© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Infrastructure as a Service Based Data Transfer in Cloud Server during Disaster

S. Rajarajeswari, Dr. L. M. Nithya

Department of Information Technology, SNS College of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Remote monitoring system is growing rapidly based on the growth of supporting technologies. The problem that may occur in remote monitoring are such as i) the number of objects to be monitored and how fast ii) how much data to be transmitted to the data centre for proper processing. The study proposes on cloud computing infrastructure as processing centre in the remote sensing data. This study focuses on the situation for sensing the environment condition and disaster early detection. The proposed method keeps on tracking the database architecture for data transfer with remote monitoring system which detects whenever destruction occur the database architecture will transfer the database to the concern location which is assigned by the administrator. The main objective of this project is to enhance the data storage security and secured data transfer during disaster. So that IaaS (Infrastructure as a Service) methodology will be implemented here. This is to provide prior security for the storage devices during malware attacks and also during disaster. With this process data loss will not occur at any cost and the proposed method is based on IP conflict method in which roll back process is possible so that the proposed method will show the data up to last minute transaction. The proposed method enhances the data storage security during malware attacks, transfers the data safely during disaster and it is cost effective.

Keywords: Cloud computing, data storage security, secure data transfer, IaaS (Infrastructure as a Service).

I. INTRODUCTION

Cloud computing is a general term that involves for anything in delivering hosted services over the Internet. Many definitions have been presented for cloud computing [2, 3, 4]. These services are further divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). As per survey most of the banking server and data centers are placed in metropolitan cities, most of the metropolitan cities are in sea shore. For example in India: Chennai, Mumbai and etc. Even in USA New York city is in sea shore only. For last 10 years tsunami destroyed the cities 3 times. In some case data centers may get destroyed due to earth quake or in flood. In our project we are finding out a solution to safe hand the data centers and banking servers. The main objective of this project is to enhance the data storage security and secured data transfer during disaster. So that IaaS (Infrastructure as a Service) methodology will be implemented here.

This is to provide prior security for the storage devices during malware attacks and also during disaster. Basically massive NC Cloud computation power and storage capacity of the cloud computing systems allow scientists to deploy computation and also data intensive applications without infrastructure investment, where the large application data sets can be stored in the cloud. Based on the pay-as-you-go model [1], storage strategies and benchmarking approaches have been developed for cost-effectively storing a large volume of generated application data sets in the cloud network. However, they are either insufficiently cost-effective for the storage to be used at runtime. In this paper, toward NC Cloud achieving the minimum cost benchmark, we propose a novel highly cost-effective and practical storage strategy that can automatically decide whether a

generated data set should be stored or not at runtime in the cloud.

The main focus of this strategy is the local-optimization for the tradeoff between computation and storage, while secondarily also taking users preferences on storage into consideration. Both theoretical analysis and simulations conducted on random data sets as well as specific real world applications with Amazon's cost model [5] show that the cost-effectiveness of our strategy is close to or even the same as the minimum cost benchmark and the efficiency is very high for practical runtime utilization in the cloud. In added with the remote monitoring system will keep on tracking the database architecture for the data transfer. Whenever destruction occur the data base architecture will transfer the database to the concern location assigned from the admin. So that data base can be saving exactly with the last fine transaction. Here data loss will not occur at any cost. This method is based on IP conflict procedure. So that roll backing process can also be possible. Using the same procedure of IP conflict method and this method will shows the data up to last minute transaction.

II. METHODS AND MATERIAL

A. Literature Survey

In this chapter, various methods that had been implemented in the previous work have been discussed. The methods are based on disaster recovery analysis. Disaster recovery analysis refers to the use of recovering the data during disaster. Early work in this area is done at Disaster management, Sensor network, Energy efficient, Disaster recovery, Wireless sensor network, Replication, and Backup. Disaster recovery is a special task whose objective is to recover the data during disaster. Quantum Cryptography has been used for secures the data and database during the time of data transfer. A Highly Practical Approach toward achieving minimum Storage Cost for data sets in [6] states a novel highly cost effective and practical storage strategy. An Infrastructure as a Service (IaaS)-based cloud computing is developed to identified stakeholders, and suggests for security research and development [7]. Recent disasters in Japan and Haiti [10, 11] have shown the effect that they can have on people, property, and the economy in that area. An energy efficient mechanism [14] is presented for processing spatial queries on wireless sensor networks to detect dangers in disaster situations by proposing mechanism manipulates queries with regions of interest having irregular shapes.

