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 2, February 2015

Implementation of Secured Data Using Key Partitioning and Ida Method

K.G.S. Venkatesan[1], K.P.Kaliyamurthie[2]

Assistant Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India[1]

Professor & Head, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India[2]

ABSRACT: Generally the secret sharing and erasure coding-based approaches is used in distributed environment systems to ensure the confidentiality. To achieve this performance in data grid we provide data fragmentation approaches and it is combined with dynamic replication. In this paper, we consider data partitioning (both secret sharing and erasure coding) and dynamic replication in data grids, in which security and data access performance are critical issues. In a grid, effective way to improve data accessibility and data accessing efficiency is by data replication. This paper also propose an cryptographic infrastructure to protect privacy from users with administrative privileges. The cryptographic methods are done using the DES techniques. The replication is done using Dynamic replication algorithm. We use Simple Bottom-Up which is a method used for the dynamic replication. Data partitioning is done using IDA Algorithm and the encrypted keys are also partitioned for the security of the sensitive data in the distributed environment.

KEYWORDS : Secure data, IDA, Dynamic Replication, Data grids.

I. INTRODUCTION

Today, the management of the huge distributed and shared data resources efficient around the wide area networks becomes a significant topic for both scientific research and commercial application [5]. Essentially, talking about the Data Grid is an infrastructure which manages large scale data files and provides intensive computational resources across widely distributed communities. Many data grid applications are being developed or proposed, such as Global Information Grid (GIG) for both business and military domains. These data grid applications are designed to support global collaborations that may involve large amount of information, intensive computation, real time, or non real time communication [1]. Data Grids are mainly used to hosts building safety information and it also provides confidentiality of the critical information should be carefully protected in data grids. So, data grids provide accuracy, availability, reliability of data.

Data partitioning is a process which logically partition the data into segments which provides more easy accessible and maintenance of data. The partitions of sensitive data and distributing the shares across the storage device will provide both confidentiality and survivability of data in the distributed environment. Then, Information dispersal is a data-handling technique and extension made to forward error-correction schemes [7]. Moreover Information dispersal is becoming a new weapon in the battle for protecting information in the growing digital universe through innate properties supporting Survivability, confidentiality, integrity, and availability needs of end-users [8]. And a effective key management is also addressed by an Information dispersal method.

Considering the key management system it is mostly run in a single operating system. Whereas a dispersal can work on a diverse dispersed network Under such a configuration, any compromise would require attack. In some implementations, this could be considered a less common attack scenario than a single attack against a single platform used by the key management system. Thus the Information Dispersal methods are most useful when uploading a piece of information to a system where you want redundancy.
Moreover replication is a practical and efficient method to achieve high network performance in distributed environments [5] and it is frequently used to achieve access efficiency, availability and information survivability. In

the, Data grid, replication also plays a vital role to improve the performance of data intensive computing. Mainly replication methods can be classified as static and dynamic. Since this paper, considers the dynamic replication because the static replication, after a replica is created, it will exist in the same place till it is deleted manually by users or its duration is expired. Whereas, dynamic replication takes into consideration the changes of the Grid environments and automatically creates new replicas for popular data files [5]. Though replication can greatly help with information survivability and access efficiency, but it does not address security requirements. Replication is a strategy in which multiple copies of some data are stored at multiple site (Bernstein 1987).

So further for the security requirement the paper contains the data partitioning. And the secret sharing method which mainly included in this paper. Secret sharing is a method used for distributing a secret among the group of users, each of whom is allocated a share of the secret. The secret sharing techniques are used to maintain the confidentiality of the data. And the distributed secret can be reconstructed only when there are sufficient number of shares individual shares are of no use on their own [4]. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Secret sharing schemes assures confidentiality even if some shares are compromised.

So the main purpose of this paper is to provide security for the data in the data grids. So here the data’s are partitioned and the it is dynamically replicated over the distributed environment. Where it provides a security, confidentiality, integrity, and availability of sensitive information.

The existing work is carried out using java and the grid user details are maintained using MySql server. Since java is used because it platform independent, secure and provides high performance.

