www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 6 June 2016, Page No. 16836-16841

An Optimization And Security Of Data Replication In Cloud Using Advanced Encryption Algorithm

S.Suganya[1], *R.Kalaiselvan*[2]

[1]M.E. Student, Department of CSE, Parisutham Institute of Technology and Science, Tamil Nadu, India
[2]Asst. Professor, Department of CSE, Parisutham Institute of Technology and Science, Tamil Nadu, India
[1]sugan.suga2@gmail.com,[2]rk.kalai@gmail.com

Abstract- **Cloud computing is an emerging pattern that provides computing, communication and storage resources as a service over a network. In existing system, data outsourced in a cloud is unsafe due to the eaves dropping and hacking process. And it allows minimizing the security network delays in cloud computing. In this paper to study data replication in cloud computing data centers. Unlike another approaches available in the literature, consider both security and privacy preserving in the cloud computing. To overcome the above problem we use DROPS methodology. The data encrypted using AES (Advanced Encryption Standard Algorithm). In this process, the common data are divided into multiple nodes also replicate the fragmented data over the cloud nodes. Each data is stored in a different node in fragments individual locations. We ensure a controlled replication of the file fragments, here each of the fragments is replicated only once for the purpose of improved security. The results of the simulations revealed that the simultaneous focus on the security and performance, resulted in improved security level of data accompanied by a slight performance drop.**

Keywords:Fragmentation, Replication, Performance.

I.INTRODUCTION

In Cloud Computing, Database Replication is the frequent electronic copying of data from a database in one computer or server to a database in another so that all users share the same level of information. The result is a distributed database in which users can access data relevant to their tasks without interfering with the work of others. On thepractical side, data replication plays a key role in a wide range of contexts like caching, back-up, high availability, wide area content distribution, increasing scalability, parallel processing, etc. Finding a replication solution that is suitable in as many such contexts as possible remains an open challenge. Data replication has been widely used to improve the performance of data access in traditional wireless networks. With data replication, users can access the data without the support of network infrastructure, and can reduce the traffic load. The replication mechanism determines which file should be replicated, when to create new replicas and where the new replicas should be placed. Replication methods can be classified as static and dynamic. Replication components can therefore be subjected to realistic large scale loads in a variety of scenarios, including fault injection, while at the same time providing global observation and control. Replication is a cost effective way to increase availability and used for both performance and fault tolerant purposes thereby introducing a constant trade-off between consistency and efficiency. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information.

The data outsourced to a public cloud must be secured. Unauthorized data access by other users and processes (whether accidental or deliberate) must be prevented [14]. As discussed above, any weak entity can put the whole cloud at risk. In such a scenario, the security mechanism must substantially increase an attacker’s effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud. Moreover, the probable amount of loss (as a result of data leakage) must also be minimized.

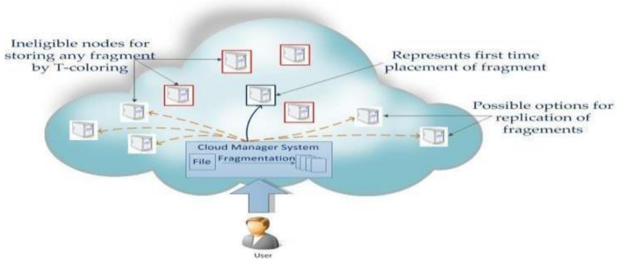
II.PROBLEM STATEMENT

The off-site data storage cloud utility requires users to move data in cloud’s virtualized and shared environment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physical resources to be shared among many users. The data outsourced to a public cloud must be secured.

DOI: 10.18535/ijecs/v5i6.19

Unauthorized data access by other users and processes must be prevented.

The security mechanism must substantially increase an attacker’s effort to retrieve a reasonable amount of data even after a successful intrusion in the cloud. A difficulty that arises immediately is that some sites holding a copy of the object might be unavailable. Data replication is that an update to any given logical object must be propagated to all stored copies.


Ineligible nodes for storing any fragment by T-coloring
Represents first time placement of fragment
Possible options for replication of fragements
Cloud Manager System
File
Fragmentation
User

III.PROPOSED SYSTEM

The scheme for outsourced data that takes into account both the security, performance and replicates the data file over cloud nodes. The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. The DROPS methodology fragments the file and makes use of the cloud for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even a successful attack on the node leaks no significant information.AES (Advanced Encryption technique) on traditional encryption techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations on the data. Deduplication has an important role in many applications such as in cloud storage.

