**CHAPTER 2: BACKGROUND AND LITERATURE REVIEW**

1. **INTRODUCTION**

In this chapter a brief examination is reported on cloud computing background and on disaster recovery systems in cloud computing. The work done by many researchers all around the world until date now on these my selected topics like (cloud computing background, its service models and type of architectures). These all topics are present in this chapter accordingly.

1. **BACKGROUND**

IT experts define Cloud Computing in different ways. NIST defines cloud computing as “a model for enabling ubiquitous, suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, storage, applications, servers and services) which can be rapidly provisioned and released with nominal management effort or service provider dealings”. (Mell and Grance 2011)

Traditional client / server environment and cloud computing key architectural differences is that; There is only a single physical place, where customer application is located connected with a single database management object in the case of traditional client/server model. Whereas on the other side, when an application is to develop for the cloud-computing environment, it is possible that the application instances are running on several different data centers at different locations simultaneously throughout the world. In addition, the application data is stored and fetched from different data centers throughout the world simultaneously with efficiency and effectively.

Regardless of the cloud computing possible or expected security concern and isolation threats or data integrity issues, cloud computing has advantages that the government IT and public sector organizations want to use it. Now trend of cloud computing also follow in Pakistan due to situation of risk is face by many organizations.

**There are number of benefits used of cloud computing in respective of IT environment of Pakistan as follows:**

|  |  |
| --- | --- |
| * Device and location independence | * Flexibility in Use |
| * Reduced cost | * Backup and Recovery |
| * Increased storage | * Resource Management |
| * Highly automated | * Economies of Scale |
| * Utilization and efficiency improvement | * Easy implementation |
| * Skilled practitioners | * On-demand self service |
| * Quality of Services (QoS) | * Greener technology |
| * Quick Deployment |  |

**Figure 1: Benefits of Cloud Computing [30]**

**Cloud Computing has many advantages over traditional computing environment, but it also has drawbacks related to cloud computing that typically differ from provider to provider. These disadvantages are summarized as:**

|  |  |
| --- | --- |
| * Lesser customer control | * Data security and confidentiality concerns |
| * Data Transfer Cost | * Anchoring problem |
| * Technical Issues | * Some Hidden costs involved |
| * Network dependability | * Legacy compatibility |
| * Security | * Need of Reliable Internet Service |
| * Bandwidth Issues |  |

**Figure 2: Disadvantages of Cloud Computing Used [30]**

1. **CLOUD COMPUTING STRUCTURE**

There are many cloud technologies available now a day in this time-to-time changing world, now cloud computing / cloud provider in Pakistan also allows developing organizations, businesses and employees to execute their applications online on rented tools instead of owing that and save a finance to buy IT costly equipments. All processing’s, data and information saving will be done in the cloud environment on their online data centers and this process is a new one , specially for Pakistanis as cloud user only needs to plug into that cloud each day in order to fulfill their computing needs.

**Based upon the structure cloud computing can be classified as;**

* Software as a Service
* Platform as a Service
* Infrastructure as a Service

**SERVICE MODEL**

**SaaS**

**(Software as a Service)**

**PaaS**

**(Platform as a Service)**

**Software, Application Layer**

**IaaS**

**(Infrastructure as a Service)**

Standard ApplicationPlateform

**Figure 3: Cloud Computing Service Model [30]**

* **Software as a Service (SaaS)** delivery model provides the commercial software that is running through Web on cloud infrastructure for its customer and cloud users. The cloud service providers always provides on-demand software services for specific time of period according to user requirement ,which means that customers access a network-based or cloud based application created specifically for SaaS distribution or SaaS Access Purpose.

* **Platform as a Service (PaaS)** the cloud supplier provides a platform to cloud users or customers for computing their application as their requirement. Consumer acquired applications created using programming languages and tools supported by the cloud provider and necessary for access of cloud computing. Always configurations of software stack and operating system is the responsibility of cloud service provider. Through PaaS, using this utility customers are able to execute their existing applications or testing new applications on rented virtual servers within time.
* **Infrastructure as a Service (IaaS)** referred sometimes as hardware as a service because in this service capability is to provide to cloud consumer to provision of hardware services like processing, storage and other basic resources according to their demand. In the case of Infrastructure as a Service (IaaS), the cloud service provider is liable for providing on priority the hardware as their service. Service provider is also responsible for services like accommodating, operating and maintaining the equipment and run arbitrary software’s and their patches also.

