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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on Cloud Data Access Privilege with Fully Attribute-Based Encryption with Geo Social Security

Bhole Laxmikant, M.Shaikh, PatilPratikkumar, Salve Rahul, Warade Pratik

Dept. of Information Technology, JSPM's RajarshiShahu College Of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT: In cloud computing main security concern is outsourcing data to Third–party Administrative control. The data damage may occur due to attacks by unauthorized user and attacker.High security measures are required to protect data within the cloud. However, security strategy must take focus towards optimization of data retrieval time. In the proposed system, a Division Encryption and Replication are implemented on data over cloud to improve optimal performance and security. The geo social approach is an impressive way for location based security to access file after authentication of location. In geo-social approach, using Geo attribute security is provided for data in system for file transaction over cloud storage.

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

I. INTRODUCTION

Data storage has been recognized as one of the important growing factor of information technology. The advantage of network based applications leads to the moving from server attached storage to distributed storage. Along with variant advantages, the distributed storage also poses new challenges in creating a secure and reliable data storage and access facility over insecure or unreliable service providers [1][6]. Aware of that data security is the kernel of information security, a plethora of efforts has been made in the area of distributed storage security. During past decades, most designs of distributed storage chose the form of either Storage Area Networks (SANs) or Network-Attached Storage (NAS) on the LAN level, such as a network of an enterprise, a campus, or an organization[6]. Either in SANs or NAS, the distributed storage nodes are managed by the same authority. The system administrator has the access and control over each node, and essentially the security level of data is under control [1]. The reliability of such systems is often achieved by redundancy, and the storage security is highly depending on the security of the system against the attacks/intrusion from outsiders[4].

The confidentiality and integrity of data are mostly achieved using robust cryptograph schemes [7][9]. However, such a security system is not robust enough to protect the data in distributed storage applications at the level of wide area networks. The recent progress of network technology enables global-scale collaboration over heterogeneous networks under different authorities. For instance, in the environment of peer-to-peer (P2P) file sharing or the distributed storage in cloud computing environment [10], it enables the concrete data storage to be even transparent to the user. There is no approach to guarantee the data host nodes are under robust security protection. In addition, the activity of the medium owner is not controllable to the data owner[7]. Theoretically speaking, an attacker can do whatever he/she wants to the data stored in a storage node once the node is compromised. Therefore, the confidentiality and the integrity would be violated when an adversary controlled a node or the node administrator becomes malicious[9]. Location based approach is used for better security of data over cloud. Various attribute present in Geo-Social approach applying in system for security mechanism [10][11].

II. RELATED WORK

A:PDDS: Partitioning and Domain integrity checking for Data Storage

In PDDS, Integrity checking concepts is used to detect and avoid misbehaving server considering data correction and error localization. The distributed verification scheme achieves the storage correctness insurance and data error localization. when data corruption has been detected during the storage correctness verification, it will guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server[9]. Main aim of work designing an efficient storage scheme to ensure the availability and correctness of data using partitioning over cloud.Partitioning plays an important role data storage security. It breaks larger files into smaller parts to store the data efficiently enhancing easy access to data in cloud[7][8].This partitioning is known as slicing ,which partitions the data both horizontally and vertically. Generalization and bucketization are overcomes by slicing for better protection against privacy [8]. cloud storage is not just a third party data warehouse. The data stored in the cloud not only be accessed but also be frequently updated by the users ,such as insert, delete, modify, append, etc. This dynamic feature supports the integration for the cloud storage [9].

B. DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security

The fragmentation used for fragmenting the files for security purpose at sever side having local file as input and produces the file fragments as output. To keep an attacker uncertain about the locations of the file fragments and improve the security. This ensures that even in the case of a successful attack, no meaningful information is received to the attacker [1][5].The replication is used for creating duplicate copy (replicas) of fragments. These replicas of fragment are useful when one of fragment is damaged by attacker. This damaged fragment is replacing by replica of fragment and combines all fragments for reconstructing original fragment [2][5]. Security and replication are essential for a large-scalesystem, such as cloud, as both are utilized to provide services to the end user. Security and replication must be balanced such that one service must not lower the service level of the other [1]. The optimal performance provides an automatic update mechanism that identify fragment and then update necessary fragment [1]. Fragments are encrypted before storage which allows identical files to be detected with high probability, even with different names and encrypted with different keys. File storage focuses mainly on dynamic secure file allocation in such large-scale distributed infrastructures. [5].

