IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Fragmentation of Data for Security in Cloud Services

S.Daniel[1*], P. Azeem ul haq[2], S. Sureshkrishnan[3]

[1,2,3] Dept. of Computer Science and engineering, Government College of engineering, Tirunelveli, India

[*]*Corresponding Author: kewindaniel460@gmail.com Tel.: +91-8012254197*

DOI: https://doi.org/10.26438/ijcse/v7i4.468472 | Available online at: www.ijcseonline.org

Accepted: 09/Apr/2019, Published: 30/Apr/2019

***Abstract*—**The data compromise could occur thanks to attacks by different users and nodes inside the cloud. Therefore, high security measures square measure needed to safeguard knowledge inside the cloud. However, the utilized security strategy should additionally take into consideration the improvement of the information retrieval time. In our proposed system propose the Division and Replication of Data in the Cloud for Optimal Performance and Security with NTRU Algorithm that for file storage and data security. In this system consist of two phase they are NTRU Encryption method and FDSCS methodology. In this methodology, we tend to divide a file into fragments, and replicate the fragmented knowledge over the cloud nodes. Each fragment is encrypted by NTRU Encryption Algorithm. Each of the nodes stores solely one fragment of a selected record that ensures that even just in case of an eminent attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments square measure separated with bound distance by means that of graph T-coloring to ban associate assaulter of dead reckoning the locations of the fragments. Finally our Experimental result shows our proposed method ensures complete security of the data, reduce the data overhead and reduction the encryption and decryption time.

***Keywords*—** Fragmentation, NTRU algorithm, T-coloring, cloud security, optimization

I. INTRODUCTION

Cloud computing may be a paradigm of computing, a replacement Manner of wondering IT business however not any specific technology. A Cloud may be a style of parallel and distributed system consisting of a set of interconnected and virtualized computers that square measure dynamically provision and given in concert or additional unified computing resources supported service-level agreements established through negotiation between the service supplier and shoppers.

Cloud computing and storage provides users with capabilities to store and method their knowledge in third-party knowledge centres. Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, Public, hybrid, and community). Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (Organizations providing software-, platform or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their client's data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud security

Alliance report, insider attacks are the sixth biggest threat in cloud computing. Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, cloud service providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

II. RELATED WORK

It ensures logical thinking of servers of differential acquisition. In short it formulate the source domain to object domain. In this proposed model the formal data patterns are protested in steps of fragmentation. So the intrusion action of every single set of data is encrypted. Though cloud servers

perform grid pattern. The data of each cloud patterns are insisted to a server of action. In somehow the intruder comprises the node of action. In some how the existing proposed systems doesn't posses the valuable source of retrieval time. In this we increase the resurrection time lapse so that the feasible time action is easily associated.

Servers posses a cloud layers segment so that that retrieval of data can be easily capable so in this theory we use a special case of encryption known as NTRU so that the retrieval are can't be easily function able because the data uploading packages posses a authorized form of information. This methodology utilizes the concept of data fragmentation for securing the user data. To improve the retrieval time of fragments the fragments are stored in central nodes this increases the data security and high level of security performance.

III. NEED OF STUDY

It ensures conceptual action of high level of security it posses logical growth drive of cloud possession it formulates high functional performance of security of intrusion it visualizes each thread of action in a frequent time of initialization it posses benefits of low cost, negligible management and greater flexibility with increased security concerns

It posses striking candidate for business, organization and individual users for adoption

IV. METHODOLOGY

1. Registration:

At first all the data holder is register our details in the organization. After registration the data holder can upload the data to the cloud. The authorized user can be downloading or view the encrypted File. If the user want upload the file then at first the user can login our id. Login is success then enters into the Data holder page.

2. Data Uploading:

After Login the Data holder then upload the data into the cloud by sending the uploading file with request to the cloud server.

