EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.185-192
SANA ACADEMIC PRESS

Data lock, fault tolerance and disaster recovery mechanism in Cloud computing

L. Deepika[1], R.Subhashini[2], S.Brindha [3]
[1]Research Scholar, St.Peter's University, Chennai.
[2]Asst.Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai
[3]Prof. & Head., Dept. of Computer Applications, St.Peter's University, Chennai
deepika.mca109@gmail.com

Abstract-*Cloud computing is a model which provides convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources that can be processed immediately and released with minimal management effort or service provider interaction. Since cloud computing has many features like increased efficiency, flexibility, disaster recovery and security many businesses are moving to cloud computing. The advent of proposed model has capabilities to ensure maximum performance of features like data locks, fault tolerance and disaster recovery. Data lock-in has potential to obstruct portability and interoperability however the proposed model has tools and techniques to manage data in cloud that keeps it accessible and portable to ensure cross-provider compatibility. The existing cloud computing systems are prone to failure which can be then dealt with fault tolerance feature that assesses the ability of a system to respond gracefully to an unexpected hardware or software failure. The proposed solution helps to achieve robustness and dependability in cloud computing by handling failure effectively. Cloud disaster recovery is a backup and restores strategy that involves storing and maintaining records in a cloud computing environment as a security measure. The proposed framework provides an organization with a way to recover data and implement failover in the event of a man-made or natural catastrophe.*

Keywords: *Cloud disaster recovery, fault tolerance, geographical redundancy*

I.INTRODUCTION

In recent years, the technological trend has gained popularity and rapid growth in processing speed and vast storage technologies and the success of the Internet, which leads computing resources become cheaper, more powerful and more ubiquitously available than ever before. This technological trend is popularly known as cloud computing. This technology allows the user to use the internet and central remote servers to maintain data and applications. Cloud computing provides an adaptable online environment which offers the capability to handle many works without affecting on the execution. This allows user to use applications without installation and access their personal files at any computer with internet access. With this technology the user will compute efficiently by centralizing data storage, processing and bandwidth. With the advent of Cloud computing technology, number of cloud providers can be increased and the variety of service offerings has made it difficult for the researcher and poses numerous challenges to cope with. Over the years, researchers are working around the world which enables this technology towards worldwide business opportunity and in other areas of IT infrastructure, utilizing the cloud computing services and mechanism. Cloud computing is broken down into 3 segments such as application, storage and connectivity.

Each segment provides different purpose and offers different products for businesses and individuals around the world. A study has been conducted on cloud computing and found that 91% of senior IT professionals are not sure about cloud computing concepts, whereas two-thirds of senior finance professionals are clear in cloud computing concept and highlighting the young nature of the technology.

Even though cloud computing changing the current IT delivery model for services it has many concerns including security, disaster recovery and business continuity, supplier management, legislations and regulations, and the lack of standards and guidelines. To overcome these concerns, risk mitigation provides benefits of protecting and safeguarding systems and data. Though with advent of risk mitigation, implementation of control is further complicated due lack of standards and guidelines which dealt with security of cloud computing. Cloud computing offers cheaper storage and faster response times which shifts this technology to concurrency control. This feature facilitate data owner to outsource more IT operations. Hence cloud providers can use this as a measure to distinguish them from existing competition. As with any technology, though, cloud computing has biggest barrier which constitute data security risk. Some cloud provider still reluctant to move data to cloud due to the risk of data leakage which may tends to confidentiality and privacy risks. When the business is of high criticality it is reluctant to move application and data to cloud. If data has been leaked it may seize companies cloud due to sharing violated company laws to other company.

