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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Encrypted Division and Replication of Data Stored in Cloud

H.Aashika Parveen[1], A.Bhavani[1], D.Brindha[1], P.Haripriya[1], R.Sharanya[2]

U.G. Student, Department of Computer Engineering, Saranathan College of Engineering, Trichy, Tamilnadu, India[1]

Associate Professor, Department of Computer Engineering, Saranathan College of Engineering, Trichy, Tamilnadu, India[2]

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. Proposed approach presents 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 breaks into pieces is performed based on a given user criteria such that the individual pieces do not contain any meaningful information. The fragmented data encrypted using AES encryption algorithm. Like most any other cryptosystem AES is just a method of obscuring the relationship between the plain text and cipher text, diffusing this data, and making ensuring the cryptosystem cannot be cracked without a key. Proposed approach also focuses on secure file sharing with user's data. Time based access is implemented for improvised access control. Also it provides the authorization to file access, if any key mismatch occurs on file retrieval that sends an alert mail to the data owner.

KEYWORDS: Cloud Storage, Encryption, Fragmentation, Replication, Graph Topology

I. INTRODUCTION

Cloud computing is a promising model for business computing. It describes important infrastructure to have an upcoming type of service provision which includes the benefit of reducing expense by sharing computing and storage sources. Currently, Cloud Computing has become a huge technology that is exceeding all of the earlier technologies of computing in this competitive and demanding Information technology industry.

Cloud computing is consistently growing and there are many main cloud computing service providers including Amazon, Google, Microsoft, Yahoo and many others who are offering solutions including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a- Service and Infrastructure-as-a-Service (IaaS). In addition, considering the possibility to substantially minimize the expenses by optimization and also maximize operations as well as economic effectiveness. Furthermore, cloud computing can tremendously boost its cooperation, speed, and also range, thus empowering a totally worldwide computing model on the internet infrastructure. On top of that, the cloud computing has advantages in delivering additional scalability and fault tolerance services.

II. LITERATURE SURVEY

Authors: S.Suganya, R.Kalaiselvan

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. They integrate multiple security assets

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

to identity predictive anomalous behavior during access. 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.

III. THEORITICAL FRAMEWORK

EXISTING SYSTEM

The trusted third party is used for providing security services in the cloud. The authors used the public key infrastructure (PKI) to enhance the level of trust in the authentication, integrity, and confidentiality of data and the communication between the involved parties. The keys are generated and managed by the certification authorities. The trusted third party is responsible for the generation and management of public/private keys. The trusted third party can be a single server or multiple servers. The symmetric keys are protected by combining the public key cryptography and the (k, n) threshold secret sharing schemes. An encryption key is divided into n shares and distributed on different sites within the network. The division of a key into n shares is carried out through the (k, n) threshold secret sharing scheme. The network is divided into clusters. The number of replicas and their placement is determined through heuristics. A primary site is selected in each of the clusters that allocate the replicas within the cluster. The existing scheme combines the replication problem with security and access time improvement.

PROPOSED SYSTEM

In a cloud environment, a file in its totality, stored at a node may leads to a single point of failure. A successful attack on a node might put the data confidentiality or integrity, or both at risk. In the DROPS methodology, we proposed not to store the entire file at a single node. Rather we encrypted the file before fragmenting it and maked use of the cloud for replication. The fragmented files 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. In DROPS methodology, each of the fragments has replicated only once in the cloud to improve the security. In the DROPS 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 for storing one fragment over each of the selected node, and **(**c) second cycle of nodes selection is for fragments replication. This system uses fragmentation technique by using T-Coloring method. The cloud manager keeps recording of the fragment placement and is assumed to be a secure entity. AES encryption algorithm is to implement to provide secure data storage through encryption process.

ALGORITHM USED

Advanced Encryption Standard: with 10 rounds for 128-bit keys

Encryption is a popular technique that plays a major role to protect data from intruders. AES algorithm uses a unique structure to encrypt data to provide the best security. The algorithm begins with an **Add round key** stage after the completion of 9 rounds of four stages and a tenth round of three stages. This is applicable for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes: The 16 input bytes are substituted by looking up a fixed table S − box given in design. The resultant 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. Shift is carried out as follows –

- First row - no shift
- Second row - shift one byte position to the left.
- Third row - shift two positions to the left.
- Fourth row - shift three positions to the left.
- The resultant is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

3. Mix Columns: 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 resultant should be a new matrix consisting of 16 new bytes. It is important that this step should not be performed in the last round.

4. Add Round Key: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output of this round is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and repeat another similar round.

Decryption Process: The tenth round simply leaves out the **Mix Columns** stage. The first nine rounds of the decryption process consist of the following: Inverse Shift rows, Inverse Substitute bytes, Inverse Add Round Key and Inverse Mix Columns**.** Again, the tenth round simply leaves out the **Inverse Mix Columns** stage. Each of these stages will now be considered in more detail.

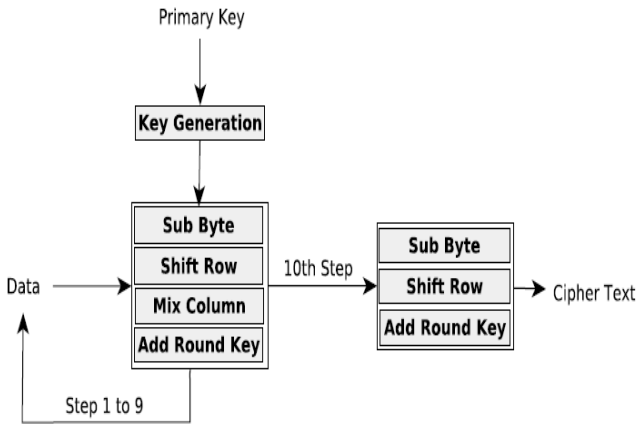

Fig 1. AES Algorithm for 128 bit key

GRAPH TOPOLOGY

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.
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 found invoke 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

IV. IMPLEMENTATION

Proposed system will be implementing using PHP for front end and MySQL for back end process. This approach has modules like Cloud Framework, AES Encryption, File Fragmentation, Replication, Time based Access Control and File Retrieval.