C.Location Privacy in Geo social Applications

In Geo social approach introducing *LocX*, an alternative way that provides significantly-improved location based security. LocX provides location privacy for users withoutany errors into the system. In LocX, users easily transformtheir location and shared with the server and encrypt all location data stored on the server [10].The vital key is applied to secure user-specific, distance-preserving coordinate transformationsto location.Geo-social system operate on fine-grain, time-stamped location information. The lead role of geo Social application is to location based security to access file after authentication of location [11]. Geo social system have mainly taken three approaches to improving user privacy in systems: (a) introducing error into location data (b) depending on trusted servers for user identities and private data and (c) relying on heavy-weight cryptographic or private information retrieval techniques. The trusted proxies or a server in the Geo-social system plays an important role to protect user location privacy.

III. PROPOSED SYSTEM

The proposed methodology in cloud storage security thatwillbe used to improve security and performance in retrieval time. The data file was first encrypted and fragmented. The fragments are dispersed over multiple nodes.The nodes were separated by means of T-coloring. The fragmentation and dispersal ensured that no related information was obtainable by an attacker in case of a successful attack.Only single fragment of file will be stored in single node [1] .No node in the cloud, stored more than a single fragment of the same file.The geo-attribute will be attached to file at the time of storing and it will be accessible when user accomplishes all the attributes.The results of the simulations revealed that the simultaneous focus on the security and performance resulted in increased security level of data accompanied [10].

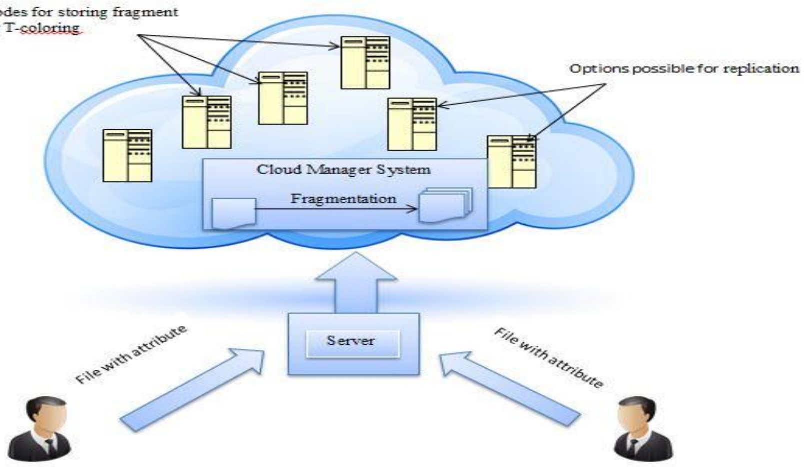

Fig. 1 Fragmentation and Replication in Server

The proposed scheme is for cloud data storage thattakes geo-attributes and division and replication techniques to improve both security and performance.The proposed scheme fragments andreplicates the data file over cloud nodes. The proposed scheme ensures that evenin the case of a successful attack, no meaningfulinformation is revealed to the attacker.It will not rely on traditional cryptographic techniquesfor data security. The non-cryptographic (Elliptical Curve Cryptography Algorithm)nature of the proposed scheme makes it faster toperform the required operations (placement andretrieval) on the data [1][7]. System will ensure a controlled replication of the file fragments, where each of the fragments is replicated only once for the purpose of improved security.

