International Journal of Computer Science and Engineering Communications
Volume.6, Issue.1 (2018): Page.1813-1820
www.ijcsec.com

Secure Data Migration of Data Center during Disaster using Disaster Monitoring in Cloud Computing

V.Kavitha[1], V.B.Hendhujaa2, P.Sabitha2, N.Swathika2 and R.Indhumathi[2]
[1,2]Department of Computer Science and Engineering
[1,2]Cheran College of Engineering, Karur, India
[1]Kavithataru2015@gmail.com,[2]hendhujaa12@gmail.com, [2]sabics9796@gmail.com,
[2]swathikass01@gmail.com,[2]indhuranjith2017@gmail.com

Abstract : *The remote monitoring system is growing very rapidly due to the growth of supporting technologies as well. And also problem that may occur in remote monitoring such as the number of objects to be monitored and how fast, how much data to be transmitted to the data center to be processed properly. This study focuses on the situation for sensing on the environment condition and disaster early detection. Sensors are used to predict the disaster situations. Data are automatically get change over based on sensor information. Where those two things, it has become an important issue, especially in big cities big cities that have many residents. This study proposes to build the conceptual then prototype model in a comprehensive manner from the remote terminal till development method for data retrieval. We also propose using FTR-HTTP method to guarantee the delivery from remote client to server.*

***Keywords**: Cloud, hardware, software, Data, TPA*

Citation: V.Kavitha, V.B.Hendhujaa, P.Sabitha, N.Swathika and R.Indhumathi. Secure Data Migration of Data Center during Disaster using Disaster Monitoring in Cloud Computing. *International Journal of Computer Science and Engineering Communications* 6(1): 1813-1820, April 2018.

1.INTRODUCTION

The main objective of this project is to increase 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. 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.

Fundamentally huge counting power and the scientists allow the cloud computing systems to deploy computation of storage capacity and large data applications without understructure investment, large supplication data can be stored in the cloud. However, they are either incompletely cost-effective for the storage or impractical to be used at runtime. Regarding the minimum cost benchmark, a highly cost-effective and practical storage blueprint that can automatically decide whether a generated data set should be stored or not at runtime in the cloud. The important of this blueprint is the expansion for replacement between computation and storage, while subsidiary also taking users' optional on storage into consideration. Both conceptual analysis and replication conducted on random data sets as well as specific real world supplication with Amazon's cost model show that the least cost of our strategy is close to or even the same as the minimum cost benchmark, and the efficiency is very high utilization takes place the practical runtime 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 upto last minute transaction.

1.1.DEPLOYMENT MODELS OF CLOUD

1.1.1.PUBLIC CLOUD

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model.

1.1.2.PRIVATE CLOUD

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud.

1.1.3.HYBRID CLOUD

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing.

2.SYSTEM ANALYSIS

2.1EXISTING SYSTEM

Data backup in data center networks (DCNs) is critical to minimize the data loss under disaster. This paper considers the cost-efficient data backup for DCNs against a Disaster with ε early warning time. Given geo-distributed DCNs And such a ε-time early warning disaster, we investigate the issue of how to backup the data in DCN nodes under risk to other safe DCN nodes within the ε early warning time constraint, which is significant because it is an emergency data protection scheme against a predictable disaster and also help DCN operators to build a complete backup scheme, i.e., regular backup and emergency backup. Specifically, an Integer Linear Program (ILP)-based theoretical framework is proposed to identify the optimal selections of backup DCN nodes and data transmission paths, such that the overall data backup cost is minimized.

Extensive numerical results are also provided to illustrate the proposed framework for DCN data backup.

2.1.1.DISADVANTAGE OF THE EXISTING SYSTEM

No prior admin available for assigning the rollback of database. So this architecture may face data loss at anytime. 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.