**UNDERSTANDING THE CLOUD SERVICE MODELS**

**LESS END USER MANAGEMENT**

**SOFTWARE AS A SERVICE**

**LESS END USER MANAGEMENT**

**MORE END USER CONTROL**

**PLATFORM AS A SERVICE**

**INFRASTRUCTURE**

**AS A SERVICE**

**Figure 4: Understanding of Cloud Service Model [31]**

**MORE END USER CONTROL**

1. **CLOUD DEVELOPMENT MODEL**

Similar to SaaS/PaaS/IaaS, clouds may be working and deliver their services and hosted in different manners with different ways. Until now, there have been a number of trends of clouds to grow from private local infrastructure to guarantee accessibility of extremely demanded data. Initially data centers use these features for domestic purposes like acknowledge the local resources of country especially a Pakistan prior to consider and sell it publicly. The emergence of public and private cloud gave birth to the hybrid solution of cloud computing, as for availing benefits of both the public and private cloud and utilize the services of both at their best.

**DEPLOYMENT MODEL**



**HYBRID CLOUD**

**PRIVATE CLOUD**

**(INTERNAL)**

**PUBLIC CLOUD**

**PRIVATE CLOUD**

**(EXTERNAL)**

**Figure 5: Deployment Model [32]**

**Cloud computing service is offers four different deployment model. These models are;**

**2.4.1 PRIVATE CLOUD**

The private cloud infrastructure is provide same facilities and resources as compared to public cloud for selected use by a single organization in which may be consisting of multiple clients or cloud users. It might manage, operated, owned by a single organization / group and a third party or some combination of them and it may exist on or off site. A private cloud is a closed network is almost dedicated to one organization or multiple organizations. There are two types of private cloud: Internal and External, In Internal Private Cloud all computing resources are maintained by internal organizations, owns by IT department and work under special instructions and on the other side in External Private Cloud, resources are maintained and always checked by the service providers for a fee to using it by the organization.

**2.4.2 PUBLIC CLOUD**

The cloud infrastructure is allowed to use by the public or all cloud users, it is all about general model of cloud computing. Business/ Academic/ Government Organization or combination of them, might be owned all, operated and manage. It may exist on the premises of the cloud provider and it is free or pays as use model policy.

**2.4.3 COMMUNITY CLOUD**

The cloud infrastructure is to be provisioned for the selective use, to specific community clients from organizations that have shared concerns (like; mission, security requirements, compliance, policy, jurisdiction and compliance considerations). It is collaborative effort and may be managed, operated and owed by a single organization, a third party or hosted internally or externally.

**2.4.4 HYBRID CLOUD**

Hybrid cloud infrastructure consists of two or more clouds (private or public) that remain exclusive entities with the orchestration between two platforms, they all are bound together by identical or proprietary technology that enables data and application portability and interchange all easily (like; cloud bursting is a load balancing between different types of clouds always).

**COMPANY**

**PRIVATE**

**CLOUD**

**HYBRID**

**CLOUD**

**PUBLIC**

**CLOUD**

**Figure 6: Cloud Deployment Model [33]**

**Hybrid Cloud Architecture**

Off-Premise

**Hybrid Cloud**

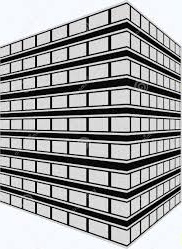
**VPN**

**Public**

**Cloud**

**Private**

**Cloud**



On-Premise

**Figure 7: Hybrid Cloud Architecture [34]**

1. **DISASTER RISKS IN THE PRESPECTIVE OF PAKISTAN.**

A disaster is serious disruption in the normal activities of a society or operation of any organization and sometime this situation is beyond the capacity of the dwellers to cope with in the perspective of local resources of country. Pakistan is a country where situation is always danger from natural or manmade disasters, There is big threat also is Terrorist Attacks and its alarming ratio is increasing day by day in Pakistan, which cause causing huge loss or damage of human and financial assets specially to information technology field . As we all know, disaster's severity is measure by how much impact a hazard has on society and their environment and how many consequences of that. Disasters observed as the consequence of inappropriately managed risk especially in the field of Information Technology. These risks are the product of a combination of both hazards and vulnerability in the field of Information Technology.