Increasing the cloud computing performance. Storage systems have become more efficient and can now do offsite, cloud-based backup and replication. Reduce capital computational costs. High-speed, reliable network connectivity so that replication can be handled quickly and efficiently on a wide-area network. Improve secure accessibility.

3.1.CLOUD REGISTRATION FOR DATA STORAGE

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third- party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility over a network. In this module the user has to register by entering personal details and create his/her User Id and Password. Based on the User Id and Password, the user has to login and enter into the system. And the cloud Access provides comprehensive security-as-a-service from the cloud. We integrate multiple security assets to identity predictive anomalous behavior during access.

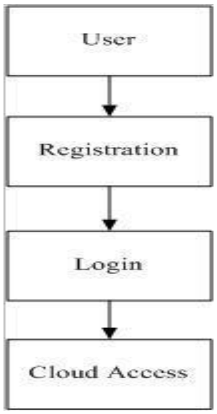


Figure.1Cloud Registrations for Data Storage

3.2. ENCRYPTION USING AES (ADVANCED ENCRYPTION STANDARD ALGORITHM)

Cloud is used for store the data privately in secure protected server. In cloud, the database access anywhere through internet. Data is unsafe in the cloud, the eaves dropper hacks the data. To avoid the data leakage and to prevention the data to use encryption process. In this AES (Advanced Encryption standard) is used for Encrypt the data. The encrypting time of traditional AES algorithm is a fast encryption algorithm. For this point, the high- performance computing capability of secure in a cloud computing process.

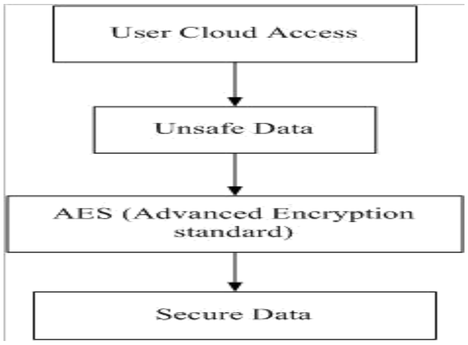


Figure.2 Encryption using AES

3.3.SYSTEM ARCHITECTURE

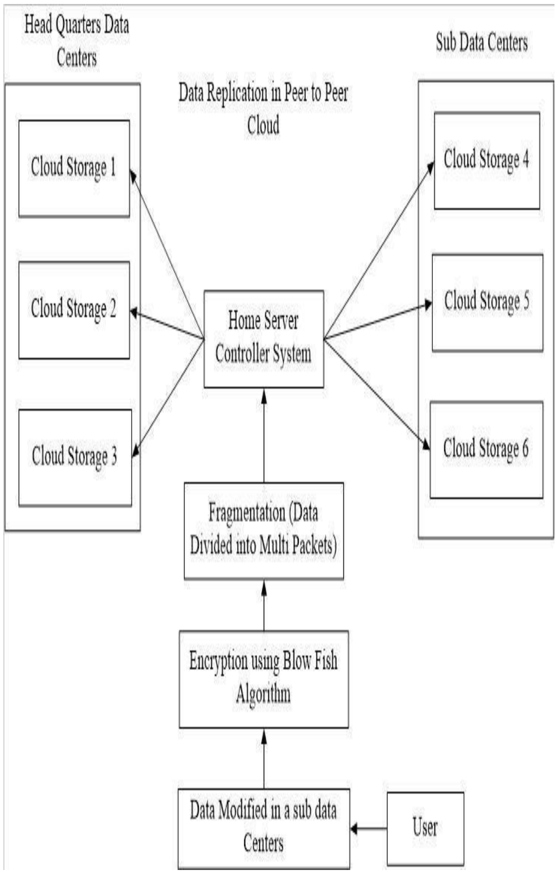

Head Quarters Data Centers
Sub Data Centers
Data Replication in Peer to Peer Cloud
Cloud Storage 1
Cloud Storage 2
Cloud Storage 3
Cloud Storage 4
Cloud Storage 5
Cloud Storage 6
Home Server Controller System
Fragmentation (Data Divided into Multi Packets)
Encryption using Blow Fish Algorithm
Data Modified in a sub data Centers
User

