International Journal of Engineering Research and Development
***e**-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com*
Volume 3, Issue 12 (September 2012), PP. 10-13

Design a Reliable Cloud computing strategy for efficient data accessibility and resource sharing

S.Bharanisethupandian[1], Dr.M.Sumathi[2]
[1]*Assistant Professor, Department of MCA, SOURASHTRA COLLEGE, Madurai, Tamilnadu, India*
[2]*Assistant Professor, Department of Computer Science, Sri Meenakshi Government College for Women, Madurai, Tamilnadu, India*

Abstract*—Cloud computing is the modern day hymn. Efficient Data accessibility in cloud is a tedious process in Multi stored architecture. This architecture was used in most of Big B organization. The purpose of this architecture is to satisfy the user in the form of data accessibility and to access the data in secure tunnel. The nature of multi stored architecture is used to classify the data in terms of accessibility, classifying user, and the required data. But the unanswered questions come in the aspects of efficient data retrieval. In this work, we have focused on efficient data accessibility strategy among several thousand nodes or systems and to share and retrieve data with its accessibility path (zone). This also focuses on efficient resource sharing which satisfy the need. Via this work we have also focus on resource sharing and its efficient utilization. The cloud itself reduces complexity via SAAS architecture but how far the data reduce complexity in terms of accessible rate. This architecture works as public cloud were accessibility plays a major role. The result put over here will reduce the data accessible rate in public cloud. Though this work focus on public cloud it also deals with hybrid cloud since it combine more than a public cloud.

***Keywords*—Cloud computing, public cloud, cloud deployment, Hybrid cloud**

I. INTRODUCTION

The advent of network model and the core concept of distributed system were well addressed in cloud computing. Rightly we can address that cloud computing is the mixture of both the concept. Despite cloud computing also address data accessibility in multi diversified networks irrespective of its locations. The data accessible rate in individual network system will be fast enough in trade off with normal networked model. But as the network grows rapidly the advantage faced in individual cloud invokes reverse strategy.

Cloud is a well known application for commercial aspects. Since the entire networked model does the same, cloud in its own terms its different based on its kind. Internet is a diversified medium which connects all the networked systems for sharing the data. It has its own merits and demerits for doing it so. Hence Internet is also a commercial medium. The connection thus formed with the help of internet as backbone service; there are so many questions to answer what internet actually demands? Internet acts as a communication medium for data sharing and it lost connection to explore utilization. Hence private organization want to address this points hence cloud computing were served as an answer for this.

Cloud computing does the role of data accessibility and its utilization. The cloud can be off three types; this would also be referred as its deployment model. They were Private, Public, and Hybrid. Were as private is provided by an organization for sharing its resources and itself measures its utilization need, public cloud is provided by third party who shares its resources accessed by registered customers, Hybrid is combination of private and public or within itself. All these three deployment model address data accessing date and it's deploy ability [1].

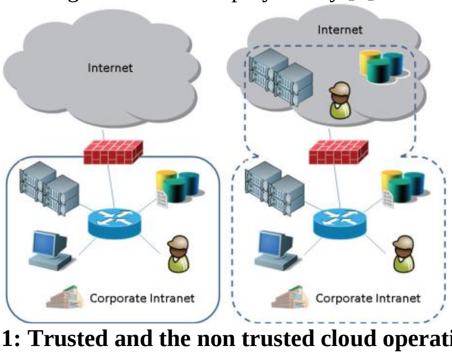

Fig 1: Trusted and the non trusted cloud operations

The Cloud architecture will never comprise in privacy [2]. This concept will be very well addressed in terms of security issues [3]. Perhaps the security issues will be more in terms of public cloud were data accessing is the primary task. The utilization of the data is the underline fact as the cloud speaks in volume of data. Even cloud architecture is modeled to do an operation based on accessibility it should also address utilization of data along with the said operations.

The point of trust is another exemplar to be addressed very seriously. The service provider though focuses on the data accessibility metrics but they negotiate with the term security. The security in cloud computing is a great challenges and it provides ample of source for the researchers to provide their own solution to address this issue. The collision of agreement between the third party service providers and user leads to security breaches. Though this area which is to be addressed very seriously in later half, but the primary task in this work will focus on data accessibility and the effective utilization of resource. If neither of these terms not addressed properly then cloud operation will fail in its services and its lays non dependable.

The Fig 1 above depicts the cloud and its dependability. If a cloud said to be deployed in any of the three models then it should address the privacy issues by incorporating with security measures.

II. REVIEWED ARTICLES

The work of Bertino, E [2] addresses Privacy-preserving Digital Identity Management for Cloud Computing in its transcripts on IEEE Data Engineering Bulletin. Here in this paper it focus on how privacy preservation were done on cloud based on digital identify management.

The work of Imam [5] focus on news challenges and issues in cloud computing. This paper addresses all the issues in cloud starting from the technology, privacy and security, and technical challenges in cloud.

The aspects of legal challenges in cloud come from Angela mari [2009] who address the issues of cloud privacy and its dependability.

The work of Gardner gives stand alone exposure to identify security risk in cloud computing. It also works with the provider access since it does not convey what to be protected as in the aspect of public cloud.

The factor influenced by Gardner finding address

- Internal risk assessment
- Legal and regulatory services in cloud
- Transparency in data access

All these factors should be balanced with security services provides by the cloud stack.