Cloud computing is based on virtualization, networking, distributed computing, software and web services. The cloud user may use these services without knowing about hardware and software details. A real time system utilizes the immense computing capabilities and virtualized environment of cloud for the execution of tasks. On the other hand, most of these are safety critical systems require high reliability and high level of fault tolerance for their execution. Fault tolerance aim to achieve robustness and dependability in any system. The fault tolerance techniques can be classified into two types such as proactive and reactive. The Proactive fault tolerance policy will avoid recovery from fault, errors and failure by predicting them and proactively replace the affected component means detect the problem before it actually come. Reactive fault tolerance policies reduce the effort of failures when the failure occurs. These can be further classified into two sub-techniques fault treatment and error processing. Error processing aims at removing errors from the computational state. Fault tolerance is carried out by error processing which have two phases. First phases namely effective error processing which aimed at bringing the error back to a latent state, if possible before occurrence of a failure and latent error processing aimed at ensuring that the error does not become effective again.

Though the features of cloud computing being reason for popularity there might be a situation wherein when the cloud may corrupted or damaged which leads to the loss of all important and private data. This situation needs to be handled efficiently and in order to satisfy the continuity of application and the security of data, the structure of disaster recovery system is included in cloud. To accomplish this task, many different techniques have been proposed till date. The optimal disaster recovery planning should consider as a key parameters including the initial cost, the cost of data transfers, and the cost of data storage.

II. PROPOSED MECHANISM IN CLOUD COMPUTING

Before getting deep into mechanism which is proposed for cloud computing, let us have a overview of cloud computing which will help us to understand much about the mechanism such as data lock, fault tolerance and disaster recovery.

BRIEF ABOUT CLOUD COMPUTING:

Cloud computing provides on demand services to external customers with the illusion of infinite resource and then using the same resource pool for all customers. Hence cloud computing offers customer with several advantages such as reduced cost for customer, flexibility for customer and increased resource utilization rate [10].

A cloud can collaborate with client through capacities called services. The cloud computing has three service models namely Software as a service, Platform as a Service and Infrastructure as a service.

Let us see about cloud computing service model

1. Software as a service (SaaS): This service allows consumer to use applications running on a cloud infrastructure using web browser to access software which offers as a service over the web. The consumer will not have direct control or figure out how the actual frameworks including system, operating systems, storage, servers, network, or even individual application capacities.
2. Platform as a Service (PaaS): This service provides the consumer to deploy onto the cloud infrastructure, consumer created applications, produced using set of programming languages and tools which are supported by the PaaS provider. The consumer will not view or control the underlying cloud framework including operating systems, network, servers, or storage, but consumer has control over the sent applications. Even though it is same as SaaS model, clients do not have control or access to the underlying base being utilized to have their applications at the PaaS level.
3. Infrastructure as a service (IaaS): This service provides the consumers with the capability to provision processing, networks, storage and other computing resources from an IaaS provider. This allows the consumer to deploy and run any software, which can include operating systems, services and applications. The consumer will have direct control over operating systems, storage, deployed applications but constrained control for selected system administration parts. Unlike PaaS model, the IaaS model is a low level of reflection which permits clients to the right of the entering in the underlying foundation through the utilization of virtual machines.

Deployment models of cloud computing are categorized into four models. They are private cloud, public cloud, community cloud, and hybrid cloud. Each model impacts the comparing properties such as scalability, reliability, security, and cost. Lets us see brief about these models:

Private cloud: A cloud that is used exclusively by one customer. Such customer can be company or organization. The cloud may be operated by customer or a third party and hence private cloud offers increased security at greater cost.

Public cloud: A cloud that can be used by more than one customer which can be general public. Due to its availability, the cloud may be less secure. Public cloud is the best option for less secured with less

expensive. This model of cloud will suit for large organization and offer services. This model requires significant investment and hence usually owned by large corporations.

Community cloud: A cloud which is shared by two or more organization or company is termed as community cloud. This model is usually setup for some specific requirements. This cloud is typically for the shared concern.

Hybrid cloud: A cloud with mixture setup of two or more private, public, or community cloud. In this model, the cloud could be freely overseen yet applications and this information will be permitted to move over the cloud.

Consequently, thorough characterization of cloud application features is an essential for the further improvement of cloud framework. On the other hand, cloud computing is still in infancy and experiences due to absence of institutionalization in many aspects. In current scenario, most of the new cloud providers propose their own solutions for access to resources and services which may lead to the heterogeneity problem and raises barriers to cloud realization. As users get more experienced in using cloud infrastructures, their capabilities, strengths and deficiencies become more and more apparent. Hence the cloud providers are working under growing pressure to fulfill the promises, and provide better services to their users.

