A Review on Secure Methodology Fragmentation and Replication of data in cloud for Data Secrecy and Ideal Performance

Radhika Chavan, Prof. S.Y.Raut

Abstract— **Cloud computing is an emerging technology which attracts customers by giving offers like reduced cost, space and virtually unlimited dynamic resources for storage, computation etc. User shared the sensitive data over the cloud which gives rise to security issues in cloud computing. So, to protect user's data a secure methodology fragmentation and replication of data is used in this paper. The data is fragmented into pieces and then replicate them over the cloud nodes for maintaining the availability, performance level and backing up the data.T-coloring term is used here which is not giving any idea about locations of the fragments to an attacker. Centrality is used for node selection process.**

***Index Terms*—Cloud security, Fragmentation, Replication, Performance.**

I. INTRODUCTION

The concept of cloud computing has been evolving for more than 40 years. The term "cloud" comes from the telecommunications world of the 1990s, when providers began using virtual private network (VPN) services for data communication [2]. Now a day, people are connecting with cloud to get benefits from applications such as Email, instant messaging, business application software and web services on low cost [4].Cloud computing is a coalesce of many computing fields and became more popular in the recent years. Cloud computing provides computing, storage, services, and applications over the Internet. Moreover, cloud computing facilitates to reduce capital cost, decouple services from the underlying technology, and provides flexibility in terms of resource provisioning [5].

Now a day, people are connecting with cloud to get benefits from applications such as Email, instant messaging, business application software and web services on low cost. Cloud computing has three levels, Figure 1shows

1) Software as a service (SaaS),
2) Platform as a service (PaaS) and
3) Infrastructure as a service (IaaS) [17].

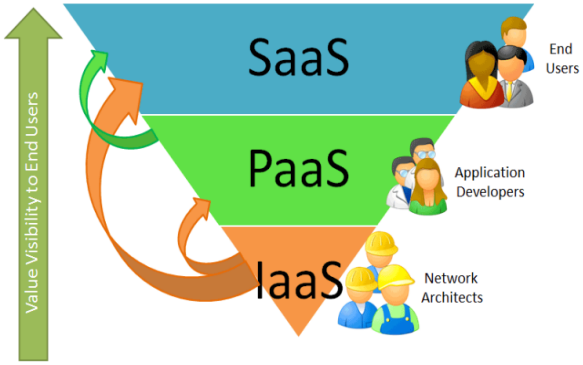

Fig 1: Cloud Services

For a cloud to be secure, it is necessary to be secure all of the participating entities. In any given system with multiple units, it must be equal that the highest level of the system ´ s security and the security level of the weakest entity [2]. The off-site data storage cloud utility requires users to move data in cloud's virtualized and shared environment that may result in various security concerns. Pooling and elasticity of a cloud, allows the physical resources to be shared among many users [1].

Security and performance together are needed for large scale systems. Therefore here in this paper we concentrate on together the issue of security and performance.

When file is not fragmented then if any successful attack happens then there will be single point failure. So it is important to fragment the file and increase the secrecy level. Replication improves the data retrieval time.

II. LITERATURE SURVEY

Providers such as Google and Amazon have the existing infrastructure to deflect and survive a cyberattack, but not every cloud has such capability. If a cybercriminal can identify the provider whose vulnerabilities are the easiest to exploit, then this entity becomes a highly visible target [2].

"An analysis of cloud computing security issues",Akhil Behl and Kanika Behl [7] investigating the vivid security issues and present a cloud security solution.

Radhika Chavan, *Computer Engineering, Pravara Rural Engineering College,Pune University,,Ahmednagar,India,9975662185.*
Prof.S.Y.Raut*, Computer Engineering, Pravara Rural Engineering College Pune University, Ahmednagar, India, 9689963062.*

ISSN: 2278 – 1323

"Secure Approach for Data in Cloud Computing", Bharti Dhote, A.M. Kanthe [8] described the method for data security, which is the major parameter of the quality of service. Paper includes data division, server misbehavior, checking integrity of data with the help of token pre-computation. The previous work does not support for dynamic insertion but here supports. This also ensures the data availability in case of communication link failure.

W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," [9] presented the data replication in cloud computing data centers with energy-efficiency and bandwidth consumption of the system. The results obtained guide the design of future data replication solutions.

D.Boru,D.Kliazovich,F.Granelli,P.Bouvry,andA.Y.Zomaya, "Energy-efficient data replication in cloud computing datacenters" ,[3] this paper reviews the topic of data replication in geographically distributed cloud computing data centers and proposes a novel replication solution which in addition to traditional performance metrics, such as availability of network bandwidth, optimizes energy efficiency of the system. Moreover, the optimization of communication delays leads to improvements in quality of user experience of cloud applications.