Pakistan is a country; declared a disaster-prone country due to geo-physical conditions (always threat of Earthquake), climatic extremes, high degrees of exposure and vulnerability. There are a number of ranges of geo-physical and biological hazards in our country including floods, earthquake, storms, droughts, glacial lake outburst floods (GLOF), landslides, epidemic pose risks to Pakistani society. Some of these hazards (e.g. floods, landslides etc.) are predominantly seasonal and occur on an annual basis, whereas other hazards such as earthquakes is rare events but potentially highly destructive. In addition to natural hazards, a variety of human-induced hazards also threaten Pakistani society, economy and environment specially information technology field.

1. **CAUSES OF DATA LOSS**

There are number of causes of data loss due to disaster occurrence either natural or manmade;

|  |  |  |
| --- | --- | --- |
| 01 | **Natural Disaster** | No one know priority basis about the data loss and this will mostly disrupt a routine and daily work unexpectedly. |
| 02 | **Mission**  **Significant**  **Application failure** | Catastrophic effect or failure always occurred due to unusable applications or programs. This failure can be reduce by using all stored applications, updated software services and their patches also. |
| 03 | **Network Failure** | In cloud computing, cloud and clients are to be link by internet. Systems are crash as network failure occurred, because all system link to cloud. |
| 04 | **Network intrusion** | Possibility of disaster occurrence can be reducing by prior found of invaded in .exe file virus, for advance prevention of disaster occurrence. |
| 05 | **Hacking or Malicious code** | Hacking or Malicious code is to produce to change crucial data. Always avoid dealing inside or outside of the organization with any hacking or malicious code for advance reduction of any disaster. |
| 06 | **System Failure** | As infrastructure is basic of working for a whole system and for their operations, if infrastructure in an organization fails then completely systems will be collapse and all data will be lost, which is difficult to recover or restore. |

* The main reason for occurrence of disaster is human. Due to Human Error, 60% of the data centers are crash and failed according to analysis.
* According to survey, 40% small businesses using cloud are fails to reopen their business after catastrophic affect or disaster.

1. **DISASTER AND INFORMATION TECHNOLOGY**

Every organization requires a business continuity plan (BCP) or disaster recovery plan (DRP) having following targets:

1. Falls within cost constraints of the organizations,
2. Achieve the target recovery requirements in terms of recovery time objective (RTO), recovery point objective (RPO) and test time objective (TTO).

The organizations must identify the likely events or possible hazards especially in the sense of Information Technology that can cause disasters and evaluate their impact on Information Technology field and their related fields. They need to set the objectives clearly, evaluate feasible disaster recovery plans specially according to the local resources , to choose the DRP that would be optimal according to the local resources available regarding information technology in Pakistan.

The paper examines tradeoffs involved and presents guidelines for choosing among the disaster recovery options.

**The optimal disaster recovery planning** should take into consideration the key parameters

1. The initial cost.
2. The cost of data transfers.
3. The cost of data storage.

The organization concern about data needs and its disaster recovery objectives need to be consider and analyzed. To evaluate the risk, the identification of disaster (natural or human-caused) is required always. The probability of a disaster occurrence to assessed along with the costs of corresponding failures. There is also an appropriate approach for the cost evaluation needs to be determined to allow a quantitative assessment of currently active disaster recovery plans (DRP) in terms of the time need to restore the service (associated with RTO) and possible loss of data (associated with RPO). This can guide future development of the plan and maintenance of the DRP. Such a quantitative approach would also allow CIOs to compare applicable DRP solutions.

When a system crashes or power failure occurs, there is always a chance of loss of data and sometimes it may result it in financial loss. This system crashing and other problems occur due to natural disasters or by human, which causing expensive service disruptions. When a disaster occurs in business continuity, the company may get huge loss of data and financial loss. A phenomenon can cause damage to life and property and destroy the economic, social and cultural life of people. When disaster occurs company need to protect the data from loss.

When disaster occurs at client side backup will be stored in cloud but if disaster occurs in cloud data will be lost. Natural disasters may occur due to bad weather results and manmade disaster may occur due to mainly Human Errors

.

**Some disaster recovery techniques: used to recover data and to overcome these disasters are as follows:**

* **Backing up the data (** is to be considering the old technique, used for disaster recovery)
* **Dedicated and shared models (**are the two approaches for disaster recovery based on cost and speed. Storing the data from cloud infrastructure in order to recover when disaster occur)

.