IV. ARCHITECTURE

The new system architecture shown below describes works and flow:

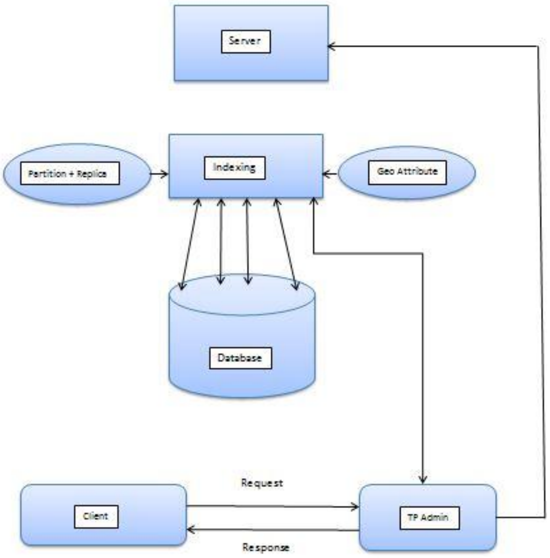

Fig.2 System Architecture

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

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 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

Elliptical Curve Cryptography Algorithm

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Let E be an elliptic curve over finite field Fp.

Let p be a point on E (Fp) and suppose that P has prime order n. then the cyclic subgroup E (Fp) generated P is <P>={ ∞,P, 2P, 3P, 4P...........(n-1)P}.

The prime P, the equation of the Elliptic curve E, and the point P and its order n are the public domain parameter. A private key is an integer d that is selected uniformly at random from the range [1, (n-1)] and the corresponding public key is Q=d*P [4], [5].

Key pair generation
Input: - Elliptic curve domain parameter (p, E, P, n)
Output: - Public key Q, private key d.
1. Select d =R [1, (n-1)]
2. Compute Q=d*P.
3. Return (Q, d)

The first task is to encode the plane text message m to be sent as an x-y point Pm. It is the point Pm that will be encrypted as cipher text and subsequently decrypted. To encrypt and send a message Pm to B, A Chooses a random positive integer k and produces the cipher text Cm = {K*P, Pm + k*Q}, where Q is B's public key. The sender transmits the point C1=k*P and C2=Pm+ K*q to the recipient. To decrypt the cipher text, B multiplies by the first point in the pair by B's secret key and subtract the result from the second point as Pm+ k*q-d(k*P)=Pm+ k(d*P)-d(kP)=Pm..

A. *Elliptic Curve Encryption*

Input: Elliptic curve domain parameter (p, E, P, n), public key Q, plain text m
Output: Cipher text Cm
1. Represent the plane text m as a point Pm in E (Fp).
2. Select k [1, (n-1)].
3. Compute C1=k*p
4. Compute C2=Pm+ K*q.
5. Return (C1, C2).

B. *Elliptical Curve Decryption*

Input: Elliptic curve domain parameter (p, E, P, n), private key d, Cipher text Cp.
Output: Plain Text m.
1. Compute Pm =C2-d*C1
2. Compute (Pm)

C. *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
```

D. 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 $O_k$ in do
    Select $S^i$ that has max ( $R^i_k$ + $W^i_k$ )
    If $col_{si}$=o_color and $s_i$>= $o_k$ then
            $S^i$ ← $O_k$
            $S_i$  $S_i$ ← $O_k$
            Col $_{Si}$ ← c_color
                $S^i$ ← distance ( $S^i$ , T )    / * returns all nodes at
                Distance T from $S^i$ and stores in temporary set $S^i$ */
               Col $_{si}$ ← c_color
    end if
end for
```

