IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

# Implementation of Meta Data Storage using Fragmentation method for more security in the cloud

**V. Kiran Kumar[1*], E. Hari Prasad[2]**

[1]Department of Computer Science, Dravidian university, kuppam, India
[2] Department of Computer Science, Dravidian university, kuppam, India

[*]*Corresponding Author:* Hariprasad.e@gmail.com , *Tel.: +91-9949945900*

**Available online at: www.ijcseonline.org**

Accepted: 23/Jan/2019, Published: 31/Jan/2019

***Abstract***— Cloud Computing has wide range of opportunities for research and industry purpose. There are many issues to consider in cloud. The one of the main issue in cloud is Security. Protecting more secured data in cloud is a big task. To achieve more security for a sensitive data, a model is proposed .In this paper, providing more security for sensitive data is achieved by fragmenting the data and allocating the preferences to the data and only high secured data is encrypted and stored. The detailed implementation of the work is discussed clearly in the paper.

***Keywords*—** sensitive data, fragmentation, Public Data Segment (PDS), Sensitive Data Segment (SDS)

## I. INTRODUCTION

Computing is one of the emerging technologies in Computer Science. Cloud provides various types of services to us. Database Outsourcing is a recent data management paradigm in which the data owner stores the confidential data at the third party service provider's site. The service provider is responsible for managing and administering the database and allows the data owner and clients to create, update, delete and access the database. There are chances of hampering the security of the data Due to untrustworthiness of service provider. So, to secure the data which is outsourced to third party is a great challenge. The major requirements for achieving security in outsourced databases are confidentiality, privacy, integrity, availability. To achieve these requirements various data confidentiality mechanisms like fragmentation approach, High-Performance, optimization Engine approach etc. are available. In this paper, various mechanisms for implementing Data Confidentiality in cloud computing are analyzed along with their usefulness in a great detail.

IT businesses are migrating to the Cloud environment at a rapid elasticity. Security of information that is being processed by way of the purposes and finally getting saved in the data facilities are of gigantic issues of this newly evolving environment. The protection of the data is a quandary not most effective in the course of transferring of information by means of the wires but additionally for the duration of its storage. The architecture that is wanted to at ease the saved information is of so much value than whilst the information is getting transferred given that of the truth that the info resides fairly for a very long time within the storage subject than within the wires.

To make certain the safety of the data stored within the knowledge facilities, a new methodology is proposed which would not thoroughly help in proscribing a hacker to access the information but will make the information worthwhile if it is extracted through a hacker but at the identical time ensures the best of the info that is being furnished to its respective proprietor or licensed consumer. A metadata based knowledge segregation, storage methodology and solutions is proposed to access this segregated information. This system ensures that data is important in the course of static house and positive aspects worth most effective for the duration of acquisition or updating.

## II. FRAGMENTATION OF DATA

Fragmentation can be horizontal, vertical or mixed/hybrid. Horizontal Fragmentation (HF) lets in a relation or elegance to be partitioned into disjoint tuples or times. Vertical Fragmentation (VF) allows a relation or magnificence to be partitioned into disjoint units of columns or attributes besides the primary key. Combination of horizontal and vertical fragmentations to combined or hybrid fragmentations (MF) are also proposed (Navathe 1995). Allocation is the procedure of assigning the fragments of a database at the web sites of a distributed network. When statistics are allotted, it is able to either be replicated or maintained as a unmarried replica. The replication of fragments improves reliability and efficiency of read-handiest queries however will increase update price The major motives of fragmentation of the relations are to: growth locality of reference of the queries submitted to database, enhance reliability and availability of statistics and overall performance of the gadget, balance storage capacities and reduce communication costs amongst sites (Baio 2004).

Fragmentation is a layout method to divide a single relation or class of a database into or more partitions such that the mixture of the partitions provides the unique database with none lack of information (Ozsu et al 1999). This reduces the amount of inappropriate records accessed by using the packages of the database, accordingly reducing the wide variety of disk accesses.