III. DATA LOCKS IN CLOUD COMPUTING

Data lock in cloud will allow multiple users to read the data concurrently since the data in cloud remains consistent. But when a user attempts to write anything to the data then other users will be excluded from using the same data. Here comes two lock mode namely shared mode lock and exclusive mode lock. A read lock is termed as shared mode lock, and a write lock is termed as exclusive mode lock. When a data object is locked in an exclusive mode, only current user can use the data and no other user can lock the same object in any of the mode. Whereas data object which is locked in a shared mode allows multiple users to access the same object at same time.

The lock protocol in cloud consists of interactions between four parties such as data owner, a central time server, data user, and cloud provider. The interaction will occur among these parties when a user wishes to access data. First the user will obtain a timestamp from the central time server before querying the cloud for data. The purpose of this timestamp is to detect any reordering of operations from the cloud. When the cloud receives the request from user, then the cloud will perform necessary locking operations. As a result of this locking operation, the cloud will return some verification information along with the data to the user. The user will update some information to the data owner when the user releases the lock and data updates back to the cloud. The data owner will maintains this information in a table which contains information about lock number, requested, issued and released. Using this table, the data owner able to determine whether cloud has met the latency requirement or not.

The purpose of data lock in cloud is to ensure safety of data in cloud. This safety will be achieved by following several rules which is explained below.

1) More than one read locks will be issued safely
2) Write lock will be issued only when all read locks for the particular object has been are released
3) When a write lock has been issued for the object then no other lock can be issued until the current write lock has been recovered

With this lock protocol, a cloud provider can provide consistency protection with the use of read locks and write locks. This locking protocol will help cloud to defend against potential attacks.

IV. FAULT TOLERANT TECHNIQUE IN CLOUD

A cloud consists different layers which may affected by many types of faults. So it is necessary to ensure that these layers are equipped with different levels of fault tolerant techniques from which we can make sure that cloud will provide seamless service. Cloud computing failures can be broadly classified into two classes. They are data failures and computation failures. Data failures involves failures due to corruption of cloud data, missing source data and other flaws in the data whereas Computation failure involves hardware and infrastructure failures like faulty or slow virtual machines, storage access exception, etc.

Fault tolerance technique in generic will deals with quick repairing and replacement of faulty devices to retain the system. But in Cloud computing, fault tolerance is nothing but the ability to withstand the abrupt changes which occurs during hardware faults, software faults, network congestions etc. Fault tolerance aim is to achieve the robustness and dependability in any system. Based on the fault tolerance policies we can classify this technique into two types namely proactive and reactive fault tolerance. The Proactive fault tolerance in cloud will predict the problems such as fault, errors and failure before it occurs and proactively replace the suspected component. Reactive fault tolerance technique in cloud will reduce the effort of failures when the failure effectively occurs. Let us see about these techniques in detail.

A. Proactive Fault Tolerance

The principle of proactive fault tolerance policy is to predict and avoid failures proactively by taking preventative measures. Proactive fault tolerance technique will predicts the faults proactively before it occurs and replaces the suspected components by other working components and hence avoiding recovery from faults and errors. These measures are handled by studying the pre-fault indicators and predicting the underlying faults. The next step is to apply remedial measures during the development time by replacing the components which are prone to failure. This technique makes sure that the process will be completed without any reconfiguration.

Two main fault tolerance techniques which developed based on proactive fault tolerant techniques are Preemptive migration and Software Rejuvenation.

1) Preemptive Migration achieves fault tolerance with the help of feedback-loop control system in which applications are constantly monitored and analyzed.
2) Software Rejuvenation achieves fault tolerance by scheduling reboots for system on periodic basis. The system will resumes clean state when reboot occurs each time.

B. Reactive Fault Tolerance

The principle of reactive fault tolerance is to the effect of fault which is already occurred in Cloud. Check pointing/Restart, Replication and Task Resubmission are some of the fault tolerant techniques which are used based on the reactive fault tolerance policy.