"Fragmentation and Data Allocation in the Distributed Environments", this paper focuses on fragmentation and data allocation. The fragmentation in a distributed database management system improves the level of concurrency and so automatically increases the system throughput for query processing. [10]

In the existing system the data compromise may occur due to attacks by other users and nodes within the cloud and the employed security strategy must also take into account the optimization of the data retrieval time.

In this paper we propose a secure methodology fragmentation and replication of data.

III. PRELIMINARIES

1] Cloud Security

With the increasing popularity of cloud computing, technology experts along with security specialists are always trying different standards to secure their infrastructure in cloud locking them from outside networks. As of today there are no universal perfect solution for cloud security. Cloud devices are likely to attacks from cyber criminals.

Data privacy and data protection are major concerns for any security expert in an organization regarding their infrastructure in the cloud. Data may not get stored in the same system within a public or community cloud, resulting in multiple concerns legally. As of today, there are no safety standards and regulations stated by the providers for the customers to ensure sufficient security. Virtualization security, identity and access management, threat management, content security, and data privacy need to be given priority and require more focus.

Data encryption all through the lifecycle can be one method of data protection. In cloud we are not known where our data resides, what we know is these are shared servers. Our information is shared among cloud nodes. So the chances are that the data might be leaked. It is important to have a strong security strategy for giving relief. This can curb data leakage and protect your valuable data [11], [9].

2] Data Fragmentation

In large –scale system the security depends upon the whole system as well as the single node of a system. If the file is attacked by an attacker then there will be single point failure. So to avoid this data division or fragmentation technology is used. Fragmentation can increase an attacker's effort. In a fragmentation schema file f is split into n fragments, all fragments are signed and distributed to n remote servers, one fragment per server. The user can reconstruct file f by accessing m fragments arbitrarily chosen. [12].

3] Replication

The tremendous growth of cloud computing enabled the deployment of immense IT services that are built on top of geographically distributed platforms and offered globally. For better reliability and performance, resources are replicated at the redundant locations and using redundant infrastructures. , Number of data replication methods have been proposed to address an exponential increase in Internet data traffic and optimize energy and bandwidth in datacenter systems [3]. Availability is assured by replication, without encryption, with the idea that files can be encrypted by the client before storing when confidentiality is an issue [12].

Data replication means maintaining multiple copies of same data on same server or on different servers. If data is present at one site only, then it will be single point failure. Server will face a heavy load balancing condition and system performance. Also if that site fails, all that data will be lost, this is also a serious concern. Replication is necessary for maintaining the availability, performance level, backing up the data and also for balancing load [15].

4] T-coloring

T-coloring is basically used for channel assignment, such that the channels are separated by a distance to avoid interference. Suppose we have a graph G= (V, E) and a set T containing non-negative integers including 0. The T-coloring is a mapping function f from the vertices of V to the set of non-negative integers, such that $| f(x) - f(y) | \notin T$, where$(x, y) \in E$. The mapping function f assigns a color to a

ISSN: 2278 – 1323

vertex. In simple words, the distance between the colors of the adjacent vertices must not belong to T [18].

5] Centrality Measures

The centrality of a node in a graph provides the measure of the relative importance of a node in the network. The objective of improved retrieval time in replication makes the centrality measures more important.[18].

IV. PROPOSED SYSTEM ARCHITECTURE

From the survey of cloud security, both security and performance are very critical for the large-scale systems. So, in this paper, we concentrate on the issue of security and performance. We present here fragmentation and replication methodology for data secrecy and ideal Performance.

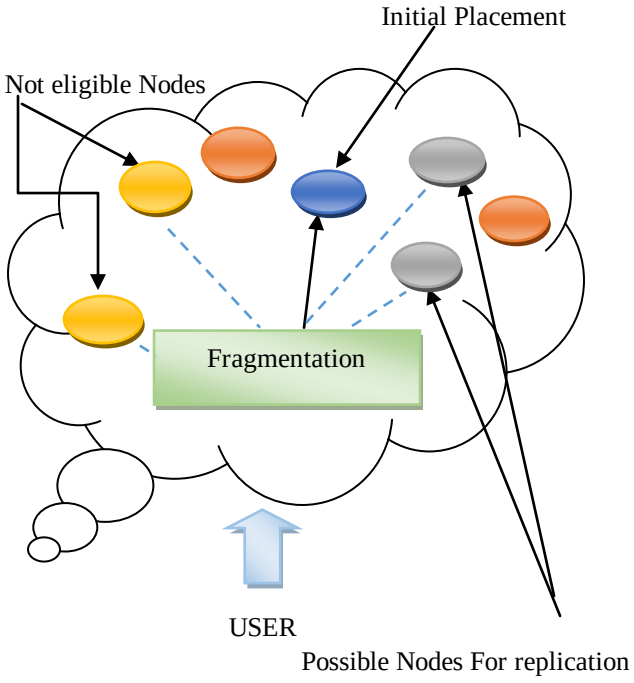

Fig 2: Fragmentation and Replication Methodology

The figure 2 shows this methodology. The Fragmentation of a file into fragments is done which is based on a given user criteria such that the individual fragments do not contain any sensitive data. Each of the cloud nodes contains a different fragment which automatically increases the data security. A successful attack on a single node will never leak any valuable information. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not nearby and are at certain distance from each other. The node separation is done by using the term T-coloring. To improve data retrieval time, the nodes are selected based on the centrality measures that ensure an improved access time.