## III. FRAGMENTED META DATA STORAGE

The model defined deals handiest with the facts security at the storage centers. This in turn has two issues: One issue is about the actual physical unit wherein the facts are stored and the alternative one is the intrusion into the facts. The proposed model specifically focuses in presenting security to avoid intrusion. This model does not prevent hackers from getting maintained of the data. Rather it makes the records precious although its miles accessed by means of an interloper. To adhere to this version, care needs to be taken right from the design segment of the facts storage. Data needs to be segregated into Public Data Segment (PDS) and Sensitive Data Segment (SDS). The SDS has to be further fragmented into smaller units till every fragment does now not have any value individually. The fragmentation want now not be of a couple of stages. Instead, effort is required to perceive the key element that makes the data touchy and should be fragmented one after the other. Below Figure explains this fragmentation.[6]

The proposed methodology is quite unique from commercially available sliced records garage answers like Symform and Cleversafe which was evaluated by Paul (2011). In those answers, the statistics is considered in byte formats. In a typical state of affairs, data is broke into 64MB chunks and each bite is encrypted with AES 256 bit encryption and then these chunks are saved in distinct locations. These solutions are applicable for raw facts, but this could not be powerful for data stored in relational databases that have records interdependencies and are logically saved based on schemas.[6]

The DME now has to fragment these facts. The DME have to be able to be configured or custom designed with appreciate to the level of safety required. Considering the desired example, if DME desires to provide medium degree protection, it needs to fragment most effective records which are of 'Critical' criteria. And if excessive stage safety is required, it should fragment facts present in each 'Critical' and 'Sensitive' standards. The DME isn't always privy to the real statistics residing within these tables. Hence alongside the metadata of the tables, the number one key column call needs to be provided in addition to it. This is without problems available with the schema statistics of the database tables. The specific levels of protection wanted and their corresponding metadata need to be configured with the DME.[6]

After fragmentation is finished, the DME segregates the schema, separating out the information changed by means of DME, 'Originally Sensitive' information and 'Normal' information. The DME then actions the 'Normal' data to at least one database and 'Originally Sensitive' statistics to any other database and AD of 'Sensitive DME' information to another database at exclusive vicinity and MD of 'Sensitive DME' to the database with 'Normal' statistics. With recognize to the AD, if DME creates its very own desk, then this desk will be the more secured records and may be saved in a exclusive vicinity. Different region here states the both specific server on the same geographical location or at different geographical vicinity. Additionally one extra mapping is required for mapping the original desk with the fragmented facts set. This can be saved in a separate table.

## IV. IMPLETATION

The proposed data storage model was initially implemented with an algorithm and parts of it were fine tuned to provide a efficient fragmentation mechanism. It was made sure that the algorithm developed uses simple data structure so that the processing time per cycle of the algorithm is minimal. This algorithm is the core part of the fragmentation mechanism and is used in the creation of the fragmented schema. This algorithm takes care of the sensitivity information for each element of the schema and also the number of resources being used in the distributed environment in which the fragmented data is stored.

**A typical algorithm used for fragmentation is depicted in the pseudo code below.**

Let us consider the number of Tables as 'x' and the number of. Database Servers (DBS) as 'a'

```
    For m = 1 to a
    DBS[m].used = 0;
     For loop end
     For n=1 to x
    Retrieve Metadata_ Sensitivity (Table[n])
    For loop end
    For n=1 to x
    If (Table (n) .Sensitivity = = regular)
    {
    DBS xy = retrieve_ idle DBS ()
CopyTableWithinDBS (xy, Table[n])
```

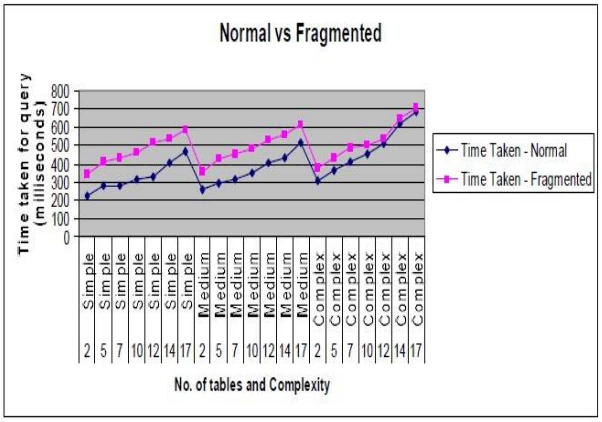
```
            ('CopyTableWithinDBS copies the data of the
            tables 'which is stored in the DatbaseServer as a
            hash table that can be accessed by the 'dynamic
            environment to restore the table lively 'during run
            access )
                    Continue;
                    }
            Else if (Table (n).Sensitivity = = Sensitive)
                    {
                    If (required Security = = critical)
                    {
                    DMA_Table [ ] dma_d_high = Split
                    (Table[n])
                    DMA_MapperTable dma_map_d =
            _CreateDMAMapperTable (Table[n], dma_d_high)
            DBS xy = get_UnusedDBS ()
            StoreTableInDBS (xy, dma_d_high)
            xy = get_UnusedDBS()
            StoreTableInDBS (xy, dma_map_d)
                    }
 }
Else if (Table (n).Sensitivity = = high)
{
DMA_Table [ ] dma_d = Split (Table[n])
If (required Security = = critical)
{
            Split Fine (dma_d)
}
DMA_MapperTable  dma_map_d = _
CreateDMAMapperTable (Table[n],dma_d)

DBS xy = get_UnusedDBS ( )
StoreTableInDBS (xy, dma_map_d)

'Let us consider number of DMA Tables as 'c'
DBS xy_sensitive = get_UnusedDBS ( )
 DBS xy_high = get_UnusedDBS ( )
For z=1 to c
If (dma_d[c].isDMA_Sensitive = = Low)
{
StoreTableinDBS (xy_sensitive, dma_d[c])
Else
 StoreTableinDBS (dbs_critical, dma_d[c])
}
For loop end
 }
For loop end
```

