International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195358

Efficient Cloud Storage with Data Partitioning and Replication Using Advanced Encryption Standard

Abirami. S, Shanmuga Priya. P
Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India

ABSTRACT

Cloud computing associate the computing and storage resources controlled by different operating systems to make available services such as large-scaled data storage and high performance computing to users. The benefits of low-cost, negligible management (from a user's perspective), and greater flexibility come with increased security concerns is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. The data outsourced to a public cloud must need to be secured. This work gives Division and Replication of Data (DROPs) inside the Cloud for Optimal Performance and Security that judicially fragments user files into portions and replicates them at strategic places in the cloud. The division of a files into fragments is achieved based on a given consumer standards such that the individual fragments do not comprise any meaningful facts. The node separation is ensured by the means of the Grid Topology algorithm. To further improve the retrieval time, replicate fragments over the nodes that generate the highest read/write requests. The data encrypted using AES encryption algorithm. Duplication checking is implementing to provide efficient storage and time based access control for secure file access system.

Keywords : File Splitting, Replication, Graph Topology, AES Encryption, Duplicate Checking.

I. INTRODUCTION

The word "cloud" has been used to say to structures for distributed computing. Cloud Computing is a form of internet-primarily based computing which gives dynamic resources, virtualization, flexibility, scalability to users. [3] The aim of cloud computing is to reduce down the price and allow customers to take advantage from all of the offerings supplied via the cloud and allows them to awareness on their core enterprise. Cloud computing is closely related to Grid computing however specific from it. Cloud computing associates the computing and garage assets managed by way of exclusive working systems to make to be had offerings inclusive of huge-scaled information storage and high performance computing to customers. Circulation of data is in a extraordinary way of cloud computing, evaluating with the grid computing. Nowadays, companies and groups are shifting and spreading their enterprise by way of accepting the cloud computing to decrease their price. In the cloud computing surroundings, clients of cloud offerings do no longer need whatever approach not going into element about the implementation and they could get entry to their records and complete their computing obligations only by using the Internet connection. Throughout the get entry to the facts and computing, the clients do no longer even recognize in which the facts are positioned away or the place of the facts. Thus, right here the safety difficulty stands up unexpectedly. Data security inside the cloud computing is greater complicated than facts security inside the conventional records structures.

The advantages of the cloud garage are bendy with decreased price and in addition they manage the information loss risk and so on. Recently many cloud approaches focus in the direction of third party auditing and the file integrity checking, providing the data dynamics. Remote archive provider is liable for properly maintaining the data. The remote data integrity checking protocol detects the information corruption and misbehaving server inside the cloud storage.

In proposed method, Enhancing cloud Security with the aid of Fragmenting and replicating records that fragments consumer's documents into portions and replicate them at algorithmically decided place inside cloud. To growth the overall performance blowfish algorithm is to implement. Also take care that a successful attack on a single node will not reveal the locations of fragments in file sequence within the cloud. To keep the attacker unknown about the location of the file fragments and further enhance security, select nodes in such a manner that they are not adjacent and are at certain distance from each other. Also use Graph Topology Grid algorithm for node separation.

The objectives of the paper are

1. To design a device so that it will provide better authentication system this avoids legal users to enter.
2. To improve the security concerns with usage of blowfish encryption.
3. To offer controlled replication to increase the performance.
4. To provide time oriented access permission to control for secure data sharing with users.

II. BACKGROUND WORK

The limitation of existing mechanism was, that takes much more time and cost to perform the dynamic processing of data encryption and decryption techniques to store data in cloud with security. The proposed approach of Data Partition and Replication Technique overcomes such limitations with high performance, reduced cost and limited data storage space in cloud. It also ensures resilient against threads, attacks and misbehaving server.

DROPs methodology is a new field of research in information security in cloud environment. This will provide more secure file storage compared to existing encryption system. In DROPs methodology Division and Replication are perform to protect data security and also consider the data retrieval process. Efficient encryption technique applied to encrypt the fragmented files. This proposed approach considers three parts that are Data Owner, Cloud Service Provider and Data User.

III. IMPLEMENTATION

AES Encryption

The AES cipher is also referred to as the block cipher. No a success attack has been mentioned on AES. Some advantages of AES are easy to enforce on 8-bit structure processors and powerful implementation on 32-bit architecture processors. AES encryption is accomplished in more than one rounds. Each round has 4 important steps along with sub-byte, shift row, mix column and add round key. Sub-byte is the substitution of bytes using look-up table. Shift row is the transferring of rows according to byte length. Mix column is multiplication over Galois field matrix. Finally, within the upload spherical key step, the output matrix of mix column is XORed with the round key. The wide variety of rounds used for encryption relies upon on the important thing size. For a 128-bit key, these 4 steps are implemented to nine rounds, in which the 10th round does no longer consider the mixture column step. Since all steps are recursive, decryption is the opposite of encryption.

Algorithm Procedure

The set of rules starts with an Add round key degree observed by using 9 rounds of 4 levels and a tenth round of three stages. This applies for both encryption and decryption with the exception that every degree of round the decryption set of rules is the inverse of its counterpart within the encryption algorithm. The four degrees are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The 10th round definitely leaves out the Mix Columns stage. The first 9 rounds of the decryption algorithm consist of the subsequent:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the 10th round simply leaves out the Inverse Mix Columns level. Each of these stages will now be considered in greater element.

GRAPH TOPOLOGY GRID

Step 1: Submit jobs to grid.

Step 2: Every request sent to Replica manager of Regional servers.

Step 3: Replica manager query Replica Catalog to determine which grid site contains the desired replica (Candidate sites).

Step 4: If the file not found in lower level its Manager send Request to upper level.

