**CHAPTER 5: PROPOSED SOLUTION**

**5.1 INTRODUCTION**

In Chapter 5, Implementation is done after results obtained from survey or data calculation, experiments conducted, and results are analyzed. This section organized and presents as

1. Implementation details of the proposed solution.
2. Analyzes different disaster recovery plans as an example of the problem under study.
3. Study of implementation examples of proposed solution.
4. Analysis of different problem under this scope.
   1. **IMPLEMENTATION DETAILS OF THE PROPOSED SOLUTION.**

This proposed technique / approach / model can be implemented and tested in a simulation or experimental environments. This approach / method all will be implemented in the perspective of Pakistan and their I.T & Cloud Environment.

* **The objective of proposed technique is : -**
* To help the users to collect and recover the files in case of the file deletion –
* To recover files if the cloud gets destroyed due to any reason.
* To recover same size data.

* To develop Disaster Recovery Model / approach save a valuable data is to in the perspective of Pakistan having better performance parameters such as RPO, RTO, TTO, Cost, security and availability as compared to existing approaches of disaster recovery.
* **PROPOSED METHOD / TECHNIQUE**

Many techniques have been proposed for recovery and backup such as HSDRT, PCS, ERGOT, Linux Box, Cold/Hot backup strategy etc. As discussed already low implementation complexity, low cost, security, RPO,RTO,TTO issues are still challenging in the field of cloud computing. To tackle these issues we propose **this SBA algorithm.**

The proposed technique is broadly categories into PARTS.

The Seed Block Algorithm is time efficient technique to recover the file. It maintains the data integrity and solves the issues like cost, implementation complexity. SBA also focuses on the security concept for the back-up files stored at remote backup server, without using the existing encryption techniques.

What is SBA Algorithm Architecture?

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

This algorithm focuses on simplicity of the data backup and recovery process. It basically uses the concept of Exclusive OR (XOR) operation of the computing world. For Example if we take two data files A and B. When we XOR A and B, it produced X i.e. X =𝐴⨁𝐵 as follows.

First consider the following OR operation

A B A OR B

1 1 1

1 0 1

0 1 1

0 0 0

Consider X =𝐴⨁𝐵 operation

A B A ⨁ B

1 1 0

1 0 1

0 1 1

0 0 0

If suppose for example A data file get destroyed and we want our A data file back then we are able to get A data file back, with the help of B and X data file .i.e. A = 𝑋⊕𝐵.

B X 𝑋⊕𝐵

1 0 1

0 1 1

1 1 0

0 0 0

SBA architecture consists of the Main Cloud and its clients and the Remote Server. Here, first we set a random number in the cloud and unique client id for every client. Second, whenever the client id is being register in the main cloud; then client id and random number is getting EXORed (⊕) with each other to generate seed block for the particular client. The generated seed block corresponds to each client is stored at remote server. Whenever client creates the file in cloud first time, it is stored at the main cloud. When it is stored in main server, the main file of client is being EXORed with the Seed Block of the particular client. And that EXORed file is stored at the remote server in the form of file’ (pronounced as File dash). If either unfortunately file in main cloud crashed / damaged or file is been deleted mistakenly, then the user will get the original file by EXOR file’ with the seed block of the corresponding client to produce the original file and return the resulted file i.e. original file back to the requested client

EXAMPLE:

As it’s architecture shows the main cloud, it’s clients and the remote server. Here first we set a random number for e.g. 100 the cloud and unique id for every client e.g. 101 for client 1. Second whenever the client is being register in the main cloud then the client id and random number is getting EXORed (⊕) with each other to generate seed block for the particular client. The generated seed block (001) corresponds to each client is stored at remote server. Whenever client creates the file in cloud first time, it is stored at the main cloud (e.g. 010). When it is stored in main server, the main file of client is being EXORed with the Seed Block of the particular client. And that EXORed file (100) is stored at the remote server in the form of file’ (pronounced as File dash). If either unfortunately file in main cloud crashed / damaged or file is been deleted mistakenly, then the user will get the original file by EXORing file’ with the seed block of the corresponding client to produce the original file (010) and return the resulted file i.e. original file back to the requested client. It is found that size of original data file stored at main cloud is exactly similar to the size of Back-up file stored at Remote Server.

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

* **DESIGN OF THE PROPOSED METHOD**

**PROPOSED ALGORTHIM**

**…………………………………**

* **PROPOSED OUTCOME**
* **EXPERIMENTATION AND RESULT ANALYSIS**

**Notations**

Cpu\_Threshold --- CPU Threshold

Time\_Threshold --- Time Threshold

Event\_Threshold --- Event Threshold

Current\_Cpu --- Current Cpu

Current\_Time --- Current Time

MHD --- Main Hard Disk

|  |  |  |
| --- | --- | --- |
|  | **Main Cloud Server** | **Remote Cloud Server** |
| **CPU** | Core2 Quad Q660  2.40GHz | Core2 Quad Q660 2.40GHz. |
| **Memory** | 8GB (DDR2-800) | 12GB (DDR2-800) |
| **OS** | Any Windows / Linux Platform | Any Windows / Linux Platform |
| **HDD** | SATA 250GB or more (7200rpm) | SATA 500GB or more (7200rpm) |