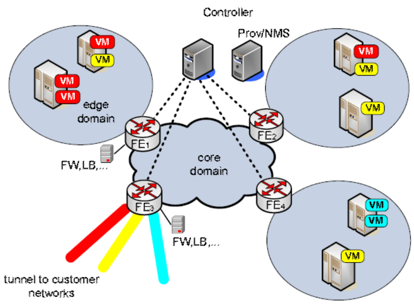

Fig 2: Elastic Cloud

The figure displayed is elastic cloud architecture. The objective of elastic cloud will eradicate the means of scalability. It’s a data centric architecture. It will partition the data based on access, aggregation, and its core. This architecture implements VLAN. The general aspect of this architecture partitioned the data using FE (Forwarding element and CC (Center controller).

The gateway of data communication works with FE between different processing elements and it’s been controlled by CE. This elastic cloud was very well addressed for its security services known as SEC- Secure Elastic cloud.

III. EXISTING WORK

Data accessibility in cloud was addressed in PbD by Min-Yu Hsueh, Toshikazu Fukushima, Jun Du, and Takahiro Sugiyama. This concept deals with the Data accessibility and security issues in cloud computing. The strategy deployed in this work focus on cloud computing paradigm and works based on the defined principles.

The existing work also addresses Data and its security. The needs for security also mend for fixing the security issues ensuring data and its security. The statement of problem works in cloud computing deployment models. The way how the works is deployed necessarily ensures the possibilities of cloud stack.

This works also imprints on data security schemes. Based on this scheme the architecture was fine tuned as per the need for security.

Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service and many others.

The next phase of virtualization is cloud computing. The Cloud computing paves way for virtualization by sharing the hardware resources equally among application. How effectiveness is the virtualization as fast as the data access can be.

Virtualization works as the hardware were away from the server software. This concept also involves OS, application and its services. Based on services the virtualization data accessibility was implemented and accordingly the service. The concept of virtual server can be served with one or more host.

The areas to be addressed here are based on variable demands like batch processing, Forbes, provoking with unknown demands. These all demands were addressed with efficient data accessing rate despite number of processing elements increased in size.

The advantage over the demerits is not being affiliated to any hard ware resources that to be bought for accessing cloud (private and public).

IV. PROPOSED WORK

This work addresses on the data accessibility by the cloud stack. The simulation result of the cloud stack shows the result of data accessibility based on time, its complexity.

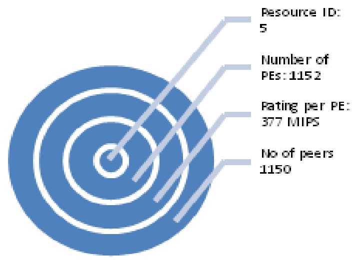

Fig 3: Cloud stack

The stack show above will provide necessary information about the Resource ID, Processing Element identified as the system uses cloud services. The simulation results were measure in terms of MIPS and actually it's 377 MIPS and the number of peers used in the evaluation process is 1150.

Message	Send Time	Acknowledgement	Process Completion time	No of Public/ Private Cloud
0	5	1454896	1654896	500
1	15	1.21E+00	2.21E+07	350
2	25	3594528	3894528	300

Table 1: Data accessibility in Private and Public cloud

Fig 4: Simulation result

The above mentioned is the simulation result evaluated from cloudsim. This result shows the classification of processing element based on its accessibility efficiency. The efficiency of the data accessibility was measured using send time which is the data transfer time with acknowledgement time. It's also focused on message capabilities based on the send time, acknowledgement time by the processing element. The resource id is the individual public or private cloud. Each and every public and private cloud were deployed in this resource id. We have taken 5 resource id and its data accessing possibilities.

This result also address scalability by with transparency is maintained. Further this also addresses location independence of each and every cloud.

V. CONCLUSION AND FUTURE WORK

In this work we have dealt with cloud and its data accessing rate. We have worked on the scalability of the cloud were the location transparency is maintained. The result works well for data accessing rate and the problems arises in the name of location transparency. Since every aspect of data is transparent there arise the issues of security breech. The graph mentioned above addressed the send time and acknowledgement of individual processing element based on data accessed rate and it proven to be effective as per the indication shows as positive acknowledgement and processing flow. In our future work we have planned to implement security issues along with the data services and try to prove its significance.

REFERENCE

[1]. Altman, I. (1997) Privacy Regulation: Culturally Universal or Culturally Specific. Journal of Social Issues, 33:3, p. 66-84.

[2]. Bertino, E. (2009) Privacy-preserving Digital Identity Management for Cloud Computing. IEEE Data Engineering Bulletin, 32, p. 21-27.

[3]. Brodkin, J. (2008) Seven Cloud-Computing Security Risks. *InfoWorld*. Available online at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[4]. Cavoukian, A. (2008) Privacy in the Clouds – A White Paper on Privacy and Digital Identity: Implications for the Internet. Information and Privacy Commissioner of Ontario. Available online at:http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=748

[5]. Imam, A. (2009) Cloud Computing: Prospects and Challenges. Newcastle University Business School.

[6]. Ferguson,(2008, October) *The future of cloud computing* eWeek,Vol. 25 Issue 30, p17-17, 1p Retrieved November 26, 2008 from Business Source Premier database

[7]. Global Environment for Network Innovations. *http://www.geni.net*, 2006.

[8]. T. Wood, P. Shenoy, K.K. Ramakrishnan, and J. Merwe, The Case for Enterprise-Ready Virtual Private Clouds. In *HotCloud*, 2009.

[9]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In *CCS*, 2009.

[10]. F. Hao, T.V. Lakshman, S. Mukherjee, and H. Song, Enhancing Dynamic Cloud-based Services using Network Virtualization, In *VISA*, 2009.

[11]. R. Mysore, A. Pamboris, N. Farrington, N. Huang, P. Miri, S. Radhakrishnan, V. Subramanya, and A. Vahdat, PortLand: A Scalable Fault-Tolerant Layer 2 Data Center Network Fabric. In *ACM SIGCOMM*, 2009.