3. FDSCS:

FDSCS methodology utilizes the concept of data fragmentation for securing the user data within the cloud. To further enhance the security, the fragments are not stored on the adjacent nodes. To separate the storage of fragments by certain distance, the concept of T-coloring is used. To improve the retrieval time of fragments, the fragments are stored on the most central nodes. The selection of central nodes is carried out by evaluating the centrality measures for the nodes.

3.1. Data fragmentation:

Let us take into account a cloud with M nodes and a file with z range of fragments. Let's be the amount of booming intrusions on distinct nodes, such that s>z.

The likelihood that s range of victim nodes contains all of the z sites storing the file fragments. The FDSCS methodology fragments the file and makes use of the cloud for replication. The fragments square measure distributed such no node during a cloud holds quite one fragment, so that even a successful attack on the node leaks no significant information. The FDSCS methodology uses controlled replication Wherever every of the fragments is replicated one time within the cloud to boost the protection. In the FDSCS methodology, user sends the data file to cloud. The cloud manager system (a user facing server in the cloud that entertains user's requests) upon receiving the file performs: (a) fragmentation, (b) first cycle of nodes selection and stores one fragment over every of the chosen node, and (c) second cycle of nodes selection for fragments replication. The cloud manager keeps record of the fragment placement and is assumed to be a secure entity. Once the file is split into fragments, the FDSCS methodology selects the cloud nodes for fragment placement. The selection is formed by keeping AN equal specialize in each security and performance in terms of the time interval. We choose the nodes that square measure most central to the cloud network to produce higher time interval. For the said purpose, the FDSCS methodology uses the thought of spatial relation to scale back time interval.

3.2Centralities Calculation:

FDSCS with three centrality measures, namely: (a) betweenness, (b) closeness, and (c) eccentricity centrality. However, if all of the fragments are placed on the nodes based on the descending order of centrality, then there is a possibility that adjacent nodes are selected for fragment placement.

$$C(v)= \frac{N-1}{\sum d(v,a)}$$

Where N is total number of nodes in a network and d(v, a) represents the distance between node v and node a.

3.3. T-coloring:

Such a placement can provide clues to an attacker as to where other fragments might be present, reducing the security level of the data. To deal with the security aspects of placing fragments, we use the concept of T-coloring that was originally used for the channel assignment problem. We generate a non-negative random number and build the set T starting from zero to the generated random number. The set T is used to restrict the node selection to those nodes that are at hop-distances not belonging to T. For the said purpose, we

assign colors to the nodes, such that, initially, all of the nodes are given the open color. Once a fragment is placed on the node, all of the nodes within the neighbourhood at a distance belonging to T are assigned close colour. In the aforesaid process, we lose some of the central nodes that may increase the retrieval time but we achieve a higher security level.

4. Data Downloading:

To handle the transfer request from user, the cloud manager collects all the fragments from the nodes and re-assembles them into one file. Afterwards, the file is sent to theuser.3.Encryption Module (NTRU Method): Before placing the fragment of data into the storage node, NTRU encryption scheme executed. It consists of key generation, Data encryption and Decryption.

• KeyGen()→ (pk, sk): let f ∈ R, g ∈ R, while f, g follows the discrete Gaussian distribution, f = 1 mod q, and f is reversible. Thus, the secret key is denoted by sk = f; the public key is denoted by pk = h = g • f−1 mod q.

• Enc(pk = h, μ ∈ Rp)→ c ∈ Rq: let r ∈ R,m ∈ R,m = μ mod p. Both m′ and r follow the discrete Gaussian distribution, and we have m = p • m′ + μ, c = p • r • h + m mod q.

• Dec(sk = f, c ∈ Rq) → μ: calculate _b = f • c mod q, and make it an integer polynomial bewitch factors within [−q/2, q/2). Thus, we have μ = b mod p. After Encrypted data, the data will be placed in the storage node.