**Table No 00 System Environment**

During Experimentation, we found that the files stored at the remote cloud Server are of the same size that of the files stored at the main cloud server by the client. The following table shows that mentioned method preserves the size of the file which is uploaded at the main cloud server by the client

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Size of original file in main cloud** | **Size of Back Up File in Remote Server** | **Size of Recovery File after Recovery Process.** |
| Text (.txt/.docx/.doc/.pdf.xl) | 450 KB | 450 KB | 450 KB |
| 2.3 MB | 2.3 MB | 2.3 MB |
| Image  (.jpeg/.png/.bitmap) | 120 KB | 120 KB | 120 KB |
| 3 MB | 3 MB | 3 MB |

**Table No.00 Performance Analysis for different types of files**

Processing time means the time taken by the system to process all the requests.Client uploads file on the main cloud server,it gets encrypted sing Advance Encryption Statndard Algorithim.After that the main cloud server takes a backup of the file uploaded by the client and stores backed up file on the remote cloud server.Following table shows the processing time of all tasks.We also observed that as the size of file increase the processing speed also increases.

|  |  |  |  |
| --- | --- | --- | --- |
| **Practical Data Size** | **Processing Time on Main Cloud Time (Approximate in Sec.)** | **Processing Time on Remote Cloud Time (Approximate in Sec.)** | **Performance (MB/sec)** |
| **1KB** | 9.15 | 4.5 | 80 |
| **64 KB** | 17.63 | 6.43 | 95 |
| **2 MB** | 4100 | 9.30 | 125 |
| **32 MB** | 8200 | 15.17 | 170 |
| **64 MB** | 13500 | 18.23 | 185 |
| **1 GB** | 19200 | 22.35 | 220 |

**Table No 00 Effect of Size of Data on Performance**

……………………………………………

**5.3 ANALYZES DIFFERENT DISASTER RECOVERY PLANS AS AN EXAMPLE OF THE PROBLEM UNDER STUDY.**

There are number of benefits before analysis of different disaster recovery plans, always consider these benefits before any plan or give more focus.

**5.3.1 BENEFITS OF DISATER RECOVERY PLAN.**

* Always mitigate the impact of unavoidable (Natural or Manmade) disasters to any organization and their I.T Operation.
* Curtail potential economic loss of an organization.
* Decrease the ratio of the probability of occurrence
* Strengthen the organization and their I.T Operation to recover business operations after any disaster.
* Improvement for smooth working of operations always
* Protects your organization’s assets and employees from disasters (Nature or Manmade).
* For smooth and good working of operation work reduces reliance on certain key individuals and functions

**5.3.2 DEVELOPING AN IT DISASTER RECOVERY PLAN**

The Disaster Recovery plan included simple design, basic architecture and all complications at hardware level should be curtailed as much as possible. The Disaster Recovery Plan consists of all solutions and should provide a standardized answer for all services. There is always tough to provide detailed solutions from separate components without any plan.

During any disaster recovery plan, always focus on centralized management for easy detecting changes at any stage and for proper monitoring. This will also offer easy testing process, because when we regularly test all processes and all the changes will be automatically observed in Disaster Recovery Plan.

The Recovery Plans phase involves the formulation of strategies for replacing systems, networks, and end users in the wake of an unplanned interruption event. Every organization differs, so there is no standard approach to effectively create a Disaster Recovery Plan (DRP). Further, it always needs to include that the Disaster Recovery design should secure data transfer and all their operations between both sites without any interruption mainly focus on private cloud of the organization in the perspective of Pakistan.

**5.3.3 DIFFERENT DISASTER RECOVERY PLANS**

Always, follow the plan for continuation of most important business process (specially according to Information Technology) in case of disasters (Natural or man-made like Fire, flood, hurricane, earthquake, Cyber Attacks, Plane crashes, Network Connectivity Issues, terrorism or anything that diminishes or destroys normal data processing capabilities) destroy data processing capabilities. There is required more focus on Preparation, testing and maintenance of specific actions to recover normal processing in case of disasters.There is need to focuses on planning of an disaster recovery plan for the unexpected event, when the use of technology is disrupted and business operations come close to a standstill.

* If you have sensitive or confidential data, your DRP must preserve its confidentiality.
* If your DRP doesn’t preserve the integrity of your data, it doesn’t matter if you’ve made it available.
* On average, over 40% of businesses that don't have a disaster plan go out of business after a major loss.

Each time the organization rehearses its plans, it should learn from the process, improve the plans, and then rehearse again. Through the constant evaluation and improvement, the organization continues to move forward, and continually improves upon the process, so that it can strive for an improved outcome.

**5.3.4 FOR ANY DISASTER RECOVERY PLAN FIRST CONSIDER THE CONTINGENCY PLANNING?**

The overall planning for unexpected events is called contingency planning (CP) and CP is the process by which organizational planners; position their organizations to prepare for detect, react to and recover from events that threaten the security of information resources and assets, both human and artificial (Nature or Manmade). The main goal of CP is the restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event.