1) Check pointing/Restart: The applications can be restarted when a failure occurs. This is efficient fault tolerance technique since restart will be done from the checkpoint prior to the point of failure instead of rebooting from the starting point.

2) Replication: The process of keeping multiple copies of data or object is known as replication. In a replication technique, these copies are termed as replicas and client requests for a copy from a set of replicas. Different resources will run different replicas until the task has been completed.

3) Task Resubmission: The task is submitted, when a fault is detected either to the same resource or to a different resource at a runtime without interrupting the workflow of the system.

Both proactive and reactive fault tolerance policies have its advantages and disadvantages. This technique needs to be configured based on the requirement of the customer. Even though proactive fault tolerance is more efficient than reactive fault tolerance, these are not much used because the system is less affected by incorrect predictions whereas reactive methods are comparatively simple to implement. On the other hand, reactive techniques will not opted for the system which requires higher availability because when a failure occurs, then the system availability will be decreased dramatically.

Various parameters will be consider while choosing fault tolerance technique in cloud computing. Such parameters are performance, scalability, response-time, throughput, availability, security, usability, reliability and associated over-head. Sometimes the type of fault tolerance techniques (Proactive or reactive) will also be considered based on the requirement. Let us see brief about these metrics element. Performance is nothing but the efficiency of the system. This needs to be improved at a reasonable cost by reducing response time besides keeping acceptable delays. Scalability is the ability of a system to perform fault tolerance with any finite number of nodes. Response time is turnaround time from the request to respond received. This time needs to be minimized to improve the performance. Throughput is to calculate the number of tasks whose execution has been completed. With the increased throughput the performance of the system will be increased. Availability of a system is measured as a factor of its reliability as reliability increases, so does availability. Usability is nothing but the extent to which a product can be used by a user to achieve goals with effectiveness, efficiency, and satisfaction. Reliability is to give correct result within a time bounded environment. Associated overhead determines the amount of overhead involved during implementation of a fault tolerance algorithm. Overhead due to movement of tasks, inter-processor and inter-process communication will be considered.

V. DISASTER RECOVERY IN CLOUD COMPUTING

Disaster Recovery refers to act of implementing in a wide range of applications to recover resources even after an outage event induced by natural or human factors. Disaster is unexpected events in a system which can be natural as well as human made. Natural disasters are earthquake, flood, volcano, Tsunami whereas terrorist attack is human made disaster. Both natural and human made disaster may destroy huge volume of data and information. Even though such events are unexpected and non predictable, we have to be careful about such events and needs to be ready with recovery plan. The cloud computing architecture should have enough capability to handle disaster recovery effectively.

There are different approaches in cloud system to implement disaster recovery based on the nature of system. One among such approach is geographical redundancy approach with cloud system. Even though geographical redundancy used in traditional approach of disaster recovery, because of requirements such as extra manpower, physical infrastructure, and other resources will make it very expensive and cannot be affordable. But it is necessary and difficult to ensure business continuity in cloud storage system. In order to maintain the continuity of application and also the security of data, the structure of disaster recovery system is made as distributed computing and centralized storage. Physical separation of the primary and backup sites is the key concept in disaster recovery plan. The active processing of incoming transactions in cloud due to disaster when switched from the failed primary site to the backup site, then this switch is termed as failover. When the cause of primary site failure has been addressed and when the switch is made back from backup site to the primary site, then this switch is termed a failback. Based on the nature of backup site, numbers of options are available to link the process at the primary site. These backup situations are usually described as follows.

Cold standby is backup situation in which recovery requires hardware, operating system and application installation which can take place on multiple days. Hot standby is backup situation in which recovery requires a second data center that can be made available within seconds or minutes. Warm standby is actually a tradeoff between a hot and a cold site. Sometimes recovery levels are described in the terms of tiers. Recovery time objective and recovery point objective are a key measure by which tiers are characterized, which needs to be satisfying criteria when assessing the optimal solution with a given overall price. Recovery time objective is the duration in which functions are unavailable and needs to be repaired. This depends on the tasks needed to restore the transaction by handling capabilities on the backup server.Recovery point objective is the duration between two successive backups, and thus the maximum amount of data that can be lost when restoration is successful. Based on user requirements, disaster recovery has three levels namely data-level disaster recovery, system-level disaster recovery and application level disaster recovery. The basic level of disaster recovery is data-level disaster recovery which ensures the security of the application data. System-level disaster recovery reduces disaster recovery time as short as possible for operating system of application server and make sure that users could not feel that disaster has been occurred.