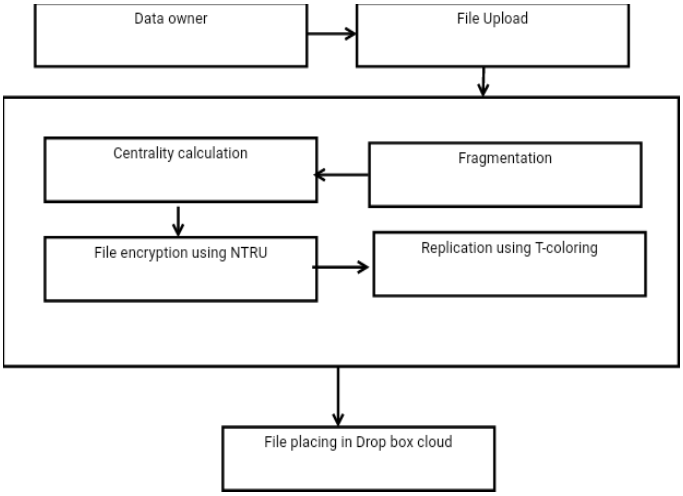

Fig:1 Function Architecture

5. System implementation:

User to uploading the input file to cloud server and then file will fragmented in several part and then encrypted by using NTRU Algorithm and store to cloud in different server nodes.

Admin can view the available space of server details. Once server is available it will be indicate the open color. Server is not available it will be indicate the close color

Admin can view the user details and then CSP (cloud service provider) is the major role for allocating the service store the cloud server. User and Admin interaction between works will be maintain by the cloud service provider. Then store and download the data secure in cloud environment.

V. RESULTS AND DISCUSSION

RC versus number of nodes for FDSCS variations with maximum available capacity constraints

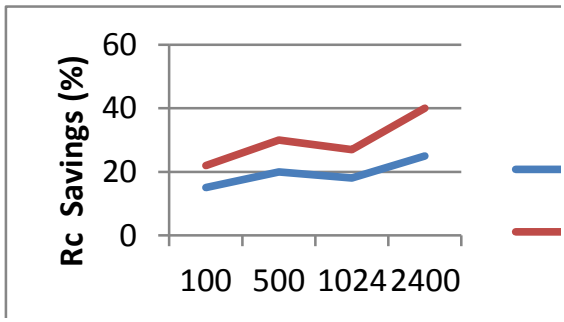

Fig: 2 comparison of capacity

The read/write (R/W) ratio for the simulations that used fixed value was selected to be 0:25 (The R/W ratio reflecting 25% reads and 75% writes within the cloud). The reason for choosing a high workload (lower percentage of reads and higher percentage of writes) was to evaluate the performance of the techniques under extreme cases. The simulations that studied the impact of change in the R/W ratio used various workloads in terms of R/W ratios. The R/W ratios selected were in the range of 0:10 to 0:90. The selected range covered the effect of high, medium, and low workloads with respect to the R/W ratio. In this graph compare the maximum available capacity constraints with existing and proposed system. Finally our proposes work give best result.

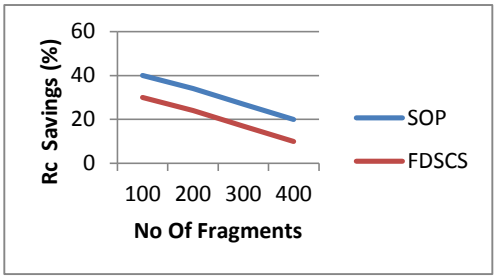

Fig: 3 comparison of fragment

The increase in number of file fragments can strain the storage capacity of the cloud that, in turn may affect the

selection of the nodes. To study the impact on performance due to increase in number of file fragments, we set the number of nodes to 30,000. The numbers of file fragments selected were 50, 100, 200, 300, 400, and 500. The workload was generated with C = 45% to observe the effect of increase number of file fragments with fairly reasonable amount of memory and to discern the performance of all the algorithms. It can be observed from the plots that the increase in the number of file fragments reduced the performance of the algorithms, in general. However, the greedy algorithm showed the most improved performance.

