IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Cloud Data Security on Cloud Using Geo-Social Attributes

Laxmikant Ashok Bhole[1], Pratik Kumar Vikas Patil[2], Rahul Subhash Salve[3], Pratik Datta Warade[4], Mrs. M. Shaikh[5]

Student, Information Technology, RSCOE, Pune, India [1, 2, 3, 4]

Assistant Professor, Information Technology, RSCOE, Pune, India[5]

Abstract: Cloud storage system empowers storing of data in cloud server effectually and allows the user to work with the data without any trouble of the resources. In existing system, mainly data damage occurred due to attacks by unauthorized user, attacker or hacker. High security technique is required in cloud to protect user's data from unwanted resources and unauthorized user. In the proposed system, for improving optimal performance and security some key techniques are wont such as Encryption Replication Fragmentation and Geo-Parameter. Fragmentation is used for divide the file into multiple slices. Fragmented slices are used as input for Replication to replicate these slices. Replication will improve availability of proposed system. Geo-Parameter is impressive way for file transaction in system as it provides security parameter like Time, Date, and Location. In propose system Division and Replication of Data in the Cloud for Optimal Performance and Security that collectively approaches the security and performance issues. In this methodology, we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the proposed methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies.

Keywords: Fragmentation, Replication, Cloud Security, Data Integrity, Location Privacy.

I. INTRODUCTION

In Information Technology field data storage is recognized as one of the important growing factor over cloud. Now a day's network based applications uses distributed storage rather than server attached storage (client server storage).distributed storage have many advantages but also have many more new challenges as processing reliable and secure storage and access facility in unreliable and insecure service provider [2][7] . During past decades, distributed storage works on either Network-Attached Storage (NAS) or Storage Area Networks (SANs) on the LAN level, such as a network of a campus or an organization. The distributed storage nodes are managed by the same authority in SANs or NAS. SAN or NAS node is accessed and controlled by system administrator thus data security is under control. Redundancy is important factor of cloud depending upon reliability [7]. Protection of storage is mainly depending upon how system protects data from outsider's attack/intrusion. Robust cryptograph schemes provide CIA Triangle security to cloud data (confidentiality, integrity and availability) [1]. However, such a security system is not robust enough at the level of wide area networks to protect the data in distributed storage applications.[2] The recent progress of network technology allows global-scale association over heterogeneous networks with different authorities. Data storage is more transparent to the user in the environment of peer-to-peer (P2P) file sharing or the distributed storage in cloud computing atmosphere. In robust security protection there is no guarantee the data host nodes are under control [5]. In addition, the activity of the middle owner is not controllable to the data owner. Logically speaking, an attacker can do whatever he/she wants to the data stored in a storage node once the node is negotiating. If node or the node administrator becomes malicious then the confidentiality and the integrity would be violated over cloud. In cloud for providing better security Location based approach is used for transformation of data [11]. Geo-Social attribute such as date time location are applying in system for security mechanism. Geo functionality comes with remarkably decreased risks to personal privacy. Geo social application operates on fine-grain, time-stamped location information. Time-stamped location information technique achieved by using time and date parameters. [11][12] Fine-grained access control system facilitates granting various access rights to user. Longitude and latitude gives accurate location of user for accessing files or users data over cloud.

II. PROPOSED SYSTEM

The proposed methodology concern with retrieval time to improve security and performance of cloud storage. The data file was first fragmented and then encrypted. The fragments are scattered over multiple nodes [6]. The nodes were separated by use of T-coloring algorithm-coloring

DOI 10.17148/IJARCCE.2016.54117

allows to place node at certain distance which provide more confidentiality for data, in system it store fragments in alternative manner at node[8]. The fragmentation guaranteed that no related information was gain by an attacker in case of a successful attack. Single node stores the single fragment with encrypted format. Only single fragment of particular file is stored on single node in cloud, it means no redundancy will occurs. When file is stored on cloud at that time geo attribute will attached to file [2][8]. Receiver has to accomplish the entire attribute successfully then only file will be accessible to user. The results of the simulations that focus on the security and performance resulted in increased security level of end user's data[10].