V.CONCLUSION

In this paper, we considered cloud service is well equipped with data lock, fault tolerance and disaster recovery. We first examined data lock wherein we explained that due to multiple users using same object in cloud at same time the data may be attacked. This can be avoided using lock scheme which is explained in this paper. Secondly, we concentrated on the standard fault tolerant concepts in Cloud Computing with brief about characterization of each technique. Hence fault tolerance can be configured in cloud, when the techniques are being evaluated with metrics element, based on the requirement of customer which is list in this paper. Finally, the cloud-based disaster recovery plan has been proposed in this paper through which cloud can achieve high availability, high survivability and low downtime with low cost. The approach discussed in this paper will give hope to start the cloud-based disaster recovery which will give better business continuity.

REFERENCES

[1]. Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong. “The Characteristics of Cloud Computing” 39th International Conference on Parallel Processing Workshops,2010.
[2]. Cloud Computing” International Conference on Computer Science and Electronics Engineering,2012.
[3]. Deepak Puthal B. P. S. Sahooy, Sambit Mishraz, and Satyabrata Swainz. “Cloud Computing Features, Issues and Challenges: A Big Picture” International Conference on Computational Intelligence & Networks (CINE 2015),2015.
[4]. Justice Opara-Martins, Reza Sahandi, Feng Tian. “Critical Review of Vendor Lock-in and its Impact on Adoption of Cloud Computing” International Conference on Information Society, NOV 2014.
[5]. Mariana Carroll, Alta van der Merwe and Paula Kotze. “Secure Cloud Computing Benefits, Risks and Controls” 2011.
[6]. Seyed Majid Razavian, Hadi Khani, Nasser Yazdani and Fatemeh Ghassemi. “An Analysis of Vendor Lock-in Problem in Cloud Storage” 3rd International Conference on Computer and Knowledge Engineering (ICCKE 2013),2013.
[7]. Chiu C. Tan, Qin Liu, and Jie Wu. “Secure Locking for Untrusted Clouds” 2011.

[8]. Dinesh H A and Vinod Kumar Agarwal. "Multilevel Cryptography with Metadata and Lock Approach for Storing Data in Cloud" 2014.
[9]. Alain Tchana, Laurent Broto, Daniel Hagimont. "Fault Tolerant Approaches in Cloud Computing Infrastructures" ICAS: The Eighth International Conference on Autonomic and Autonomous Systems,2012.
[10]. Ravi Jhawar, Vincenzo Piuri and Marco Santambrogio. "Fault Tolerance Management in Cloud Computing: A System-Level Perspective" 2012.
[11]. Amal Ganesh, Dr. M.Sandhya and Dr. Sharmila Shankar. "A Study on Fault Tolerance methods in Cloud Computing" International Advance Computing Conference,2014.
[12]. Prasenjit Kumar Patra, Harshpreet Singh and Gurpreet Singh. "Fault Tolerance Techniques and Comparative Implementation in Cloud Computing" International Journal of Computer Applications (0975 – 8887), Volume 64– No.14, February 2013.
[13]. Zhang Jian-hua and Zhang Nan. "Cloud Computing-based Data Storage and Disaster Recovery" International Conference on Future Computer Science and Education,2011.
[14]. Manish Pokharel, Seulki Lee and Jong Sou Park. "Disaster Recovery for System Architecture using Cloud Computing" 10th Annual International Symposium on Applications and the Internet,2010.
[15]. Zia Saquib, Veena Tyagi, Shreya Bokare, Shivraj Dongawe, Monika Dwivedi and Jayati Dwivedi. "A New Approach to Disaster Recovery as a Service over Cloud for Database system" 2013.