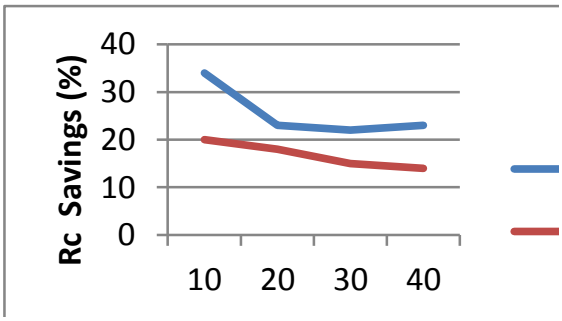

Fig: 4 comparison of ratio

It shows the performance of the comparative techniques and the FDSCS methodology under varying R/W ratios. It is observed that all of the comparative techniques showed an increase in the RC savings up to the R/W ratio of 0:40. The decrease in the number of writes caused the reduction of cost associated with updating the replicas of the fragments. However, all of the comparative techniques showed some sort of decrease in RC saving for R/W ratios above 0:40. This may be attributed to the fact that an increase in the number of reads caused more replicas of fragments resulting in increased cost of updating the replicas. Therefore, the increased cost of updating replicas underpins the advantage of decreased cost of reading with higher number of replicas at R/W ratio above 0:40.

VI. CONCLUSION AND FUTURE SCOPE

The proposed the FDSCS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time.

The data file was fragmented and also the fragments area unit distributed over multiple nodes. The nodes were separated by means of T-coloring. The fragmentation Associate in Nursing dissemination ensured that no vital info was procurable by an individual just in case of a self-made attack. No node within the cloud, stored more than a single fragment of the same file. The performance of the FDSCS methodology was compared with complete replication techniques. NTRU Encryption Reduce the key complexity.

FUTURE WORK

Currently with the FDSCS methodology, a user has to download the file, update the contents, and upload it again.
It is strategic to develop Associate in Nursing automatic update mechanism which will establish and update the desired fragments solely.

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] Sirisha Aguru, Batteri MadhavaRao, "Data Security In Cloud Computing Using *RC6* Encryption and Steganography Algorithms", International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.1, pp.6-9, 2019

[3] Poonam Devi , "Attacks on Cloud Data: A Big Security Issue", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.2, pp.15-18, 2018

[4] Mazhar Ali ; Kashif Bilal ;Samee U. Khan ;Bharadwaj Veeravalli ; Keqin Li ; Albert Y. Zomaya "FDSCS: Division And Replication Of Data In Cloud Foroptimal Performance And Security" Volume: 6 , Issue: 2 , April-June 1 2018

[5] 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.

[6] Y. Chen, V.Paxson, and R. H. Katz, "Whats new about cloud computing security," University of California, Berkeley Report No. UCB/EECS-2010-5, Jan. 20, 2010.

[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] 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.

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

[10] W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.

[11] 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.

[12] 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 of Supercomputing, Vol. 66, No. 3, 2013, pp. 1687-1706 .

Author's Profile

Mr.S.Daniel pursed Bachelor of Computer Science and engineering from government college of engineering, Tirunelveli in 2019.I have done my project based on cloud security.In generally I have quite interesting in

networking and system management.
He attend the NPTEL Course and finish the course.he participating the many workshop and paper presentation in many colleges. He attend the training in uniq technologies in 2017.He attend the international conferences. His main research work focuses on Network Security, Cloud Security and Privacy.

Mr.P.Azeem ul haq pursed Bachelor of Computer Science and engineering from government college of engineering, Tirunelveli in 2019.I have done my project based on cloud security.In generally he have quite interest in networking and system management.

He participating the many workshop and paper presentation in many colleges.
He attend the training in uniq technologies in 2017 He have provisional knowledge in hardware and computer management.He attend the international conferences. His main research work focuses on Network Security, Cloud Security and Privacy.

Mr.Sureshkrishnan pursed Bachelor of Computer Science and engineering from government college of engineering, Tirunelveli in 2019.I have done my project based on cloud security.In generally he have quite interest in networking and system management.
He have provisional knowledge in hardware and computer management.He attend the international conferences. His main research work focuses on Network Security, Cloud Security and Privacy