2.2.PROPOSED SYSTEM

The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, recording, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user’s data is redundantly stored and distributed manner. Individual user’s data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature. Cloud Computing delivers faster recovery times and multi-site availability at a fraction of the cost of conventional disaster recovery. Cloud computing, based on virtualization, takes a very different approach to disaster recovery. With virtualization, the entire server, including the operating system, applications, patches and data is encapsulated into a single software bundle or virtual server. This entire virtual server can be copied or backed up to an offsite data centre and spun up on a virtual host in a matter of minutes. Since the virtual server is hardware independent, the operating system, applications, patches and data can be safely and accurately transferred from one data centre to a second data centre without the burden of reloading each component of the server. This can dramatically reduce recovery times compared to conventional (non-virtualized) disaster recovery approaches where servers need to be loaded with the OS and application software and patched to the last configuration used in production before the data can be restored. Disaster recovery-as-a-service solutions allow you to avoid the costs of purchasing the infrastructure and software needed for a secondary or tertiary disaster recovery site and to pay for your disaster recovery solution out of your operating budget. From the proposed system, 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.

2.2.1.ADVANTAGES OF THE PROPOSED SYSTEM

No Need to depend for the disaster signal form third party. Warnings can be generated from mobile phones itself. 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 consider as hackers. More data accuracy can be provided during roll back process. Can provided unlimited bandwidth for data transfer. Transaction logs can be generated No time consuming.

3.CLOUD COMPUTING BENEFITS

3.1.REDUCED COST

There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

3.2.INCREASED STORAGE

With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.

3.3.FLEXIBILITY

This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

4.CLOUD COMPUTING CHALLENGES

4.1.DATA PROTECTION

Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

4.2.DATA RECOVERY AND AVAILABILITY

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support Appropriate clustering and Fail over ,Data Replication ,System monitoring (Transactions monitoring, logs monitoring and others) ,Maintenance (Runtime Governance) ,Disaster recovery Capacity and performance management. If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

4.3.MANAGEMENT CAPABILITIES

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling‟ for example, is a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today. The public cloud environment is the IaaS/PaaS Infrastructure or Platform as a Service that we rent from Linux (IaaS) or Microsoft (PaaS). Both are enabled for web hosting. Then, your SaaS stack will run under your Internet environment most likely in a virtualized one on your own equipment which would make it private. In this project we specialize in private cloud technology. Here we execute in a cloud environment. If strict security requirements go public or hybrid and if not, try the public or community cloud environment. So that here we are implementing a web services for the output purpose as well as the environment will be shown in actual while hosting the application. So finally SaaS can be fully utilized in cloud environment as IaaS/PaaS. Thus we formed cloud environment.

5.2.DISASTER ANALYSIS

Due to global warming our earth may face many types of disasters like earthquake, tsunami, storm, flood and etc. This disaster can be analysed through cloud remote monitoring. This module has main function to capture data from sensor both in digital or analog input. Package of specific sensors with Remote Terminal Unit will be placed in some places or objects prone to disasters. Cloud computing could be proposed as central of data processing to run service like service listener. It has function to capture and store information sent from the remote client. Otherwise, it could be used for the central data storage and application server to display the processed results to the user.

