International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 614-617 Jan 2019-June 2019 www.csjournals.com

Mitigating Impact of Disaster by Effective Method of Data Replication

[1]Shabnam Bhura, [2]Dr. Sachin Bojewar
[1]PG Scholar, [2]Professor& DAO, Department of Information Technology VIT

Abstract: In proposed system, all the data going into database is in structured format only. This data is very huge in amount. When this data is taken for analysis, it will not contain errors as compare to existing system or as it is happening in existing system. So the person who is going to analyze the data, can easily analyze it using any data analysis tool (here it is Informatics or ETL tool). Since the amounts of errors are reduced, this system of storing and/or keeping records will take less time for analysis. The user can easily view records, add records and update records a s per their privileges. Only the administrator of the system or in our case (Database Administrator) has all the rights or permissions of doing all the necessary operations on the data. We are going to design schema for the database which we are going to use. We are going to use RDBMS concepts to transform data. Also we are going to use Normalization technique to normalize the data, so that it can easily understand as well as interpreted. Also in this system we are taking regular backup of database so that, in case of any disaster or any unfavorable situation occurs with data, we will take help of this backup to recover that data to its original state, or in short we can restore the data to its previous state. In this way we are going to design our proposed system.

I. INTRODUCTION

The definition of disaster recovery is embedded in its name, according to Wiki, this is the procedure done for a business to recover easily and have business resumption almost immediately after a disruptive event happens. These disruptions may vary; it could be a high impact one, like a terrorist attack or even a natural disaster like earthquake and it may be as minor as a computer virus attacking one computer. Planning for events like this is essential as you have to remember that you will lose money and profit even for just a few seconds of system outage. A standard should be set and all employees who are tasked to take the responsibility should know the contingency plans. Disaster recovery is a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focus on the IT technology systems supporting critical business functions, as opposed to business continuity, which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery can be therefore considered as a subset of business continuity. Oracle Data Guard ensuring high availability, data protection, and disaster recovery for enterprise data. Data Guard provides a comprehensive set of services that generate, maintain, manage, and monitoring one or more immediate deployment databases to enable production Oracle databases to survive disasters and data corruptions. Data Guard maintaining these immediate deployment databases as transitionally consistent copies of the production database. Then, if the production database becomes unavailable because of a planned or an unplanned outage, Data Guard can be switch any immediate deployment database to the production role, minimizing the downtime associated with the outage. Data Guard can be used with traditional backup, restoration, and clustering techniques to provide a higher level of data protection and data availability. With Data Guard, administration can optionally improve production database performance by offloading resource-intensive backup and reporting operations to immediate deployment systems.

II. LITERATURESURVEY

Disaster is something that nobody wants too butit is something that occurs because of nature and human mistake.No matter what kind of disaster is, is always loss of documents in case of cooperate and life's, damage in general. A number of definitions of, Disaster 'have been proposed over time, many of them focusing on the actual hazard or event and its cost in terms of loss of life or damage to property. Fritz et. al. (1961), interpreted disaster as a state in which the social fabric is disrupted and becomes dysfunctional to a greater or lesser extent. According to Quarantelli (1998) disaster is something social in character. Whereas Gilbert (1998:11) stated disaster as the passage to a state of uncertainty. In 2002 the Commonwealth Government defined a (natural) disaster as: serious disruption to a community or region caused by the impact of a naturally occurring rapid onset event that threatens or causes death, injury or damage to property or the environment and which requires significant and coordinated multi-agency and community response. Such serious disruption can be caused by any one, or a combination of the following natural hazards: bushfire; earthquake; flood; storm; cyclone; storm surge; landslide; tsunami; meteorite strike; or tornado (Commonwealth of Australia, 2002).So disaster has different meaning but same result is same i.e. loss or damage[1].