Figure.3 System Architecture

3.4.METHODOLOGY AES

ALGORITHM

Advanced Encryption Standard (AES) is a Symmetric key cryptography and it is an iterated block cipher with a fixed block size of 128 bit and a variable key length, it may be 128, 192 or 256 bits. The different transformations operate on the intermediate results, called state. The state is a rectangular array of bytes and since the block size is 128 bits, which is 16 bytes, the rectangular array is of dimensions 4x4. The cipher key is similarly pictured as a rectangular array with four rows. AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds.

BLOWFISH ENCRYPTION ALGORITHM

Blowfish is a symmetric block encryption algorithm designed in consideration with,

Fast: It encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte.

Compact: It can run in less than 5K of memory.

Simple: It uses addition, XOR, lookup table with 32- bit operands.

Secure: The key length is variable ,it can be in the range of 32~448 bits: default 128 bits key length.

It is suitable for applications where the key does not change often, like communication link or an automatic file encryptor. Unpatented and royality- free.

Algorithm: Blowfish Encryption

```
        Divide x into two 32-bit halves: xL, xR

For i = 1to 16:

xL = XL XOR Pi
xR  =  F(XL)  XOR
xR   Swap   XL   and
xR
  Swap XL and xR (Undo the last swap.)

  xR = xR XOR P17 xL

  = xL XOR P18

  Recombine xL and xR
```

AES has proven reliable. The only successful attacks against it, have been side-channel attacks on weaknesses found in the implementation.
or key management of certain AES-based encryption products. (Side-channel attacks don't use brute force or theoretical weaknesses to break a cipher, but rather

exploit flaws in the way it has been implemented.) Key to use AES to encrypt data, but due to the information that key exposes, attackers managed to predict the initialization vector block used at the start of the encryption process.

Various researchers have published attacks against reduced-round versions of the Advanced Encryption Standard, and demonstrated that using a technique called a biclique attack could recover AES keys faster than a brute-force attack by a factor of between three and five, depending on the cipher version. Even this attack, though, does not threaten the practical use of AES due to its low computational process.

IV.WORKLOAD

The size of files were generated using a uniform distribution between 10Kb and 60 Kb. The primary nodes were randomly selected for replication algorithms. For the DROPS methodology, the S^{i} ′s selected during the first cycle of the nodes selection by Algorithm 1 were considered as the primary nodes.The capacity of a node was generated using a uniform distribution between ($^{1}{}_{2}$ CS)C and ($^{3}{}_{2}$ CS)C, where $0 \leq C \geq 1$. For instance, for CS = 150 and C=0:6 the capacities of the nodes were uniformly distributed between 45 and 135. The mean value of g in the OPEN and FOCAL lists was selected as the value of , for WA-star and A -star, respectively. The value for level R was set to $^{d}{}_{2}$, where d is the depthof the search tree(number of fragments).

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 use 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.

V.EXPERIMENTAL SETUP AND RESULTS

The communicational backbone of cloud computing is the Data Center Network (DCN) [2]. In this paper, we use three DCN architectures namely: **(a)** Three tier, **(b)** Fat tree, and **(c)** DCell [1]. The Three tier is the legacy DCN architecture. However, to meet the growing de-mands of the cloud computing, the Fat tree and Dcell architectures were proposed [2]. Therefore, we use the aforementioned three architectures to evaluate the performance of our scheme on legacy as well as state of the art architectures. The Fat tree and Three tier architectures are switch-centric networks. The nodes are connected with the access layer switches. Multiple access layer switches are connected using aggregate layer switches. Core layers switches interconnect the aggregate layer switches.. The Dcell is a server centric network architecture that uses servers in addition to switches to perform the communication process within the network [1]. A server in the Dcell architecture is connected to other servers and a switch. The lower level dcells recursively build the higher level dcells. The dcells at the same level are fully connected. For details about the aforesaid architectures and their performance analysis, the readers are encouraged to read [1] and [2].