**NIST describes the need for this type of planning as follows:**

“These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.”

**5.3.5 COMPONENTS OF ANY CONTINGENCY PLANNING**

* Incident response plan (IRP) focuses on immediate response to an incident.
* Disaster recovery plan (DRP) focuses on restoring operations at the primary site after disasters occur.
* Business continuity plan (BCP) facilitates establishment of operations at an alternate site, until the organization is able to either resume operations back at their primary site or select a new primary location.

**THE MAIN POINT ALWAYS CONSIDERS, BEFORE CREATION OF ANY INFORMATION TECHNOLOGY (I.T) BUSINESS CONTINUITY PLAN OR DISASTER PLAN IS.**

* MTD – maximum tolerable downtime
* MAO – maximum allowable downtime
* Recovery options will range in price and effort – must match them appropriately with the criticality of business function.

**5.4.5 COMPARING CLOUD-BASED DISASTER RECOVERY PLANNING WITH ALTERNATIVES**

There is an exact comparison among the options available is not possible because there is a range of prices that can apply to each option depending on various factors.

* Cloud computing has been suggested as the new disaster recovery solution, with low startup cost and dynamic scalability using the pay-for-what-you-use model; and it is clear that cloud computing can be a very cost effective option for disaster recovery.
* The control and security of a cloud-based server can be a concern if critical data is stored outside the organization jurisdiction.
* The backup system can be on-site, at a remote collocation site (colo), or implemented using the cloud services of a vendor, such as amazon web services.

**5.4** **STUDY OF IMPLEMENTATION EXAMPLES OF PROPOSED SOLUTION.**

However, the business is responsible for setting their RPO and RTO and also for identifying potential risks and changing levels of risk over time, which is sometimes predictable and can be set according to alerts and external threats, such as Natural Disaster Like Weather or Manmade like internal threats, such as scheduled maintenance.

Here, the optimization model will allocate more resources and increase protection during these periods; this makes the optimization model flexible. The goal of this model is to have a flexible adaptive optimization disaster recovery model that manages the resources according to some quality of service goals, financial limitations and internal and external threats, yet is applicable and practical and has very little management overhead. Moreover, the proposed model is vendor independent and can be applied to various cloud service providers, not limited to some billing and service plans.

* 1. **ANALYSIS OF DIFFERENT PROBLEM UNDER THIS SCOPE.** 
     1. **AGILITY:**

It improves with users' ability to re-provision technological infrastructure resources.

* + 1. **COST:**

It is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation. The e-FISCAL

project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

**5.5.3 VIRTUALIZATION:**

It is a technology allows servers and storage devices to be shared and utilization is increased. Applications can be easily migrated from one physical server to another.

* + 1. **MULTI TENANCY:**

It enables sharing of resources and costs across a large pool of users thus allowing for .

**5.5.4 CENTRALIZATION:**

The centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

* + 1. **UTILIZATION AND EFFICIENCY:**

It improvements for systems that are often only 10–20% utilized.

* + 1. **RELIABILITY:**

It is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

* + 1. **PERFORMANCE:**

It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

* + 1. **SECURITY:**

The security in could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

* + 1. **MAINTENANCE:**

The managing of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

**5.5.10 DATA SECURITY**

Giving full protection to the client’s data is also the utmost priority for the remote server. And either intentionally or unintentionally, it should be not able to access by third party or any other users/client’s.

**,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,**

**FUTURE SCOPE**

**5.6.1 DATA CHALLENGES: STREAMING, MULTIMEDIA, BIG DATA:-**

CLOUDs, following the web service development, still have a very classical client server like organization, i.e.

the services and applications on the CLOUD are invoked for a specific request, which is processed remotely and the result returned to the requesting agent. A growing amount of use cases requires interactivity with the service, even with multiple users at the same time and potentially involves a large degree of different multimedia streams, including e.g. voice, video chat, live virtualization etc.

**5.6.2 ECONOMIC OPPORTUNITIES & EXPERTISE GAPS:-**

It has been noted multiple times in the preceding section that relevant expertise for supporting CLOUD uptake is needed in various contexts. This lack of knowledge hinders uptake to the extent that would be possible, if new users could build up on an existing pool of expertise and in particular experience from a longer time of CLOUD employment. Such a period of knowledge gathering would also have given rise to new cost and business concepts to effectively deal with the CLOUD and thus help new up takers to assess the value / benefit of the CLOUD for their purposes.

**5.6.3 MULTI-TENANCY ISSUES:-**

The impact of multi-tenancy is easily underestimated, but can raise major technological challenges. Whilst maintenance of consistency across multiple ten nastiest an obvious concern, isolation creates actually more difficulties. Depending on what is shared and to what degree, it is currently difficult to impossible to distinguish which part of the resource consumption is caused by which user - for example shared communication over a given network line. This however is necessary for accurate usage / cost assessment per individual user.

**SUMMARY**

In this chapter we discuss the research methodology that will be used to solve the said research problem under study.