If we talk about the business the loss is in the form of documents carrying data which are the most important

entity for business. Loss of document can stop the smooth of running of business which business can't afford for this business is always ready with disaster recovery plans. Traditionally DR (Disaster Recovery) has two broad ways: firstly as a desiredoutcome and, secondly as a process leading to a desired outcome. According to Adger (2000), recovery' is depicted as restoration to a previous state of wellbeing in which people experience „closure' and communities, economies and infrastructure return to the same level as they were before. If

we talk about the resilience in DR, it provides a strong theoretical basis for the relationship between prevention of
disaster, responding to, recovering from and preparing for the next disaster. According to Caplan's(1964),coping with an adverse event can lead to increase coping skills, an enhanced sense of selfefficacy, and an increased ability to prevent and cope with future stressors[2].

The World 10 Bank's definition of recovery refers to a process (decisions and actions) with the aim of returning to living conditions that were the same or better than before and also specifically includes the reduction of disaster risk in the definition, The World Bank(2006). A traditional method of recovery of documents using ICT approach is not best suited in today's scenario. For this reason Cloud based disaster recovery is becoming more and more popular in every sector because of its streamlined, convenient and successful in delivering a novel, continually evolving and improving solution for „full-on' data storage and recovery in the whole disaster recovery world[3].

According to Forrester "DRaaS as prepackaged solutions that provide a standard DR failover to a cloud environment that you can buy on a pay-per-use basis with varying rates based upon RPO and RTO". System Architecture using Cloud Computing in DR has been explained by Pokharelet. al. (2010). In this research author's deals with cloud based disaster recovery architecture and finds it is best as cloud offers high availability, high survivability and low unavailability and low downtime with very less cost. Cloud computing system does not only provide the low cost features but also promotes the service provider to concentrate on quality of service rather than its maintenance work.

III. PROPOSEDSYSTEM

In proposed system, all the data going into database is in structured format only. This data is very huge in amount. When this data is taken for analysis, it will not contain errors as compare to existing system or as it is happening in existing system.AsshowninFigure1.Followingcomponentsareimplemented in this system.

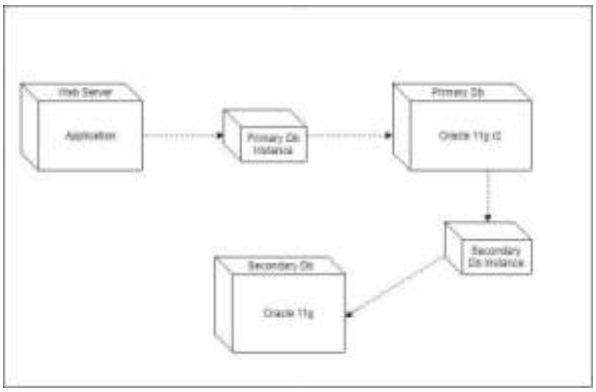

Figure1: Proposed system

The person who is going to analyze the data, can easily analyze it using any data analysis tool (here it is Informatics or ETL tool). Since the amounts of errors are

reduced, this system of storing and/or keeping records will take less time for analysis. The user can easily view records, add records and update records a s per their privileges. Only the administrator of the system or in our case (Database Administrator) has all the rights or permissions of doing all the necessary operations on the data. We are going to design schema for the database which we are going to use. We are going to use RDBMS concepts to transform data. Also we are going to use Normalization technique to normalize the data, so that it can easily understand as well as interpreted. Also in this system we are taking regular backup of database so that, in case of any disaster or any unfavorable situation occurs with data, we will take help of this backup to recover that data to its original state, or in short we can restore the data to its previous state. In this way we are going to design our proposed system.

IV. ALGORITHMUSED

Modern age of TCP implementations include a mechanism, known as the Nagle algorithm, which prevents the unnecessary transmission of a large number of small packets. This algorithm has proving the useful in protecting the Internet against heavy packet loads. However, many applications suffers performance problems as a result of the traditional implementation of the Nagle algorithm. Interact between the Nagle algorithm and TCP's delayed acknowledgment policy can create an especially severe problem, through a temporary "deadlock." These flaws in the Nagle algorithm have prompted many application implementers to disable it, even in cases where this is neither necessary nor wise. We categorized the applications that can and cannot disable the Nagle algorithm, and we show that for some applications that often disable the Nagle algorithm, equivalent performance can be obtained through an improved implementation of the algorithm.