Cloud Based Disaster Recovery Mechanisms

Mohammad Ali Khoshkholghi1, Azizol Abdullah1 [12] have discussed about Disaster recovery is a persistent problem in IT platforms. This problem is more crucial in cloud computing, because Cloud Service Providers (CSPs) have to provide the services to their customers even if the data center is down, due to a disaster. In the past few years, researchers have shown interest to disaster recovery using cloud computing, and a considerable amount of literature has been published in this area. However, to the best of our knowledge, there is a lack of precise survey for detailed analysis of cloud-based disaster recovery. To fill this gap, this paper provides an extensive survey of disaster recovery concepts and research in the cloud environments. We present different taxonomy of disaster recovery mechanisms, main challenges and proposed solutions. We also describe the cloud-based disaster recovery platforms and identify open issues related to disaster recovery

Disaster Risk Reduction and Management

Irasema Alcántara-Ayala (Mexico), Daniel Baker (USA) [8] have discussed about Natural hazard events lead to disasters when the events interact with exposed and vulnerable physical and social systems. Despite significant progress in scientific understanding of physical phenomena leading to natural hazards as well as of vulnerability and exposure, disaster losses due to natural events do not show a tendency to decrease. This tendency is associated with many factors including increase in populations and assets at risk as well as in frequency and/or magnitude of natural events, especially those related to hydro-meteorological and climatic hazards. But essentially disaster losses increase because some of the elements of the multidimensional dynamic disaster risk system are not accounted for risk assessments.

A comprehensive integrated system analysis and periodic assessment of disaster risks at any scale, from local to global, based on knowledge and data/information accumulated so far, are essential

scientific tools that can assist in recognition and reduction of disaster risks. This paper reviews and synthesizes the knowledge of natural hazards, vulnerabilities, and disaster risks and aims to highlight potential contributions of science to disaster risk reduction (DRR) in order to provide policy-makers with the knowledge necessary to assist disaster risk mitigation and disaster risk management (DRM).

B. Problem Definition

Even thou grid computing having some excellent disaster management tools, it will not perform up to the range of cloud service provider. There is still the absence of the cloud service provider. IP conflict is not available so that routing became tedious during data transfer. No prior admin available for assigning the rollback of database. So this architecture may face data loss at any time. This can't be recovered. In case of hacking or instruction of database system will response for the hacker or intruder for deletion of the data. This is because at that time of hacking the hacker or intruder may also act as an admin. Due insufficient bandwidth there are no possibilities to transfer huge number of data at a same time. Data transfer may allow according to the dead lock rules. It is much time consuming.

C. Proposed System

Cloud computing offers an attractive alternative to traditional disaster recovery. "The Cloud" is inherently a shared infrastructure: a pooled set of resources with the infrastructure cost distributed across everyone who contracts for the cloud service. This shared nature makes cloud an ideal model for disaster recovery. Even when we broaden the definition of disaster recovery to include more mundane service interruptions, the need for disaster recovery resources is sporadic. Since all of the organizations relying on the cloud for backup and recovery are very unlikely to need the infrastructure at the same time, costs can be reduced and the cloud can speed recovery time.

While the cloud offers multiple benefits as a disaster recovery platform, there are several key considerations when planning for the transition to cloud-based business resilience and in selecting your cloud partner. These include:

- Portal access with failover and failback capability
- Support for disaster recovery testing
- Tiered service levels
- Support for mixed and virtualized server environments
- Global reach and local presence
- Migration from and coexistence with traditional disaster

Cloud computing offers a compelling opportunity to realize the recovery time of dedicated disaster recovery with the cost structure of shared disaster recovery. However, disaster recovery planning is not something that is taken lightly; security and resiliency of the cloud are critical considerations. Smart Cloud Virtualized Server Recovery is hosted within the cloud network of Resiliency Centers, so clients can feel confident that cloud disaster monitoring system is helping to protect their sensitive data. Second, there is no need to rush in clients can start to work with Smart Cloud Virtualized Server Recovery with as few as five virtual machines under managed contract—so getting started is easier and relatively risk free.