In this paper the selection of the nodes is performed in two phases.

1. The initial placement of the fragments.
2. The nodes are selected for replication.

Existing System used cryptography to ensure the authentication, integrity and confidentiality .But it takes too time for processing. The scheme which combines the replication problem and with security, access time improvement seen. But the data files are not fragmented and handled as a single file. So single point failure concerns a new problem.

Proposed System Work Flow:

So here in proposed System the data is fragmented and replicate to achieve both secrecy and ideal performance. The Centrality and T-coloring method is used for node selection so it prohibits the single point failure.In this methodology, we propose to store the fragments on different nodes. After the fragmentation of file it will be used for replication. The fragments are distributed such that no node in a cloud holds more than a single fragment, so that even a successful attack on the node then also no valuable information leaks. This methodology uses controlled replication where each of the fragments is replicated only once in the cloud to improve the security. Although, the controlled replication does not improve the retrieval time to the level of full-scale replication, it significantly improves the security. Firstly, in this methodology user sends the data file to cloud. 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 node, and (c) second cycle of nodes selection for fragments replication. The cloud manager maintains 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 [18].

By using this method we can secure the data and also increases the performance level.

CONCLUSION

Cloud computing is the todays foremost technology which attracts users by providing tremendous beneficial services but the sensitive data of users shared which gives rise to security concerns. This paper proposed work gives the data secrecy as well as ideal performance. The user data is fragmented in such a way that no valuable information is revealed to an attacker and then replicated them over nodes. T-coloring and centrality plays vital role in proposed methodology. Availability, data access time and high secrecy maintained by this methodology.

ISSN: 2278 – 1323

REFERENCES

[1] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.

[2] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[3]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.

[4] Issa M. Khalil ,Abdallah Khreishah,Salah Bouktif, Azeem Ahmad , "Security concerns in cloud computing", 10th International Conference on Information Technology: New Generations , 2013.

[5] A. R. Khan, M. Othman, S. A. Madani, S. U. Khan, "A survey of mobile cloud computing application models," IEEE Communications Surveys and Tutorials, DOI: 10.1109/SURV.2013.062613.00160.

[6] Kalpana Batra,Ch.Sunitha,Sushil Kumar ,"An Effective Data Storage Security Scheme For Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 1, Issue 4, 2013.

[7] Akhil Behl and Kanika Behl,"An analysis of cloud computing security issues", IEEE 2012.

[8] Bharti Dhote, A.M. Kanthe ,"Secure Approach for Data in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 64– No.22, February 2013.

[9] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," In 44th Hawaii IEEE International Conference onSystem Sciences (HICSS), 2011, pp. 1-10.

[10] Nicoleta - Magdalena Iacob (Ciobanu),"Fragmentation and Data Allocation in the Distributed Environments",Annals of the University of Craiova, Mathematics and Computer Science Series Volume 38(3), 2011.

[11] Dilraj D N and Jerin Joy," Need for Cloud Security", by marlabs .

[12] 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.

[13] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez,"An analysis of security issues for cloud computing",Journal of Internet Services and Applications,2013.

[14] John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing",Copublished By The IEEE Computer And Reliability Societies. July/August 2009.

[15] Manisha Kalkal*, Sona Malhotra,"Replication for Improving Availability & Balancing Load in Cloud Data Centres ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[16] Dan C. Marinescu,"Cloud Computing: Theory and Practice",Computer Science Division Department of Electrical Engineering & Computer Science University of Central Florida, Orlando, FL 32816, USA,November 10, 2012.

[17] M. Hogan, F. Liu, A.Sokol, and J. Tong, "NIST cloud computing standards roadmap," NIST Special Publication, July 2011.

[18] Mazhar Ali, Kashif Bilal, Samee U. Khan, Bharadwaj Veeravalli, Keqin Li, and Albert Y. Zomaya ,"DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE Transactions On Cloud Computing.,in press.

Radhika Chavan received B.E.(I.T.) degree from Shivaji University,M.E. Computer Engineering Student.

Prof. S.Y.Raut received M.E. degree and Assistant Professor at PREC,Loni.

ISSN: 2278 – 1323