## V. RESULTS

With this setup, the performance of the info and therefore the integrity of the queries were tested. For this demand, the conventional info schema without fragmentation was setup in an exceedingly separate info. Initially, solely straightforward queries were made up of each the environments (like queries involving knowledge from a pair of or three master tables). The time variations between the 2 environments were vital with the fragmented surroundings overwhelming more time. The extra time taken by the fragmented surroundings is as expected. Then because the complexness of the queries enhanced, the time distinction became lesser, and this was largely attributed to the parallel querying of the sql server in an exceedingly single machine within the traditional surroundings with the parallel querying in multiple sql servers residing in numerous machines within the fragmented surroundings. The subsequent graph explains the time taken for various kinds of queries within the traditional and fragmented surroundings.



Performance between normal and fragmented environment

## VI. CONCLUSION

The result obtained from testing the two modules proves the efficiency of the model. The results also show that, even though the methodology is complicated, there is no adverse effect on the performance of the data communication and storage and typically very efficient for a cloud environment.

## REFERENCES

[1]. Navathe S., Karlapalem, K. and Ra, M. "A mixed fragmentation methodology for initial distributed database design," Journal of Computer and Software Engineering Vol. 3, No. 4 pp 395-426, 1995.

[2]. Balachandra, R., Ramakrishna, P.V. and Atanu, R. "Cloud Security Issues", In IEEE international Conference on Services Computing, pp. 517-520, 2009.

[3]. Cong, W., Qian, W. and Kui R., "Ensuring Data Storage Security in Cloud Computing", Cryptology ePrint Archive, Report, http://eprint.iacr.org/, (accessed: 18 October 2009), 2009.

[4]. Katja, H. and Ralf, S. "Distributed Database Systems-Fragmentation and Allocation," Cluster of Excellence MMCI, October 2010.

[5]. Jay, H. "What you need to know about Cloud Computing Security and Compliance", Gartner, Research, ID Number: G00168345, 2009.

[6]. Dr.V. Kiran Kumar, E. Hari Prasad, **"*Proposed Model for Ensuring More Security in Cloud by Data Fragmentation Method*"**, International Journal of Computer Sciences and Engineering, Vol.6, Issue.11, pp.391-394, 2018.

[7]. Dr.V.Kiran Kumar, E. Hari Prasa**d**, **"*Analysis of security as a service in cloud computing: a Review*"**, International Research Journal of Management Sociology & Humanities ,Vol.8,Issue.11 ,pp:119-127, 2017 www.IRJMSH.com

[8]. Fong E, Okun V (2007) Web application scanners: definitions and functions. In: Proceedings of the 40th annual Hawaii International conference on system sciences. IEEE Computer Society, Washington, DC, USA.

[9]. Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21.

[10]. Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security.http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007

## Authors Profile

***Dr. V.Kiran Kumar***, Working as a Associate Professor in the Dept of Computer Science, Dravidian Uniersity, Kuppam, Chittoor Dist. A.P. His Research area are Semantic Web, Web Technologies,

Programming.

***Mr. E.Hari prasad,*** Working asAcademic Consultant in the Dept ofComputer Science, Dravidian Uniersity,Kuppam, Chittoor Dist, A.P.

He is doing his research in domain of Cloud Computing in Dravidian University, Kuppam.