Representative network architecture for CLOUD data storage is in three different network entities can be identified as follows:

- User: users, who have data to store in the CLOUD and rely on the CLOUD for data computation, consist of both individual consumers and organizations.
- CLOUD Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed CLOUD storage servers, owns and operates live CLOUD computing systems.
- Third Party Auditor (TPA): an optimal TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of CLOUD storage services on behalf of the users upon request.

Security threats faced by CLOUD data storage can come from two different sources. On the one hand, a CSP can be self-interested, un-trusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data

loss incident due to management errors, Byzantine failures and so on. On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of CLOUD data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSP for a certain period.

Advantages of the Proposed System

- Because of the availability of cloud service provider the cloud disaster remote monitoring system can be executed successfully.
- High data transfer is possible due to the availability of higher bandwidth. So that while disaster data loss will not occur.
- A highly prioritized database is available in order to prior up the data base tables during the time of destruction.
- The system will not response for the hacker or the intruder, this is because the data base will be embedded with the IP conflict procedure. So that authorized IP can do the read, write and update permission of the database. Other persons will be considering as hackers.
- More data accuracy can be provided during roll back process.
- Can provided unlimited bandwidth for data transfer.
- No time consuming.

Randomized malware process in quantum cryptography
Classical part

1. Pick a random number a < N
2. Select colours from N
3. Compute gcd (a, N). This may be done using the Colour quantum method.
4. If RGB (a, N) ≠ 1, then there is a nontrivial factor of N, so we are done.
5. Otherwise, use the period-finding subroutine (below) to find r, the period of the following function: $f(x) = a^x \mod N$, i.e. the order r of a in $(\mathbb{Z}_N)^\times$, which is the smallest positive integer r for which $f(x+r) = f(x)$ or $f(x+r) = a^{x+r} \mod N = a^x \mod N$ to database value.
6. If r is odd, no colour match, go back to step 1.
7. If $a^{r/2} \equiv -1 \pmod N$, go to application
8. RGB ($a^{r/2} \pm 1$, N) is a nontrivial factor of N. We are done.

Quantum Part: Period-finding subroutine (Malware Attacks)

The quantum circuits used for this algorithm are database designed for each choice of N and the random a used in f(x) = a^x mod N. Given N, find Q = 2^q such that $N^2 \leq Q < 2N^2$, which implies $Q/r > N$. The input and output qubit registers need to hold superpositions of values from 0 to Q − 1, and so have q qubits each. Using what might appear to be twice as many qubits as necessary guarantees that they are at least N different x which produce the same f(x), even as the period r approaches N/2 and database corruptions.

Proceed as follows:

1. Initialize the registers to $Q^{-1/2} \sum_{x=0}^{Q-1} |x\rangle\,|0\rangle$

where x runs from 0 to Q-1. This initial state is a superposition of the corresponding database of Q states.

2. Construct f(x) as a quantum function and apply it to the above state, to obtain $Q^{-1/2} \sum_x |x\rangle\,|f(x)\rangle$.

   This is still a superposition of Q states.
3. Apply the quantum Fourier transforms to the input register. This transform (operating on a superposition of power-of-two Q = 2^q states) uses a Q^{th} root of unity such as $\omega = e^{2\pi i/Q}$ to distribute the amplitude of any given $|x\rangle$ state equally among all Q of the $|y\rangle$ states, and to do o in a different way for each different x:

   $U_{QFT}\,|x\rangle = Q^{-1/2} \sum_y \omega^{xy}\,|y\rangle$.

   This leads to the final state $Q^{-1} \sum_x \sum_y \omega^{xy}\,|y\rangle\,|f(x)\rangle$.

   This is a superposition of many more than Q states, but many fewer than Q^2 states. Although there are Q^2 terms in the sum, the state $|y\rangle\,|f(x_0)\rangle$ can be factored out whenever x_0 and x produce the same value.

   Let $\omega = e^{2\pi i/Q}$ be a Q^{th} root of unity,

r be the period of f,
x_0 be the smallest of a set of x which yield the same given f(x) (we have $x_0 < r$), and
b run from 0 to $\lfloor (Q - x_0 - 1)/r \rfloor$ so that $x_0 + rb < Q$.