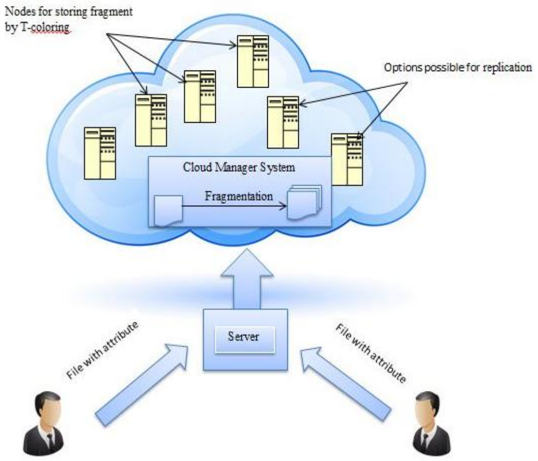

Fig 1. Replication and Fragmentation in Server

This proposed system is for improving security and performance with related to cloud data storage, by merging following techniques that is Division, Replication and Geo-Attributes. In proposed system T-coloring technique is used for fragmenting and replicating data in cloud[1]. The proposed scheme constructing in such a way that in case of victory attack, no relevant information is acknowledge to the raider. Now a day's cryptography is trending, by using this technique secure communication is achieved [9]. In the proposed system, one of the powerful encryption technique is used that is, AES (Advanced Encryption Standard). The proposed system will guarantees that controlled duplication of file fragments and each fragment concern with that file are replicates for the purpose of improving security and availability [8].

III. OBJECTIVES\SCOPE OF PROJECT

The scheme develops for outsourced data that takes into account both the security and performance. The proposed scheme fragments and replicates the data file over cloud nodes. Y The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker. The proposed system does not rely on traditional cryptographic techniques for data security. The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the data. There is a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security. Flexibility to support point, circular range, and nearest neighbor queries on location data. Efficiency in terms of computation, bandwidth, and latency, to operate on mobile devices.

Strong location privacy: The servers processing the data (and the administrators of these servers) should not be able to learn the history of locations that a user has visited.

Location and user unlink ability: The servers hosting the services should not be able to link if two records belong to the same user, or if a given record belongs to a given user, or if a given record corresponds to a certain real world location.

Location data privacy: The servers should not be able to view the content of data stored at a location.

IV. ARCHITECTURE

The new system architecture shown below describes works and flow:

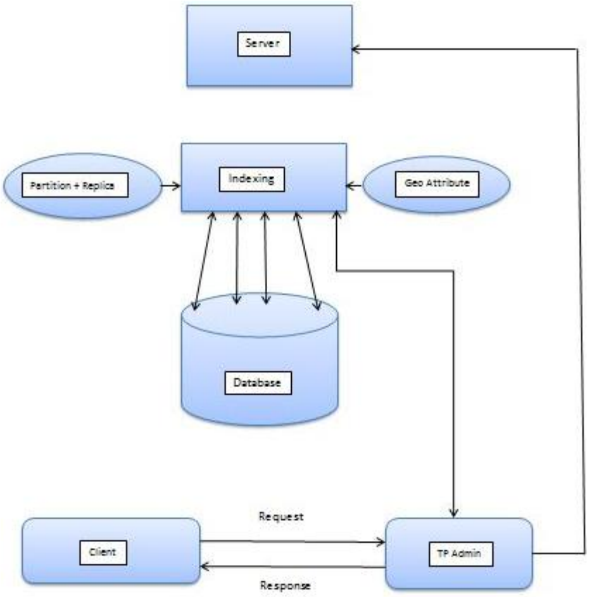

Fig.2 System Architecture

The system will not to store the entire file at a single node. It will encrypts the file first and handover to cloud server. Cloud server will send encrypted data to store in database server. The cloud manager system upon receiving the file performs: **(**a) Fragmentation **(**b) First cycle of nodes selection and stores one fragment over each of the selected nodes and then, **(**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. The fragmentation threshold of the data file is specified to be generated by the file owner. The file owner can specify the fragmentation threshold in terms of either percentage or the number and size of different fragments with geo-attributes. This methodology uses controlled replication where each of the fragments is replicated only once in the

DOI 10.17148/IJARCCE.2016.54117

cloud to improve the security. To handle the download request from user, the cloud manager checks attributes which comes with file and collects all the fragments from the nodes and re-assembles them into a single file. Afterwards, the file is sent to the user.