**Every organization should have a documented disaster recovery process and should test that process at least twice each year and when a situation going worse according to weather also.**

**Protection**

* Backup
* HA/FT
* Replication
* Continuous Availability

**Planning**

* Identification
* Fingerprinting
* RPOs,RTOs and SLAs set

**IT Continuity Management**

**Optimization**

* Cost Management
* Resource Optimization

**Assurance**

* Monitoring and Reporting
* Dynamic DR Plan Changes

**Figure 8: IT Continuity Plan [35]**

1. **DISASTER RECOVERY REQUIREMENTS**

Many disaster recovery model/plan exists for cloud computing paradigm. These disaster recovery solutions should evaluate and assessed on few parameters.

**The key features for effective disaster recovery solution are;**

* **Recovery Point Objective (RPO):**

Maximum quantity of data that can be lost, when disaster recovery is did successfully.

* Traditionally the maximum rate has been 24 hours. Recovery Point Objective output is zero, if the backup taken are the synchronous mirrored.
* Some mission critical application does not afford any data lost (RPO=0), in such circumstance continuous synchronous replication is required always. Many other applications could bear a data loss of few seconds, hours or even days according to the situation.

Therefore, the Recovery Point Objective is usually a business choice. Simply to say, the recovery point objective recognize how much data the business is willing to loss on occurrence of a disaster (naturally or manmade).

Recovery Point Objective is normally administers or supervises by the manner in which you back up and save data accordingly:

|  |  |
| --- | --- |
| **Weekly off-site backups** | There is better to perform Daily off-site backups as compared to weekly off-site backups. |
| **Daily on-site backups** | Hourly on-site backups are also better than daily on-site backups |
| **A Network Attached Storage / Storage Area Network** | Endure the loss of data on an individual server. |
| **Clustered Database** | This will ensure the loss of data on database node or an individual data storage device with no data loss. |
| **Clustered Database across Multiple Data Centers** | This will ensure the loss of data on an individual data center with no data loss. |

* **Recovery Time Objective (RTO):**This is time duration in which business operations are unavailable, always to restore for re-continue. It may also contain recognition of failure and get ready essential servers at backup site to start an interrupted application as soon as possible. RTO may be minutes, hours, and days. Recovery Time Objective depends always on the tasks needed to restore the transaction handling capabilities at the backup server. While it can take days using tape backups, it can take less than a minute in advanced systems and more.

**In simple words recovery time objective is the adequate downtime that an organization can bear in the occasion of a disaster.**

|  |  |
| --- | --- |
| **Performance** | To make disaster recovery service failure free operation by using method of synchronous replication of application to the backup site. |
| **Consistency** | The application for taken backup, it should be replicated as disaster takes place on the identical site after handling of disaster at the steady state. |
| **Disaster Recovery Capability** | It refers to the ability to recover timely and continuing to operate using disaster recovery resources and disaster recovery plans after the disaster occurred soon. |
| **Data Backup Strategy** | Data backup strategy refers to the determination of steps, process and actions in order to achieve data recovery and reconstruction objectives properly. |
| **Replication Technology** | Replication is the core technology of disaster recovery. Replication technology divided into synchronous and asynchronous methods.  (1) Synchronous Replication; it refers to copying the local data to an offsite synchronized fully by software.  (2) Asynchronous Replication; it makes sure that the completion of basic operation to the local storage system before the update remote storage view. |
| **Data Snapshots** | * Snapshot is also one of the key technologies of storage as storage establishes a snapshot logical unit number and snapshot cache. Snapshot can extract the current online business crucial data in real-time in the case of the user's normal business is not affected and maintained all properly. |

1. **DISASTER RECOVERY PLANNING**

There are some mechanisms those practically implemented for data back up when disaster recovery technique is used. So that when we want to take back up of a data, we can follow some mechanisms.

Backup sites can come from three different sources:

* Companies, those are specializing in providing disaster recovery services always on their best.
* Other locations owned and operated by your organization for backup purpose.
* There is a mutual agreement with another organization, having same capability to share data center facilities in the event of a (natural or manmade) disaster.