Then ω^{ry} is a unit vector in the complex plane (ω is a root of unity and r and y are integers), and the coefficient of $Q^{-1}|y\rangle|f(x_0)\rangle$ in the final state is

$$\sum_{x:\, f(x)=f(x_0)} \omega^{xy} = \sum_b \omega^{(x_0+rb)y} = \omega^{x_0 y} \sum_b \omega^{rby}.$$

4. Each term in this sum represents a different path to the same result, and quantum interference occurs constructive when the units vectors ω^{ryb} points in nearly the same direction in the complex plane, which requires that ω^{ry} point along the positive teal axis.
5. Perform a measurement. We obtain some outcome y in the input register and in the output register. Since f is periodic, the probability of measuring some pair y and is given by
$$\left| Q^{-1} \sum_{x:\, f(x)=f(x_0)} \omega^{xy} \right|^2 = Q^{-2} \left| \sum_b \omega^{(x_0+rb)y} \right|^2 = Q^{-2} \left| \sum_b \omega^{bry} \right|^2 .$$
Analysis now shows that this probability is higher, the closer unit Vector ω^{ry} is to the positive real axis, or the closer yr/Q is to an integer. Unless r is a power of 2, it won't be a factor of Q.
6. Perform Continued Fraction expansion on y/Q to make an approximation of it, and produce some c/r′ by it that satisfies two conditions for the location identifiers
A: r′<N
B: |y/Q - c/r′| < 1/2Q.
By satisfaction of these conditions, r′ would be the appropriate period r with high probability.
7. Check if f(x) f(x + r′) ⟺ If so, we are done.
8. Otherwise, obtain more restore for r by using values near y, or multiples of r′. If any attacks works, we are done.
9. Otherwise, go back to step 1 of the subroutine.

D. Result Analysis:

Hackers can be identified in the cloud with the available details in figure 1.

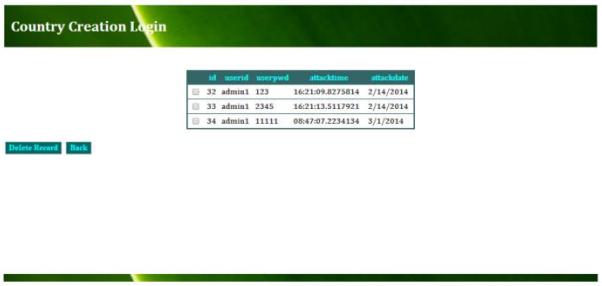

Figure 1 : Hackers List

The page displays the hackers list. If anyone tries to hack the details, it displays the hacker's details in the creation login page.

In our experiment we found that cluster running in virtual environment is significantly perform low than the one running is physical environment (physical machine), and other factor might affect the performance but in our study we focused on the environment effect which is 68% affecting the performance of the cluster.We prepared a comparison chart between the performances of existing and our current method in both environments. The above given figure represents the performance difference between the performances running in different environments. From these results, we observe that performance, confirmed that the virtual cluster performance is significantly lower than the cluster running on physical machine due to the overhead of the virtualization on the CPU of the physical host. The factors, which affect the performance (RAM size, network bandwidth), were considered in our experiment. However, our study was directed towards the effect of environmental factors on the performance.

III. RESULTS AND DISCUSSION

A comparison chart is drawn on comparing the Recovery Time and Cost with the Quantum cryptography and other techniques as Cloud Standby for retrieving the data during disaster. By using both the techniques, the retrieving data are estimated. On comparing the performance of both the algorithms based on recovery time and cost of both the techniques, it is found that Quantum Cryptography is better than the Cloud Standby Recovery technique during disaster. These comparisons are shown below

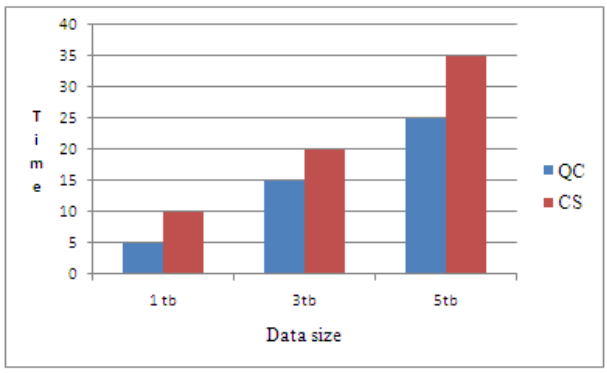

Figure 2 : Time Analysis

The costs for this approach arise from the starting of the Quantum cryptography method with Cloud standby technique. Thereby the standby costs are linked to the configured update interval.