E. 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.
Inputs and initialization
O={$O_1$ ,$O_{2,........,}$ $O_N$}
O={sizeof($O_1$) ,sizeof($O_2$),……,sizeof($O_N$)}
col={o_color,c_color}
cen={$cen_{1,}$ $cen_{2,......}$$cen_M$}
colo_ ← color∀ i
cence ← $n_i$∀ i
Compute:
for each $O_k$ $\varepsilon$ O do
select  $S^i$ | $S^i$index ← of(max($cen_i$))
if col $_S{}^i$ =o_color and $s_i$>=$o_k$ then
     $S^i$   ← $O_k$
$s_i s_i$- $o_k$   ←
$col_S{}^i$c_color ←
     $S^{i}$ ‘    ←distance($S^i$ ,T)   /* returns all nodes at
     Distance T from $S^i$ and stores in temporary set $S^{i}$ ‘   */
$col_S{}^{i}$‘      c_color ←
end if
end for
```

VI. APPLICATION

This system can be used in different real-time application such as banking sector to improve banking database security. In banking an effective way to give security for distributed storage system, it will provide for privacy based on location. In case of accessing the confidential data it will be beneficial to give location based parameter.

In education, system will be used in examination system of university. In educational system various universities and colleges prefer the online work rather than offline and examination is also taken online but unauthorized accessing issues still present. To avoid these issues location based parameter is an effective way to improve security.

VII. 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.

VIII. CONCLUSION AND 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 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. In future work will increase security and originality of file by applying the digital signature to file.In this proposed system, overall work focus on improved data storage security over cloud for optimal performance of cloud transaction. The partitioning of local file enables storing of data in easy and effective manner over cloud. The local file is fragmented and these fragments are stored on cloud for better security of data. The replication is used for creating duplicate copy (replicas) of fragments. These replicas of fragment are useful when one of fragment is damaged by attacker. This damaged fragment is replacing by replica of fragment and combines all fragments for reconstructing original fragment. The optimal performance provides an automatic update mechanism that identify fragment and then update necessary fragment. Geo approach for file provides significantly-improved location based security. Geo attribute plays vital role in location based security for file access over cloud.

REFERENCES

[1] ‘DROPS: Division and Replication of Data inCloud for Optimal Performance and Security’Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, SeniorMember, IEEE, BharadwajVeeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, andAlbert Y. Zomaya, Fellow, IEEE
[2] 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.
[3] L. Qiu, V. N. Padmanabhan, and G. M. Voelker, “On theplacement of web server replicas,” In Proceedings of INFOCOM2001, Twentieth Annual Joint Conference of the IEEE Computer andCommunications Societies, Vol. 3, pp. 1587-1596, 2001.
[4] B. Grobauer, T.Walloschek, and E. Stocker, “Understandingcloud computing vulnerabilities,” IEEE Security and Privacy, Vol.9, No. 2, 2011, pp. 50-57.
[5] A. Mei, L. V. Mancini, and S. Jajodia, “Secure dynamic fragmentand replica allocation in large-scale distributed file systems,”IEEE Transactions on Parallel and Distributed Systems, Vol.14, No. 9, 2003, pp. 885-896.
[6] M. Newman, Networks: An introduction, Oxford UniversityPress, 2009.
[7] ‘PDDS - Improving Cloud Data Storage SecurityUsing Data Partitioning Technique’C. SelvakumarDepartment of Information TechnologyMIT Campus, Anna UniversityChennai, Tamil Nadu, G. JeevaRathanamDepartment of Information TechnologyMIT Campus, Anna UniversityChennai, Tamil Nadu, M. R. SumalathaDepartment of Information TechnologyMIT Campus, Anna UniversityChennai, Tamil Nadu.
[8] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.; "Slicing: A NewApproach for Privacy Preserving Data Publishing," Knowledge and DataEngineering, IEEE Transactions on vol.24, no.3, pp.561-574, March2012.
[9] Wang Cong, Wang Qian, RenKui, Cao Ning and Lou Wenjing ,"Toward Secure and Dependable Storage Services in CloudComputing," Services Computing, IEEE Transactions on , vol.5, no.2,pp.220-232, April-June 2012.
[10] “Preserving Location Privacy in GeosocialApplications”Krishna P. N. Puttaswamy∗, Shiyuan Wang, Troy Steinbauer,DivyakantAgrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. ZhaoDepartment of Computer Science, UC Santa Barbara.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryptionfor fine-grained access control of encrypted data,” in *CCS*, 2006.