5.3. *DATA PRESERVATION USING CSP*

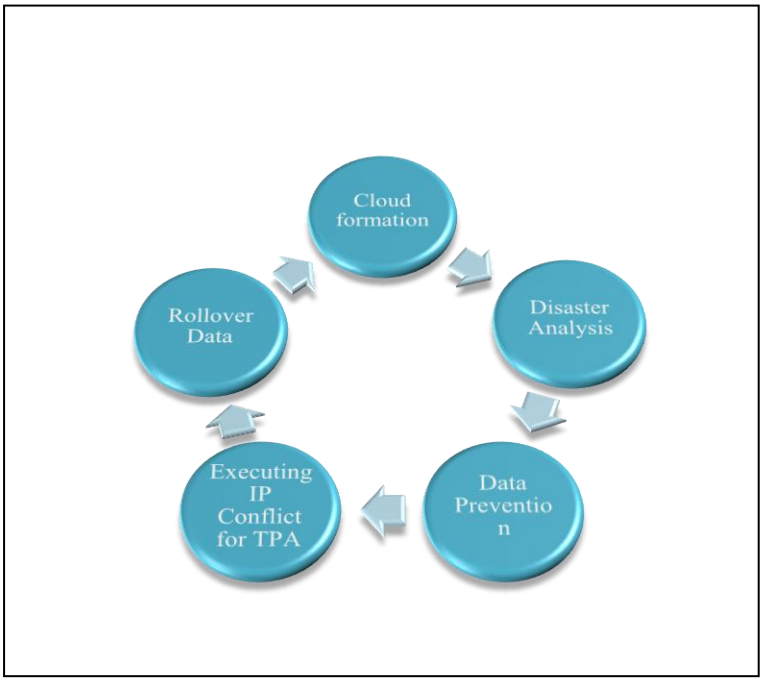
This module deals with the software architecture of the cloud service provider, which is inter related with the remote disaster tool, so that when ever disaster will occur the cloud service provider will trigger out the malware process. This process may execute through Intranet, Internet and also through GPS. So that global communication will be possible here. This architecture should be assigned during the server configuration.

5.4.EXECUTING IP CONFLICT FOR TPA

The Cloud service provider will the triggering function with the TPA(Third Party Auditing). This module will take cares the database migration process. So that when ever disaster will occur the CSP will trigger through the IP conflict and the data base will be restored in the concern location assigned by the admin. Admin can customize the database by providing priority to the table sets. So that the transfer will works according to the assigned priority. This saves the database from data loss.