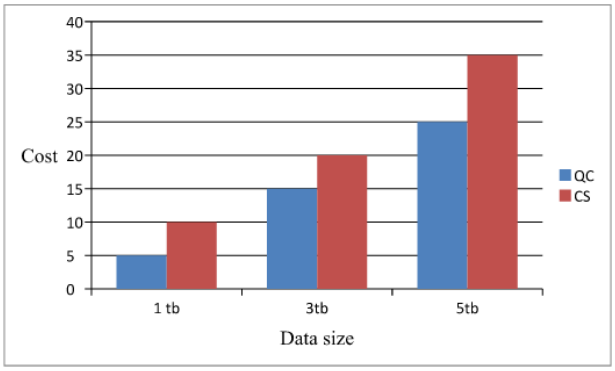

Figure 3 : Cost Analysis

The update interval also defines what RTO can be achieved with the resulting function and a cost function for periodic Cloud updates. We calculated the costs of running a standby systems, costs are slowly overhead so we are using the technique of Quantum Cryptography. A comparison graph is drawn on comparing the recovery mechanism and deployment time. By using both Techniques, Quantum Cryptography and Cloud Stanby the retrieving data are estimated. On comparing the performance of deployment time based on retrieving the data, it is found that Quantum Cryptographic technique partitioned the data transfer during disaster is better than Cloud Standby Technique.

IV. CONCLUSION

We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s). It is concluded that the application works well and satisfy the owner and customers. The application is tested very well and errors are properly debugged. The site is simultaneously accessed from more than one system. Simultaneous login from more than one place is tested.

The project works according to the restrictions provided in their respective browsers. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one. The speed of the transactions become more enough now.

V. FUTURE ENHANCEMENT

The system can be further enhanced by adding new features and facilities. Now the system is platform dependent and it can be made as platform independent software. Once it is made as platform independent software, it is can be used by any intranet user of the shop.

VI. REFERENCES

[1] A. Baig, White Paper: A Cloud Guide for HPC - Top Drivers, Barriers, Use Cases, and Vendor Requirements for Private and Public HPC Cloud Computing. May 2009. [Online]. Available: http://www.univaud.com/about/resources/files/wp-cloud-guide-hpc.pdf [Accessed: June 18, 2009].

[2] I. Foster, I. Yong, Z. Raicu and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Grid Computing Environments Workshop, (2008).

[3] L. M. Vaquero, L Rodero-Merino, J. Caceres and M. Lindner, "A Break in the Clouds", Towards a Cloud Definition, Comput. Commun. Review, vol. 39, no. 1, (2009).

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", Publication of Reliable Adaptive Distributed Systems Laboratory, University of California, Berkeley, (2009)

[5] Amazon Cloud Formation.

[6] Dong Yuan, Yun Yang, "A Highly Practical Approach toward Achieving Minimum Data Sets Storage Cost in the Cloud" IEEE transaction on parallel and distributed systems. vol. 24, June 2012.

[7] Hay, Brian , Nance, K, Bishop, M.,"Storm Clouds Rising: Security Challenges for IaaS Cloud Computing", System Sciences (HICSS), 2011 44th Hawaii International Conference, pp.1-7.

[8] Alexander Lenk, Stefan Tai, "Cloud Standby: Disaster Recovery of Distributed Systems in the Cloud" http://www.aifb.kit.edu/images/0/07/LenkESOCC2014.pdf.

[9] Stephen M. George, Wei Zhou, Harshavardhan Chenji, MyoungGyu Won, Yong Oh Lee, ," DistressNet: A Wireless Ad Hoc and Sensor Network Architecture for Situation Management in Disaster Response" IEEE Communications Magazine March 2010

[10] http://www.bbc. co.uk/news/world-asia-pacific-12709850.

[11] http://en.wikipedia.org/wiki/2010_Haiti_ earthquake.

[12] Harminder Kaur, Ravinder Singh Sawhney," Wireless Sensor Networks for Disaster Management", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012.