computing, Vol. 1,No. 1, 2013, pp.64-77.

[2] B.Grobauer, T.Walloschek, and E.Stocker, "understanding Cloud computing Vulnerabilities," IEEE Security and Privacy, Vol.9,No.2,2011, pp.50-57.

[3] 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.

[4] M.Hogan, F.Liu, A.Sokol, and J. Tong,"NIST Cloud computing standards roadmap," NIST Special Publication, July 2011.

[5] Y.Tang P.P. Lee, J.C.S. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured

deletion,"IEEE Transaction on Dependable and Secure computing, Vol.9,No.6, Nov 2012. Pp 903-916.
.[6] D.Zissis and D.Lekkas,"Addressing cloud computing security issues," Future Computer Systems, Vol.28, No.3,2012,pp. 583-592.
[7] A.N.Khan, M.L.M. Kiah, S.U.Khan, and S.Madani, "Towards Secure Mobile computing: A survey," Future Generation Computer Systems, Vol.29,No. 5,2013,pp. 1278-1299.
[8] T.Loukopoulos and i.Ahmad, "Static and adaptive distributed data replication using genetic algorithms," Journal of parallel and Distributed Computing, vol. 64, No. 11.2004,pp,1270-1285.
[9] 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, okland CA, PP.110-121.1991.