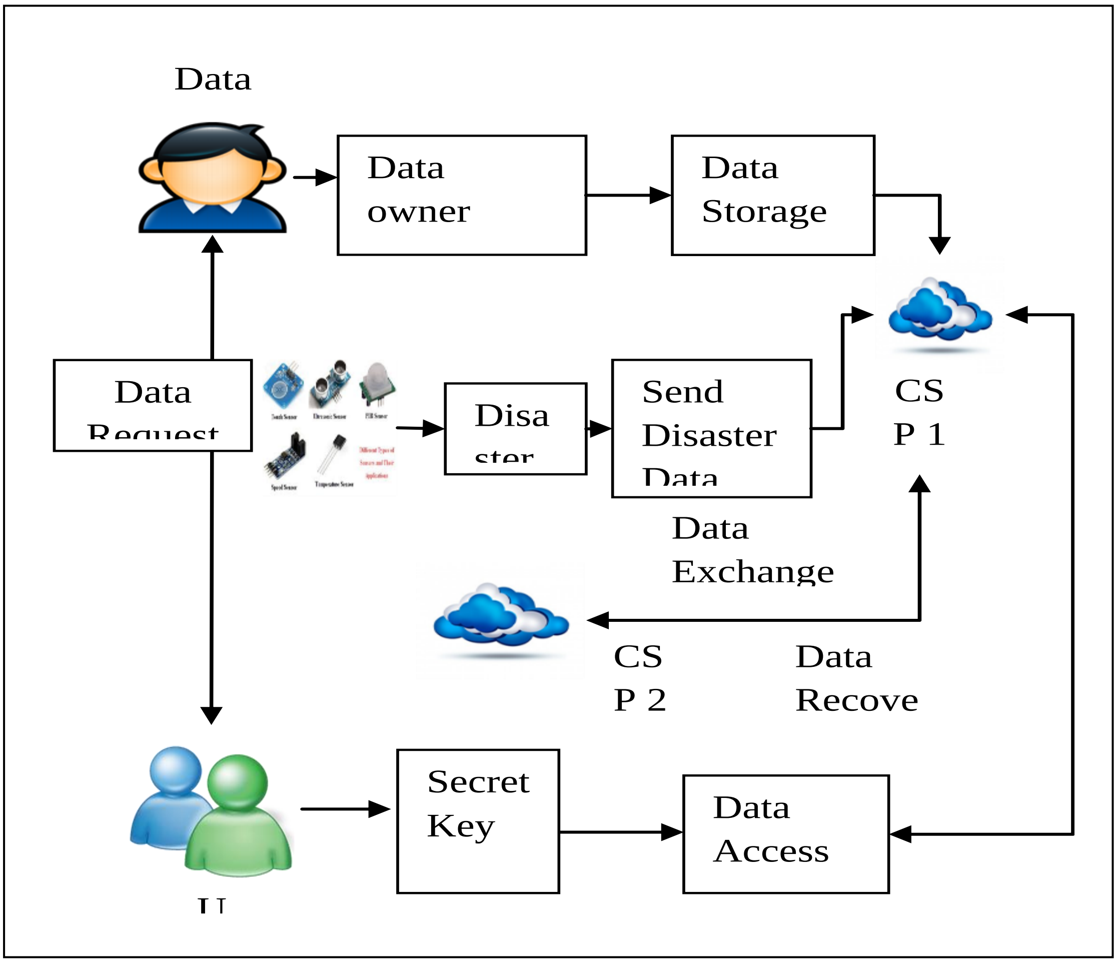
5.5.ROLLOVER DATA

This module will execute after the disaster and CSP trigger out process. The roll back process too needs IP conflict procedure for analysing the failure calculation as the location of the database. According to the admin request original database can be transfer to the default location and also transfer of duplicate database also possible.



6.SYSTEM ARCHITECHTURE

The system architecture of our project based on cloud provider, cloud owner, cloud user and cloud server. The owner should get a authority from the cloud provider to access the cloud services. Then the authorized user can act as a owner. The owner can upload their data. The user should request the owner to access the data from the owner and verify by the secret key. The cloud provider monitor the sensor continuously. If the sensor gives a alert message or information to the provider then the data from the physical sever moves to the cloud sever automatically. It can be retrieved after the normal condition.



7.CONCLUSION

Cloud computing technology to deal with disaster monitoring with sensor based disaster monitoring, and builds a web-based platform to achieve users' interaction with monitoring models. It provides an interoperability infrastructure for distributed remote sensing data resources and geospatial computing resources. The cloud computing interfaces for the high throughput computing improves the throughput during the calculation process. Sensors are used for monitoring devices, that collects the information about disaster and generate the intimation regarding disaster occurrence to the web application. After that data are transmitted from one server to another server automatically. This will help to save the data during the natural disaster. Then user can recover the data to the original server.

REFERENCE

[I] J. Xie, W. Yu, G. Li, An inter-agency collaborative computing framework for fast flood mapping using distributed remote sensing data. Fifth International Conference on Agro-Geoinformatics. 2016.

[2] A. Kotsev, F. Pantisano, S. Schade, S. Jirka, Architecture of a Service-Enabled Sensing Platform for the Environment. Sensors, 15 (2015),4470-4495.

[3] G. Stancalie, V. Craciunescu, A. Irimescu, et aI, Development of Downstream Emergency Response Service for Disaster Hazard Management Based on Earth Observation Data, AgroLife Scientific Journal,5 (I), 199-208,2016.

[4] Y. Ding, Y. Fan, Z. Du, et aI, An integrated geospatial information service system for disaster management in China, International Journal of Digital Earth, 2014, 8(11), 918-945.

[5] C. H. Yang, U. Soergel, Ch. Lanaras, E. Baltsavias, K. Cho, F. Remondino, H. Wakabayashi, Rapid Disaster Analysis based on Remote Sensing: A Case Study about the Tohoku Tsunami Disaster 2011, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XL-7, 2014.

[6] M. Karamouz, Z. Zahmatkesh, T. Saad, Cloud Computing in Urban Flood Disaster Management, World Environmental and Water Resources Congress, 2013