V. ALGORITHM

1. Fragmentation Algorithm

```
If file is to be split go to step 2 else merge the fragments of the file and go to step 10.
Input src path, destn path, sof
Size= size of source file
Print size
If size>sof go to step 6 else print file cannot be split and go to step 10
Split into fragment=sof
Size=size-sof
If size>sof go to step 6
We get fragments with merge option
End
```

Fragment replication:-

After the file is divided into fragments for the security purpose at cloud server we are making replicas of fragments. This algorithm makes only one replica of every fragment to store the space and bandwidth.

```
Input:  File Fragments.
Output: -Replicas of fragments.
for each Oκ in O do
      select $\mathcal{S}^i$ that has max ($\mathcal{R}^i_k$+ $\mathcal{W}^i_k$)
      if col$\mathcal{S}^i$ =open_color and $\mathcal{S}^i$>= $\mathcal{O}_k$ then
$\mathcal{S}^i \leftarrow \mathcal{O}_k$
$\mathcal{S}_i \leftarrow \mathcal{S}_i - \mathcal{O}_k$
col$\mathcal{S}^i$←close_color
$\mathcal{S}^{i'}$←distance($\mathcal{S}^I$,T)⊳ /*return all nodes at
Distance T from$\mathcal{S}^i$ and stores at temporary set$\mathcal{S}^{i'}$ */
col$\mathcal{S}^{i'}$←close_color
end if
end for
```

Fragment Allocation:-

All the fragments of file and its replica we have to store at database and to provide security we are allocating these fragments and replicas using T-Coloring Graph concept.

Input: -File fragments and its replicas

Output: -Fragments allocated at different nodes.

2. AES(Advanced Encryption Standard):

```
Cipher(byte in[16], byte out[16], key_array
round_key[Nr+1])
begin
byte state[16];
 state = in;
 AddRoundKey(state, round_key[0]);
for  i = 1  to  Nr-1  stepsize 1 do
 SubBytes(state);
             ShiftRows(state);
             MixColumns(state);
             AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
 ShiftRows(state);
 AddRoundKey(state, round_key[Nr]);
end
```

3. T-Coloring

T-coloring consists on coloring the vertices of a graph in such a way that the two colors assigned to two adjacent vertices i and j does not appear in Tij, where Tij is a set of positive integers associated to the edge [i,j]. The T-Coloring problem is to find the minimum length of the spectrum of colors used.

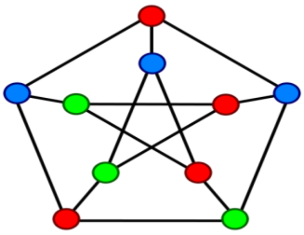

Fig 3.T-Coloring Node Representation

Coloring the vertices of a graph such that no two adjacent vertices share the same color is called a vertex coloring. Similarly, an edge coloring assigns a color to each edge so that no two adjacent edges share the same color, and a face coloring of a planar graph assigns a color to each face or region so that no two faces that share a boundary have the same color.

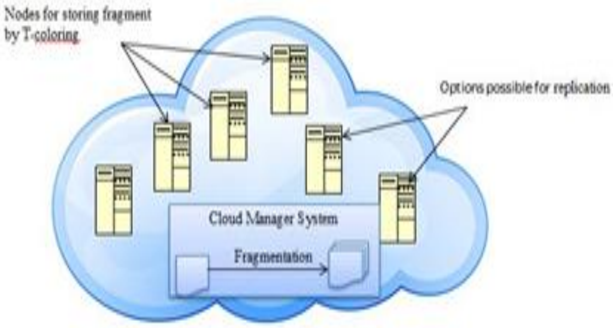
Nodes for storing fragment by T-coloring
Options possible for replication
Cloud Manager System
Fragmentation

Fig 4 T-Coloring File Nodes

VI. SYSTEM MODULES

1. Cloud Client:-

Cloud client should be Data owner or Data user.