We describe four possible modifications, including one novel proposal, and analyze their performance on benchmark tests. We also are describing a receiver side modification that can help in some circumstances. If an individual user of a shared, large, but finite resource with no explicit limits on consumption increases his or her demand by X%, he or she stands to gain nearly N% more of the resource. Yet if all users increase the demands by X%, the total demand may exceeded the carrying capacity of the resources, resulting in little net gain, or even a collapse. This is known as a "tragedy of the commons" [6]. A user's perceived self-interests conflict with the collective interest of all users, and might even be in conflicts with the user's actual self-interests. The Internet, as we have known it since it's in market, is a commons, and many people recognize its vulnerability to a tragedy of the commons. This has led to numerous proposals for technical mechanisms to limit the consumption, or economic mechanisms to force users to internalize costs. However, none of these mechanisms are in widespread use.

IP are also used in isolated networks (within organization), with the potential for excessive demand, but where administrative or other constraints prevent the use of charging or admission controls. Fortunately, enlighten self-interest can promote good consumption patterns. The primary such mechanisms now used in the Internet are Jacobson's "slow start" and "congestion avoidance" algorithms for TCP [3]. While the primary motivation for these algorithms was to avoid congestive collapse of a shared network, Jacobson showed that they also improved performance for lengthy. TCP/IP connections without competing traffic. That is, for most users, their own self-interest (in employee these algorithm) coincides with the interest of the network as a whole. Even before Jacobson's work explicitly addressing congestion using feedback mechanisms, several TCP algorithms had been devised to limit the number of unnecessary packets injected into the network.

V. METHODOLOGY

A Data Guard consists of one production database and more standalone databases. The databases in a Data Guard configuration are attached by Oracle and may be dispersed all over the world. There are no limitations on where the databases are located, provided they can communicate with each other. For ex, you haveaimmediate deployment database on the similar system as the production database, along with 2immediate deployment databases on other systems at remote locations. You can manage primary and immediate deployment databases using the SQL command-line interfaces or the Data Guard broker interfaces, including a command-line interface and a graphical user interface that is integrated in Oracle Enterprise Manager[3][5].

Primary database:

A Data Guard configuration contains one production database, also referred to as the primary database that functions in the primary role. This is the database that is access by most of your applications. The primary database can be either a single instance Oracle database or an Oracle Real Application Clusters (Oracle RAC) database [6].

Secondary database:

Animmediate deploymentdatabase is a process of changingcontradiction copy of the primary databases. Using a backup copy of the primary databases, you can create up to nine immediate deployment databases and incorporate them in a Data Guard configuration. Once created, Data Guard automatically maintains immediate deployment database by transforming redo data from the primary database and then applying the redo to the immediate deployment database. Similar to a primary database, animmediate deploymentdatabase can be either a single instance Oracle database or an Oracle Real Application Clusters database. Animmediate deployment database can be either a physical immediate deployment database or a logical immediate deploymentdatabase [4].

Physical immediate deployment database:

Provide an identical copy of the primary database, with on disk database structures that are identical to the primary database on a block-for-block basis. The database schema, including indexes, is the same. A physical immediate deployment database is kept synchronized with the primary database, though Redo Apply, which recovers the redo data, received from the primary database and applies the redo to the physical immediate deployment database. A physical immediate deployment database can be used for business purposes other than disaster recovery on a limited basis. As of Oracle Database 11g release 1 (11.1), a physical immediate deployment database can receive and apply redo while it is open for read-only access. A physical immediate deployment database can therefore be used simultaneously for data protection and reporting.