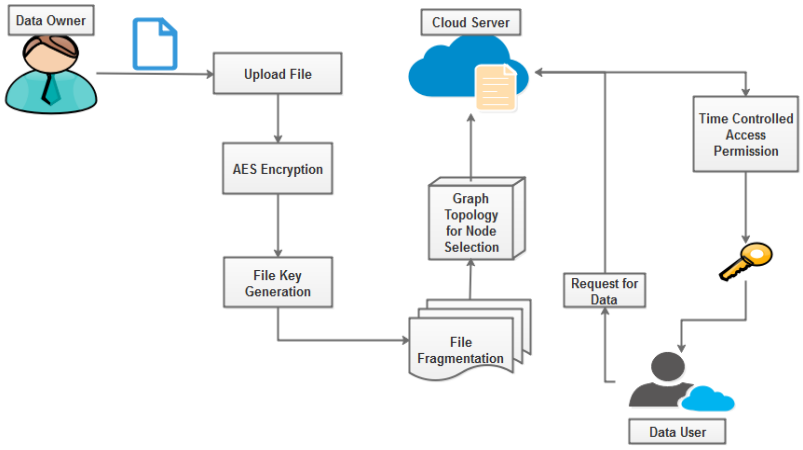

Fig 2.System Architecture

V. RESULTS

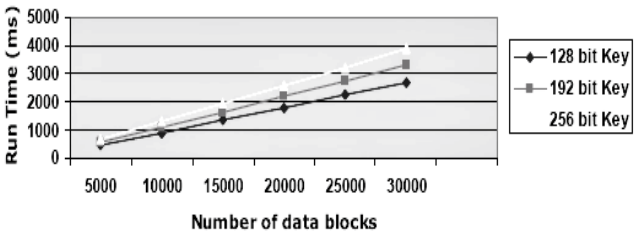

Fig 3.Performance of AES with 3 different bit key

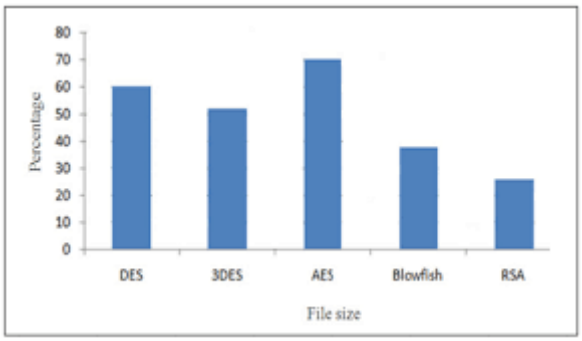

Fig 4.Decryption time vs. File size of various encryption algorithm

The fig 3 shows the performance of AES with three different bit key such as 128, 192 and 256 bit key. Thus, we use AES with 128-bit key for encrypting and decrypting the file in less time when compared with the 192-bit key and 256-bit key. As shown in the fig 4, the AES Algorithm has the highest avalanche effect when compared with the other encryption algorithm as shown in the fig 4.

VI. CONCLUSION AND FUTURE WORK

In proposed project, 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 user wants to download a file, they should enter a secret key of their file; only then the fragmented chunks will get merged. Now, the user can download the file. This provides security at client level and network level. Here also focuses on secure file access with drops methodology. A time based access control mechanism will be implementing to provide

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

access control to the data user. The aforesaid future work will save the time and resources utilized for downloading, updating, and uploading the file again.

Currently with the DROPS methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism that can identify and update only the required fragments. The aforesaid future work will save the time and resources utilized for downloading, updating, and uploading the file again. Moreover, the implications of TCP in cast over the DROPS methodology need to be studied in which it is relevant to distributed data storage and access.

REFERENCES

1. Ranjana Badre, Cloud storage with improved access control and assured deletion- International Journal of Innovations in Engineering and Technology (IJIET) ISSN: 2319 – 1058 Volume 3 Issue 3 February 2014
2. Jyoti Bansode, Anjana Ghule, A Review on Achieving Security by Fragmentation and Replication of Data (Drop)- International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2017
3. 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.
4. B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol. 9, No. 2, 2011, pp. 50-57.
5. S.Suganya, R.Kalaiselvan, An Optimization And Security Of Data Replication In Cloud Using Advanced Encryption Algorithm- International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issues 6 June 2016, Page No. 16836-16841
6. M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.
7. Varun Krishna and Veeramachaneni, Security Issues and Countermeasures in Cloud Computing Environment- International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 5, September 2015
8. Kashif Bilal, Marc Manzano, Samee U. Khan, On the Characterization of the Structural Robustness of Data Center Networks- IEEE Transactions On Cloud Computing, Vol. 1, No. 1, January-June 2013
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.
11. W. K. Hale, "Frequency assignment: Theory and applications," Proceedings of the IEEE, Vol. 68, No. 12, 1980, pp. 1497-1514.
12. 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.
13. 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.
14. 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.
15. 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.