1. ***Hot Backup Site:***

Due to duplicate of original site, its expensive to operate and work with organization as this is operate in real time processes .In this process, data loss is minimal because we can relocate the data and continue our work ,what we are performing or done. It will do all as save a virtual image of our current data. Hot backup site can bring up to full production in a few hours. This is used on priority basis in the situations of a disaster happening or occurrence.

1. **Cool Backup Site:**

Mainly this is least expensive to operate. This process is not performing at any back up of data copies as well. There is always required more time as lack of hardware can start up with a minimal cost. Before recovery operation is to be perform, required everything to restore service to the users and it must be procured and delivered to the site.

1. **Warm backup site:**

For applying a warm backup site, the last data backup should be delivering to their primary sites on prior basis as it is already saved , copied ,resides with a hardware configuration on the backup site that found in primary site / location.

* System Fails
* Business Operations

are interrupted.

* Disaster Recovery Planning Starts
* Business Data on Enterprise Server
* Day to Day Operations

**Disaster**

**Strikes**

**Normal Business Operations**

**Disaster Recovery and**

**Business Continuity**

**Reconstitution and Restoration Process**

* Resources Deployed

for Recovery are Secured and Relocated.

* Disaster Diagnosed
* Disaster Recovery plan implemented
* Business Operations Continue.

**Figure 9: Disaster Recovery Plan [36]**

**………………………………………………….**

1. **REMOTE DISASTER RECOVERY SYSTEM**

Once the location of information systems encounter major disaster (natural or main made), such as large-scale power outages, earthquakes, the local backup mode cannot play its due role, therefore, should be selected application-level remote off-site backup mode.

Moreover, the disaster recovery system cannot be homogeneous with the original information system in servers, storage and other equipment in many cases (the same brand and the same model, which is main issue in cloud computing also). The architectural design must be need to considered compatible with a heterogeneous environment, you should consider disaster recovery architecture and device-independent features, so that does not depend on the specific hardware platform features.

(Always disaster recovery architecture and device independent model is required in this regard).

**Thus, in the design of disaster backup system's overall technical solution should be subject to the following principles and follow this triangle:**

**(2) Stability Principle**

* Ensure the system is running stable all time.
* Minimize the risks of disaster recovery operation the system switch.

**(1) Compatibility Principle**

* + - * Fully compatible with

existing information systems

* + - * Existing system can

be smoothly switched to

disaster recovery system.

**Principles**

**Design of Disaster Backup System's**

**(3) Management Principle**

* Facilitate centralized monitoring and management of Disaster Recovery System.
* Information system implementation is performing of Disaster Recovery System.
* System smoothly switching is the difficult to resolve problem as on heterogeneous hardware platforms, large data volume, high frequency of data updates and real-time data on the database of the off-site disaster backup.

1. **The Design Principle and Classification of Disaster Preparedness Strategies.**

The main feature of the cloud disaster recovery center; is the integration of resources and it provides personalized disaster recovery needs for different users, so we should give full play to the characteristics of the (cloud disaster recovery centre) in terms of disaster recovery strategy design.

**The first problem of cloud disaster recovery meet is compatibility issues**, because the storage of different brands are compatible hardly always and sometimes the same brand of equipment are not compatible due to error, resulting a lot of self-built disaster recovery system restricted by equipment brands completely. Cloud disaster recovery center need to deal with multiple users who have different storage brands, so we must solve the problem of compatibility with different storage brands, but also solve the problem of limitation of ours own brand for more scope and benefits to cloud users.

* **Therefore, the first principle is compatible with mainstream brands in design of disaster recovery strategy.**

Cloud disaster recovery center is a professional disaster recovery provider to provide services for multiple users and it should meet the disaster recovery demand of different users, as they required.

* **Therefore, the second principle is disaster recovery capability should satisfy the demand of standard grade 1 to grade 6 in design of disaster recovery strategy.**

The most important indicators of disaster recovery strategy are RPO and RTO. The smaller the RPO and RTO is, the less the customers loss, of course, the greater disaster recovery invest on all. Users have all kinds of requirements, so that it is not the higher parameters disaster recovery solution is best suited to the users. We should take full account of the user's status and affordability on priority also.

* **Therefore, the third principle is achieving the highest investment returns for users in technology in design of disaster recovery strategy.**

Cloud disaster recovery center is always different from the self-built disaster recovery center, so the responsibility of the parties that need to be more clearly and many users of the system are in the running state, so we should try to avoid the changes of the user's system.