II. BACKGROUND

The existing system is mainly developed to provide availability, reliability and accessibility of data in data grids. This is achieved by the data replication.[1] Since it provides performance improvement it does not provide assurance for data security which is one major disadvantage in the distributed environment for the sensitive or critical informations in an untrust worthy environment. It provides difficult to place the replicas in distributed environment. Here the placement of replicas is done through heuristic algorithm.[2]

So, the proposed work presents a model for long-term storage and management of encrypted data in distributed environments. Furthermore, the paper outlines how this model is implemented to preserve the privacy for the sensitive or critical information in Grid-based collaborative computational infrastructure. This paper delineates a dependable security framework in overextended organizations. Throughout the assembly of this framework, organizations will encounter different degrees of data integrity and confidentiality, then for the data security in data grids, in this paper we consider, Dynamic replication and Information Dispersal with secret sharing were proposed.[4]

The dynamic replication algorithm determines when to perform replication, which file should be replicated, and where to place the replica [3]. The main purpose of the dynamic replication algorithm is to increase the data access performance from the perspective of the clients. An IDA method which is mainly used for the fragmentation of data, Files etc., It has different applications such Securing and reliable storage of informations in the distributed system. And the key partitioning is also done using the IDA method for managing the keys with more security.[8] Here we use a symmetric key cryptography method.[5]
The proposed system uses the following three algorithms :

- Information Dispersal Algorithm **(IDA).**
- Dynamic Replication Algorithm.
- Data Encryption Standard **(DES).**

Implementation of the proposed system is done using java. Since, it is platform independent and secure. And executed with the high performance.[6]

III. METHOD FOR INFORMATION DISPERSAL ALGORITHM

Information dispersal is a data-handling technique which is used to partition the data and stores in the distributed environment to provide security[7].

- An Information Dispersal Algorithm is a method to split a file F or data D into n pieces.
- It is dispersed in such a way that the file can be reconstructed from some predefined subsets of pieces.

Input: File(F)
Output: Partitions of files.
Method:
Dispersal(F,m,n).

- Let *F* be a data of size N in byte (|*F*|=N).
- *m* should be less than or equal to *n* ($m \leq n$).
- Dispersal(*F*, *m*, *n*):
  - splitting the data *F* with some amount of redundancy resulting in *n* pieces
- F_i ($1 \leq i \leq n$).
  - $|F_i|=|F|/m$
- Thus, the size of *F*, N, should be a multiple of *m*.

An IDA system by design is more resilient to device failure and data loss, which translates into an availability benefit, than a standalone encryption scheme.[9]
Example: Dispersal(*F*, *m*, *n*)

- |*F*|=32 bytes, *m*=4, *n*=8

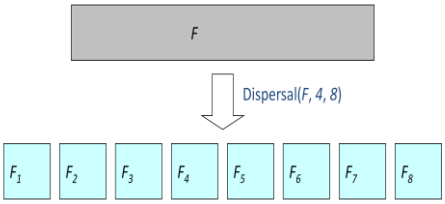

Fig 1: Information Dispersal.

IV. ALGORITHM FOR DYNAMIC REPLICATION

Replication is a practical and efficient method to achieve high network performance in distributed environments.[10] The dynamic replication algorithm determines when to perform replication, which file should be replicated, and where to place the replica. The main purpose of the dynamic replication algorithm is to increase the data read performance from the perspective of the clients [8].

This paper uses a Simple Bottom-Up(SBU) which is a method used in the dynamic replication algorithm.[11]

The basic idea of Simple Bottom-Up (SBU) is to create the replicas as close as possible to the clients that request the data files [5]. So, this will easily solve the replica placement problem.

Algorithm

Simple Bottom-Up(H,threshold)

- t ← Get-Time()
- A ← Sort-Dec(H,threshold)
- For all record r Є A do
- f ← r.fileID
- p ← Parent(r.nodeID)

```
while $p \neq$ root do
    if Exist-In(f,p) then
        Update-Ctime (f,p,t)
        break
    end if
    if Available-Spac(p,t) $\geq$ Size(f) then
        Replicate(f,p,t)
        break
    end if
    p $\leftarrow$ Parent(p)
end while
end for
```

Here the inputs given to the algorithm are the data file history and the threshold value which is easily used to distinguish the popular files according to the priority given to the file.[12] Then it needs to identify the creation time of the replicas, to record the current time at the commencement of the algorithm. Function Sort-Dec is the function. Where the records are sorted in descending order according to the *num of Accesses* and stored in the local variable array *A*.[13]

Therefore, array A contains the information of the popular files for individual clients, and these files are to be replicated on the suitable servers. For each record r in A. SBU gets its associated file ID f and the parent node ID p of the client. From the **while** loop it determines where the replica should be created [10], and the decision path is from the parent node of the client to the root. If a replica of file f exists in node p, then there is no need to replicate this file. The creation time of the replica is just updated to the current replication session time t by function update time, so that the replica of f in node p will be treated similarly as a newly created one [11]. Then, break the **while** loop and process the next record in array A .

If the replica of *f* does not exist in *p* and the available space of node *p* is large enough for file *f*. Replicate is called to create a new replica of *f* in node *p* and the creation time of the new replica will be set as *t*. Thereafter, the algorithm quits the **while** loop. Otherwise, *p* is modified to point to its parent node and the **while** loop is repeated.