Logical immediate deployment database:

Contain the same logical information as the production database, although the physical organization and structure of the data can be different. The logical immediate deployment database is keptsynchronized with the primary database though SQL Apply**,**which transforms the data in the redo received from the primary database into SQL statements and then executing the SQL statements on the immediate deployment database. A logical immediate deployment database can be used for other business purposes in addition to disaster recovery requirements. This allows users to access a logical immediate deployment database for queries and reporting purposes at any time. Also, using a logical immediate deployment database, you can upgrade Oracle Database

software and patch sets with almost no downtime. Thus, a logical immediate deployment database can be used simultaneously for data protection, reporting, and database upgrades The databaseschema, including indexes, is the same. A physical immediate deployment database is kept synchronized with the primary database, though Redo Apply, which recovers the redo data, received from the primary database and applies the redo to the physical immediate deployment database. A physical immediate deployment database can be used for business purposes other than disaster recovery on a limited basis. As of Oracle Database 11g release 1 (11.1), a physical immediate deployment database can receive and apply redo while it is open for read-only access. A physical immediate deployment database can therefore be used simultaneously for data protection and reporting.

Snapshot immediate deployment database:

A snapshot immediate deployment database is a fully updatable immediate deployment database. Like a physical or logical immediate deployment database, a snapshot immediate deployment database receives and archives redo data from a primary database. Unlike a physical or logical immediate deployment database, a snapshot immediate deployment database does not apply the redo data that it receives. The redo data received by a snapshot immediate deployment database is not applied until the snapshot immediate deployment is converted back into a physical immediate deployment database, after first discarding any local updates made to the snapshot immediate deployment database. A snapshot immediate deployment database is best used in scenarios that require a temporary, updatable snapshot of a physical immediate deployment database. Note that because redo data received by a snapshot immediate deployment database is not applied until it is converted back into a physical immediate deployment, the time needed to recover from a primary database failure is directly proportional to the amount of redo data that needs to be applied.

- Disaster recovery, data protection, and high availability.
- Complete data protection.
- Efficient use of system resources.
- Flexibility in data protection to balance availability against performance requirements.
- Automatic gap detection and resolution.
- Centralized and simple management.
- Integration with Oracle Database.
- Automatic role transitions.
- Create and enable Data Guard configurations, including setting up redo transport services and log apply services.
  Control and monitor Data Guard configurations that containApplication Clusters primary or immediate deployment databases.
- Simplify switchovers and failovers by allowing you to invoke them using either a single key click in Oracle Enterprise Manager or a single command in the DGMGRL command-line interface.
- Enable fast-start failover to fail over automatically when the primary database becomes unavailable.

VI. CONCLUSION

Thus, in the proposed approach, I am going to implement a system that can be used to crawl the data from various manufacture websites and store them in PKV structuredin .txt format fie. This can be done using the Naive Bayesian algorithm. The crawling framework can work well using Jsoup, HTML parser and DOM tree. Obtain data based on user-provided data this data can be actual product information, Xpath, Tags. Such obtained relevant data applied for web indexing, data mining, data harvesting, monitoring modifi- cations to websites and differences to content information. Online retailers have never seen back in spending millions of dollars and comparable efforts for establishing their brand appearance online and earning clientcommitment;theclientswhorepresentthelifebloodof the retail business. Still, there are retailers who work really difficult to collect data from the web that can help them steal clients from the competition and permanently win their businesses.

VII. REFERENCES

1. Disaster Recovery of data by using Data Guard IJCSMS international journal of computer science and management studies, vol. ,issue
2. Oracle technical white paper “Oracle Data Guard 11g Data Protection availability for Oracle Database”.
3. RMAN backup and recovery optimization.
4. Data Guard Concept and Administration 11g Release 2(11.2) E4113403.
5. https://jsoup.org/ - JSOUP/HTMLparser
6. World Bank: Disaster Risk Management.
7. Luis Flores Ballesteros. "Who’s getting the worst of natural disasters?" 54Pesos.org, 4 October 2008 Archived 3 September 2017 at the Wayback Machine.
8. Dus, Henry George Liddell, Robert Scott, "A Greek-English Lexicon", at Perseus.
9. Aster, Henry George Liddell, Robert Scott, "A Greek-English Lexicon", at Perseus.
10. Disaster" in Etymology online.