VI.IMPACT OF INCREASE IN THE READ/WRITE RATIO

The change in R/W ratio affects the performance of the discussed comparative techniques. An increase in the number of reads would lead to a need of more replicas of the fragments in the cloud. The increased number of replicas decreases the communication cost associated with the reading of fragments. However, the increased number of writes demands that the replicas be placed closer to the primary node. The presence of replicas closer to the primary node results in decreased RC associated with updating replicas.The higher write ratios may increase the traffic on the network for updating the replicas.

The performance of the comparative techniques and the DROPS methodology under varying R/W ratios. It is ob-served that all of the comparative techniques showed an increase in the RC savings up to the R/W ratio of 0:50. 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 0:50. 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 de-creased cost

of reading with higher number of replicas at R/W ratio above 0:50. It is also important to men-tion that even at higher R/W ratio values the DRPA-star, WA- star, A -star, and Greedy algorithms almost maintained their initial RC saving values. The high performance of the aforesaid algorithms is due to the fact that these algorithms focus on the global RC value while replicating the fragments. Therefore, the global perception of these algorithms resulted in high performance. Alternatively, LMM and GMM did not show substantial performance due to their local RC view while assigning a fragment to a node. The SA1, SA2, and SA3 suffered due to their restricted search tree that probably ignored some globally high performing nodes during expansion. The DROPS methodology maintained almost consistent performance as is ob-servable from the plots. Thereason for this is that the DROPS methodology replicates the fragments only once, so varying R/W ratios did not affect the results considerably. However, the slight changes in the RC value are observed. This might be due to the reason that different nodes generate high cost for R/W of fragments with different R/W ratio.

As discussed earlier, the comparative techniques focus on the performance and try to reduce the RC as much as possible. The DROPS methodology, on the other hand, is proposed to collectively approach the security and performance. To increase the security level of the data, the DROPS methodology sacrifices the performance to certain extent. Therefore, we see a drop in the performance of the DROPS methodology as compared to discussed comparative techniques. However, the drop in performance is accompanied by much needed increase in security level.

Moreover, it is noteworthy that the difference in performance level of the DROPS methodology and the comparative techniques is least with the reduced storage capacity of the nodes (see Fig. 6 (b), Fig. 7 (a), and Fig. 7 (b)). The reduced storage capacity pro- scribes the comparative techniques to place as many replicas as required for the optimized performance. A further reduction in the storage capacity will tend to even lower the performance of the comparative tech- niques. Therefore, we conclude that the difference in performance level of the DROPS methodology and the comparative techniques is least when the comparative techniques reduce the extensiveness of replication for any reason.A cloud stor-age security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were sepa-rated by means of T-coloring. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, stored more than a single fragment of the same file. The performance of the DROPS methodology was compared with full-scale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance, resulted in increased security level of data accompanied by a slight performance drop.

VII.CONCLUSION

In cloud computing, proposed an efficient Data Replication Model for Cloud Computing based on Frequent Pattern Mining. The Data Replication in Cloud Computing requires an in-depth analysis because it is necessary to provide complete access to the users in cloud systems with less time access. The data replication process can ease out the access process of any kind of data without making delay. In proposed method, utilized the frequent algorithm (AES) which proved to be a better mechanism to provide efficient replication process to the cloud system. The results obtain shows that our proposed method has better results when compared with the existing methods of data replication in cloud computing.

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 andComputation: 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 comput-ing,” Journal of Internet Services and Applications, Vol. 4, No. 1, 2013, pp. 1-13.

DOI: 10.18535/ijecs/v5i6.19

[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

[10] International Conference onSystem Sciences (HICSS), 2011, pp. 1-10. 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 Filesys-tems,” University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[12] L. M. Kaufman, “Data security in the world of cloud comput-ing,” IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[13] S. U. Khan, and I. Ahmad, “Comparison and analysis of ten stati heuristics-based Internet data replication techniques,” Journal of Parallel and Distributed Computing, Vol. 68, No. 2, 2008, pp. 113-136.

[14] N. Khan, M. L. M. Kiah, S. U. Khan, and S.
Madani, “Towards Secure Mobile Cloud Computing: A Survey,” Future Generation Computer Systems, Vol.29, No. 5, 2013, pp. 1278-1299.

[15] N. Khan, M.L. M. Kiah, S. A. Madani, and
Ali, “En-hanced 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 .