Data Owner:-

Data owner is responsible for uploading file on cloud as well as view files uploaded by him or others. Data owner has information about the placed fragment and its replicas with their node numbers in cloud.

Data User:-

Data user is the one who is responsible for downloading files or view files uploaded by others. To download file from cloud he has to be authenticated user otherwise he will be considered as attacker.

DOI 10.17148/IJARCCE.2016.54117

2. Cloud Server:-
Fragmentation:-
This approach is used for fragmenting the file for security purpose at sever side. This approach runs the Fragmentation algorithm. It has file as input and produces the file fragments as output.

Replication:-
This approach creates replicas (duplicate copy) of fragments. These replicas are useful when one of fragment is corrupted by attacker then to provide file for user admin replaces its replica at that place and combine all fragments and send file to authenticated user or data owner. To make replicas of file fragments this approach runs replication algorithm which takes input as fragments and produces its replicas as output.

Allocation:-
After the file is spitted and replicas are generated then we have to allocate that fragments at cloud server for storing data. While storing or allocating that fragments we have consider security issues. So we are using T-Coloring Graph concept for placing fragments at different nodes on cloud server. This approach runs Fragment allocation algorithm which takes input as fragments and produces the output as fragments allocated with node numbers.

VII. RESULTS AND GRAPHS OF WHOLE SYSTEM

1. To analyze the performance of our approach, we selected a text file with a file size of 1 MB. It shows the encoding and uploading time vs. the number of data pieces set by the user and set the parameter; like Latitude longitude, Date and Time. If all this parameter is match then it will be downloadable otherwise give error.

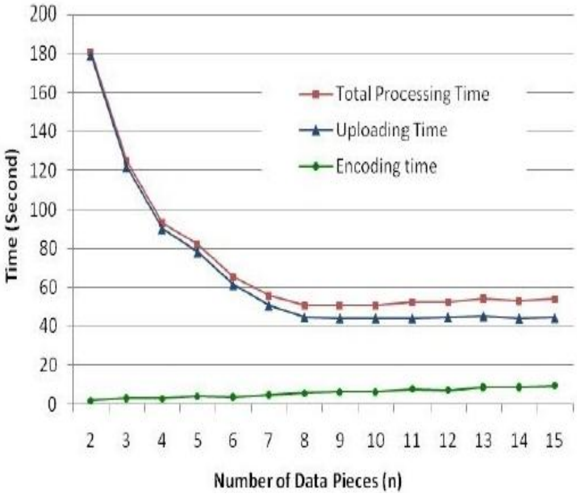

Fig 5. Encoding & uploading time vs. number of data pieces (1MB file)

From the figure, we can see that when we increase the number of data pieces from 2 to 8, the uploading time drops down significantly; while the encoding time has slightly increased. The significant performance improvement for uploading is due to the use of multithreading technique; while the increased number of data pieces along with more checksum pieces results in more overhead for encoding. However, when the number of data pieces n is further increased, the uploading time and the total processing time become relatively stable.

2 To analyze the performance of our approach, we selected a text file with a file size of 1 MB. It shows the decoding and downloading time vs. the number of data pieces set by the user and set the parameter; like Latitude longitude, Date and Time. If all this parameter is match then it will be downloadable otherwise give error.