Step 5: Determine the communication cost between requester site and candidate sites.

Step 6: Compute the Round Trip Time (RTT).

Step 7: If (d>RTT) then access the file from the remote place or else replicate.

Step 8: Check the storage element of the site selected for replication. If no storage space available request the Replica Replacement algorithm, otherwise

Step 9: The Threshold Controller checks whether the site has minimum access load, if yes, it communicates with Reservation Manager.

Step 10: If Reservation Manager succeeds in making reservations, Allocation Manager is called to allocate resources.

Step 11: Once Allocation Manager allocated resources, Replication Placement is performed.

Step 12: If Reservation Manager is not succeeded, then the Lowest Common Ancestor algorithm (LCA) is invoked.

Step 13: LCA returns a site, with this site ID, repeat steps 8 and 9.

Step 14: If the Threshold Controller results maximum access load, choose one of the sibling node and continue step 10 and 11.

CHUNK BASED SIMILARITY CHECKING

Input: a chunk data list of super-chunk S, {fp1, fp2, … , fpn}

Output: a target node ID, i

1. Select the k data chunk {rfp1, rfp2, …, rfpk} and sent the chunk to candidate nodes with IDs {rfp1 mod N, rfp2 mod N, …, rfpk mod N} in the deduplicaton server cluster with N nodes;
2. In deduplication server cluster, obtain the count of the existing representative data chunk of the super-chunk in the candidate nodes by comparing the representative data chunks of the previously stored super-chunks in the similarity index. Index comparison was performed using Map-Reduce framework. The returned k count values, one for each of the k candidate nodes, are denoted as {r1, r2, …, rk}, which are directly corresponding to the resemblances of S in these nodes;
3. Mapper find the duplicate content then reducer eliminates the redundant content.

4. Choose the deduplication server node with ID i that satisfies ri/wi = max{r1/w1, r2/w2, …, rk/wk} as the target node.

PROCEDURE

- Cloud Framework
- File Fragmentation
- AES Encryption
- Replication
- Time based Access Control
- File Retrieval

Cloud Framework

Cloud framework consists of cloud service provider, Data owner and Data user. Cloud service provider provides secure storage for data. CSP take handles of file encryption, fragmentation and replication. When data owner wants to send file on cloud server first the user should register. If all credentials are valid then only the user can send file in cloud. Data user makes use of data present the cloud environment. User should also register and get permission to access the data from cloud.

File Fragmentation

To gain reliability, performance, balanced storage capacity and security, fragmentation plays a vital role. Fragmentation is a process which partitioning every sensitive file into several fragments in such a way that it is impossible to achieve total file in one try. Once the file is stored in cloud, the file will get encrypted. Then, cloud manager will start fragmentation with the help of fragmentation engine. Based on the fragmentation threshold value, the file will get fragmented into number of pieces. Then it will be stored in cloud nodes using allocation techniques. After fragmentation, the primary node will be determined and it gets stored initially. Then, all the remaining k^{th} fragments will be placed in remaining available nodes. File splitting is used to minimize the total data transfer cost. The probabilities of finding each splited document are also very low. Fragmentation is divided into three type namely horizontal, vertical and mixed fragmentation.

AES Encryption

Encryption is a famous technique that performs a data protection role from intruders. AES algorithm makes use of a specific structure to encrypt data to offer the high safety. To do this it is based on number of rounds and inner every round incorporates of 4 sub-systems. The AES encryption set of rules defines some of transformations which can be to be performed on data saved in an array. The first step of the cipher is to put the statistics into an array; and then the cipher changes are repeated over a number of encryption rounds. The number of rounds is decided based on key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

Replication

Data replication method keeping a number of replicas at the same server or on assorted servers. In replication information is copied and distributed from one database to some other. So, it reduces the workload from the authentic server and the statistics on the server wherein it's miles copied are always which is not present in mirroring technique. Replication decreases the chance of statistics loss, increase the performance, availability and reliability. Replication will increase the variety of record copies in the cloud. Thereby, increasing the opportunity of the node protecting the file to be a sufferer of assault. Replication and Security ought to be balanced in order that any one service not lower the opposite.

Time based Access Control

The owner encrypts message for the purpose that intended users can decrypt it after a designated time. User sends the file request to the corresponding data

owner. Data owner set the time for accessing the data. The encrypted ciphertext holds the feature that only with the corresponding user's secret key and time token. The permitted accessing time, together with user's attribute constraint set, determines whether the user satisfies the policy.

File Retrieval

The user can download files by entering a secret file key, then the entire splits file get merged and can be downloaded. With the access policy embedded in the ciphertext, a user can decrypt the ciphertext to access the data, only if his/her attribute set satisfies the policy, and the access time is later than the predefined releasing time.

IV. CONCLUSION

In proposed approach, secure data storage was implemented using division and replication system. The user has to register in cloud, for each registered user, access permission send from service provider. The user when wants to upload the file, it gets splits into small chunks and for every upload of file a secret file key is also generated when data user wants to download and access a file, they should enter a secret file key of their file, then splits chunks get merged and can download the file. This provides security in both client levels as well as in network level.

Future work focuses on secure file access with drops methodology. A time based access control mechanism will be implementing to provide access control to the data user. The above mentioned future work will save the time and resources utilized in downloading, updating, and uploading the file again.

V. 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 on System 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.

Cite this article as : Abirami. S, Shanmuga Priya. P, "Efficient Cloud Storage with Data Partitioning and Replication Using Advanced Encryption Standard", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 223-227, May-June 2019. Available at doi : https://doi.org/10.32628/CSEIT195358
Journal URL : http://ijsrcseit.com/CSEIT195358