* **Therefore, the fourth principle is to try to ensure the integrity of the original system and have well defined power and responsibility in design of disaster recovery strategy.**

We need to classify the disaster recovery strategy to adapt to the needs of different users in view of different aspects and scenarios when determine the four principles in design of disaster recovery strategy.

**Generally, disaster recovery strategy divided as:**

1. File-level disaster recovery,
2. Data-level disaster recovery and
3. Application-level disaster recovery.
4. **Application-level disaster recovery** is building a set of same application system in the disaster recovery site to ensure the consistency, accuracy of the system and data by replication technology. When disaster occurs, the system can be switch to the disaster recovery site in a very short period to ensure business continuity.
5. **Data-level disaster recovery** is backing up data system environment to disaster recovery system in real-time by replication technology as well. As long as the user's operating system has no problem, they can remote access to the data system of the disaster recovery center directly, when any disaster is occurs. It guarantees data system recovery in real-time with no ambiguity and data integrity, but the operating system always level runs after recovery of certain means.
6. **File-level disaster recovery** is backing up data to disaster recovery system by means such as backup software. It needs of file level recovery to restore data and operating systems in order to complete the restoration of the system when a disaster occurs.

**The output result and working on different levels are:**

* **(Application-Level Disaster Recovery): RPO tends to zero, RTO tends to zero and misuse can be restoring for application level recovery.**
* **(Data-Level Disaster Recovery): RPO tends to zero, RTO is in hour’s level and misuse can be restoring for data level recovery.**
* **(File-Level Disaster Recovery): RPO is in minute’s level or higher, RTO is in hour’s level or higher and misuse could not be restoring for file-level disaster recovery.**

**LITERATURE REVIEW**

1. **Disaster’s in Cloud Computing**

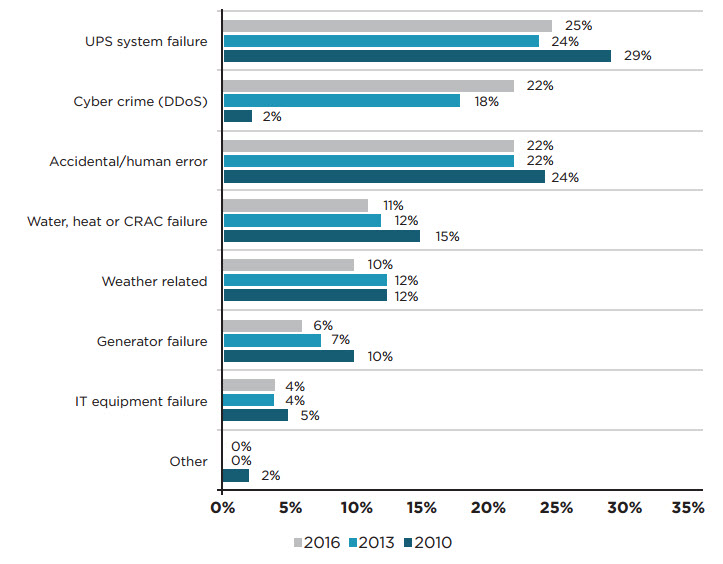
Disasters happen always and they happen everywhere beyond the borders without any limitations. Whether you leverage a public cloud, a hosting provider, or your own data center, infrastructure, the downtime is inevitable. Equipment breaks or does not function as expected, software bugs slip by, natural disasters occur and unforeseen situations lead to unexpected consequences as those are unable to cope with easily and suddenly. Sometimes services are degrade, sometimes-complete data centers go in a dark and nothing will be doing for sudden period.

**There is lot of disasters in cloud computing and Information Technology field observed locally and internationally.**

Firstly, point out the disasters that observed internationally.