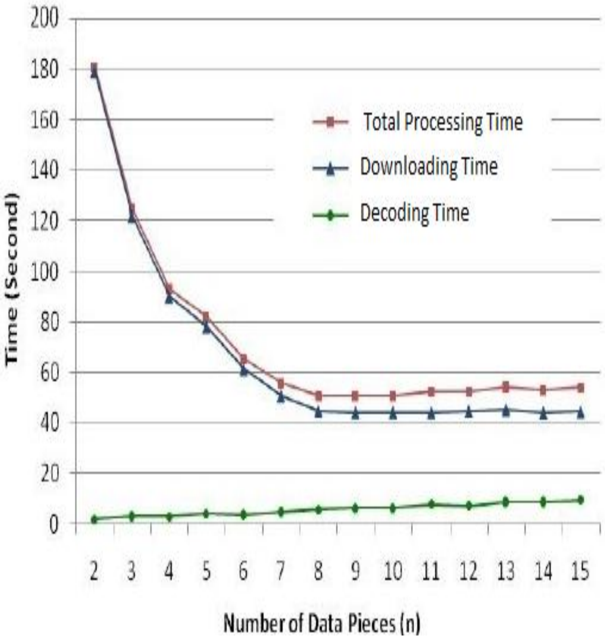

Fig.6. Downloading and decoding time vs. number of data pieces (1 MB file)

From the above experimental results, we can see that both the uploading and downloading time can be significantly reduced by selecting a reasonable number of data pieces. For example, when the file size is about 1 MB, based on experiments, the number of data pieces should normally be set to 8 as long as the network condition is excellent, and the client machine has similar performance.

VIII. ADVANTAGES

- It will keep the attacker uncertain about the locations of the file fragments.
- It will improve data retrieval time the nodes are selected based on the centrality measures that ensure an improved access time.
- It provide security tripod like integrity, availability and security.

IX. FUTURE SCOPE

Currently with the proposed methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop an automatic update mechanism

DOI 10.17148/IJARCCE.2016.54117

that can identify and update the required fragments only. The aforesaid future work will save the time and resources utilized in downloading, updating, and uploading the file again. Moreover, the implications of TCP in cast over the DROPS methodology need to be studied that is relevant to distributed data storage and access. In future work will increase security and originality of file by applying the digital signature to file.

X. CONCLUSION

The developed system, a cloud storage 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 separated 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. The system works along with geo-location and attributes like date and time.

REFRENCES

[1] Bhole Laxmikant, Mrs. M.S haikh, Patil Pratik kumar, Salve Rahul, Warade Pratik :"A SURVEY ON CLOUD DATA ACCESS PRIVILEGE WITH FULLY ATTRIBUTE-BASED ENCRYPTION WITHGEO SOCIAL SECURITY", Vol. 3, Issue 11, November 2015

[2] 'DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security' Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE

[3] T. Loukopoulos and I. Ahmad, "Static and adaptive distributeddata replication using genetic algorithms," Journal ofParallel and Distributed Computing, Vol. 64, No. 11, 2004, pp.1270-1285.

[4] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, "On the placement of web server replicas," In Proceedings of INFOCOM2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 3, pp. 1587-1596, 2001.

[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] A. Mei, L. V. Mancini, and S. Jajodia, "Secure dynamic fragment and replica allocation in large-scale distributed file systems," IEEE Transactions on Parallel and Distributed Systems, Vol.14, No. 9, 2003, pp. 885-896.

[7] M. Newman, Networks: An introduction, Oxford University Press, 2009.

[8] 'PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique' C. Selvakumar Department of Information Technology MIT Campus, Anna University Chennai, Tamil Nadu, G. Jeeva Rathanam Department of Information Technology MIT Campus, Anna University Chennai, Tamil Nadu, M. R. Suma latha Department of Information Technology MIT Campus, Anna University Chennai, Tamil Nadu.

[9] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.; "Slicing: A New Approach for Privacy Preserving Data Publishing," Knowledge and Data Engineering, IEEE Transactions on vol.24, no.3, pp.561-574, March2012.

[10] Wang Cong, Wang Qian, RenKui, Cao Ning and Lou Wenjing ,"Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2,pp.220-232, April-June 2012.

[11] "Preserving Location Privacy in GeosocialApplications"Krishna P. N. Puttaswamy∗, Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao Department of Computer Science, UC Santa Barbara.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS, 2006.

DOI 10.17148/IJARCCE.2016.54117