V. DES TECHNIQUE

DES (encoding commonplace) may be a symmetric block cipher developed by IBM. The rule uses a 56-bit key to encipher/decipher a 64-bit block of information. The key's perpetually given as a 64-bit block, each eighth little bit of that is unnoticed. However, it's usual to line every eighth bit in order that every cluster of eight bits has associate odd variety of bits set to one.

This rule is best suited to implementation in hardware, most likely to discourage implementations in software package, that tend to be slow by comparison.[16] However, trendy computers square measure therefore quick that satisfactory software package implementations of square measure

DES is the most generally used symmetric rule within the world, despite claims that the key length is simply too short. Ever since DES was 1st declared, conflict has raged regarding whether or not fifty six bits is long enough to ensure security [6].

VI. EXPECTED RESULT

Providing security for the data's in the data grid with the combination of Information dispersal with secret sharing method and dynamically replicating the data. And also providing a cryptographic fly over for key partitioning and key management.

VII. CONCLUSION

This paper have combined both data partitioning and dynamic replication to achieve data survivability, security, availability and access performance in data grids. Cryptographic methods used for key management and key partitioning which access more security. IDA (Information Dispersal Algorithm) method developed for data partitioning & key partitioning and Dynamic Replication algorithm is used for dynamic replication. So, this provides the good access performance and security for the data's in data grid. The future work can be carried as the key management and key partitioning with asymmetric cryptosystem. And we can also apply these techniques to the multi-tier data grids.

IX. ACKNOWLEDGEMENTS

The author would like to thank the Vice-Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD **Dr. K.P. Kalyiamurthie**, **Dean CSE** **Dr. A. Kumaravel** of Bharath University, Chennai for their motivation and constant encouragement. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

[1] Manghui Tu, Peng Li and I-Ling Yen, "Secure Data Objects Replication in Data Grid" IEEE trans., vol. 7, no. 1, January-march 2010.

[2] Global Information Grid, Wikipedia.

[3] Jayaraman B., Valiathan G.M., Jayakumar K., Palaniyandi A., Thenumgal S.J., Ramanathan A., "Lack of mutation in p53 and H-ras genes in phenytoin induced gingival overgrowth suggests its non cancerous nature", Asian Pacific journal of cancer prevention : APJCP, ISSN : 13(11) (2012) PP. 5535-5538.

[4] K.G.S.Venkatesan and M.Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, pp. 75 – 80, April 2013.

[5] Kalaiselvi V.S., Saikumar P., Prabhu K., Prashanth Krishna G., "The anti Mullerian hormone-a novel marker for assessing the ovarian reserve in women with regular menstrual cycles", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(10) (2012) PP.1636-1639.

[6] K.Sashi and Dr.Antony Selvadoss Thanamani," Dynamic Replica Management for Data grid" IACSIT International Jou. and Technology, Vol.2, No.4, August 2010.

[7] Subhashree A.R., Shanthi B., Parameaswari P.J., "The Red Cell Distribution Width as a sensitive biomarker for assessing the pulmonary function in automobile welders- a cross sectional study", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(1) (2013) PP. 89-92.

[8]http://en.wikipedia.org/w/index.php?title=Secret_sharing&oldid=449314778.

[9] Ming Tang, Bu-Sung Lee1, Chai-Kiat Yeo, Xueyan Tang. "Dynamic replication algorithms for the multi-tier Data Grid" School of Computer Engineering, Nanyang Technological University. Future Generation Computer Systems 21 (2005) 775–790.

[10] Gopalakrishnan K., Prem Jeya Kumar M., Sundeep Aanand J., Udayakumar R., "Analysis of static and dynamic load on hydrostatic bearing with variable viscosity and pressure", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) PP.4783-4788.

[11] Kumaravel. A, 2013. "Cryptography Automata", Indian Journal of Science &.

[12] Srinivasan V., "Analysis of static and dynamic load on hydrostatic bearing with variable viscosity and pressure", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) PP.4777-4782.

[12]http://en.wikipedia.org/wiki/Data_Encryption_Standard.

[13] Rabin, Michael O. (1989). "Efficient dispersal of information for security, load balancing, and fault tolerance". Journal of the ACM 36 (2).

[14] K.G.S.Venkatesan and M.Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, pp. 778 – 785, 2013.

[15] Andrew Tytula," Peer-to-Peer File Sharing System using an Information Dispersal Algorithm" Technical Report, TR-02-87, Department of Computer Science, DEAS, Harvard University.

[16] Kumaravel.A, 2013. "Routing Algorithm over Semi-regular Tessellations", Xplore, pp:1180 – 1184.

[17].Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and

[18].Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014

[19].Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computerand Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014

[20].KannanSubramanian,FACE ECOGNITION USINGEIGENFACE AND SUPPORT ECTORMACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.

[21].Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013