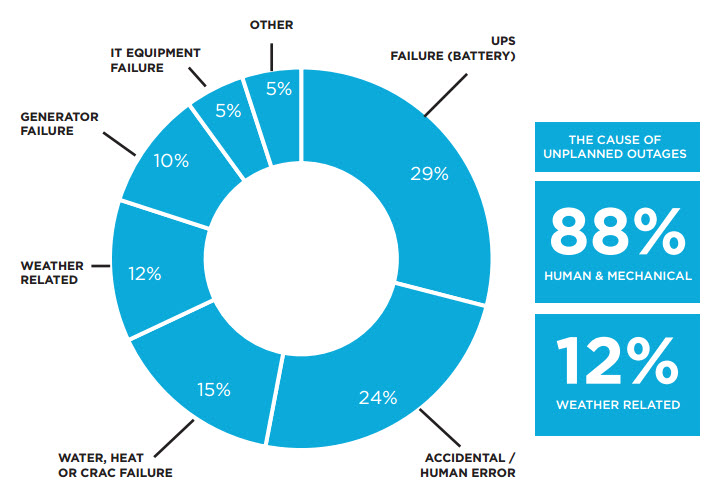
* **In the year 2015 report from IBM,** notable outages of data center or cloud computing services were down are report publicly. After assessed all that, we found that 55 percent of cyber threats were from people with insider access to an organization’s systems mainly their employees. In addition, the biggest threat is a UPS system error in developing countries where electricity shortfall is main issue, which related to operator; lack of training, misinformation, and budget constraints could be underlying causes.

A study commissioned by Emerson from USA present a detailed the causes of data center outages and cited battery failure, cybercrime, and human error as the top three reasons. UPS system failure, which accounts for one-quarter of all root causes, remains as the top cause of unplanned data center outages.



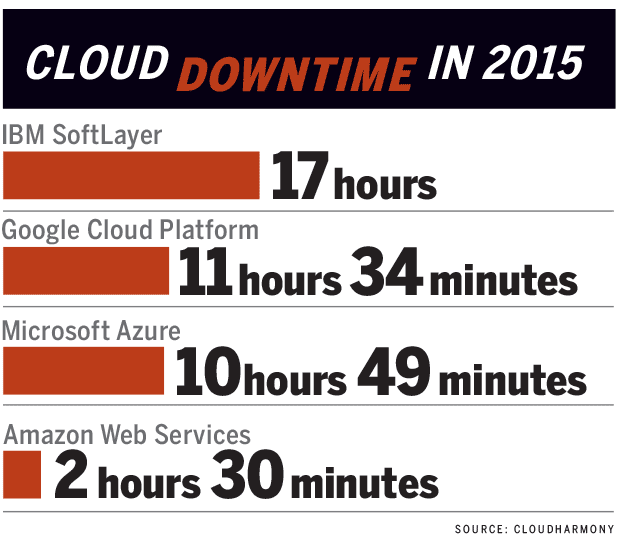
**Figure 10: Causes of Data Centre Outages [37]**

Sponsored by Emerson Network Power 



**Figure 11: Cloud outage causes [38]**

**In the last year, a number of public cloud outages** in the world and internet services down in Pakistan also have raised the question of whether the cloud is reliable enough to run business-critical environments. To try to answer that question, we looked at some data points on recent outages and analysis how important a Disaster Recovery and Data Recovery techniques for safe working of Cloud Computing of Pakistan



**Figure 12: Different Cloud Provider Down Time 2015 [39]**

* **AOL was kicked hard (Date: February , 2015 Down Time Duration: Several Hours)**



**Figure 11: AOL Services Down [40]**

AOL email users were unable to access their accounts reportedly. This all outages is due to a reason of networking issue.

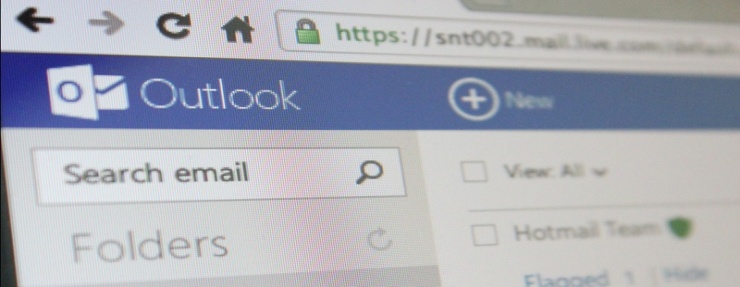
* **Level 3 Communication Centre Outage (Date: June. 2015 )**

****

**Figure 13: Level 3 Communication Outages Centre [41]**

Level 3 Communications suffered a fiber network outage as reason due to a network routing error at a tier 1 backbone internet provider at that time, it was disrupting internet traffic in the US and most of Western Europe.

* **Outlook.com went Offline (Date: April, 2015 Down Time Duration: Several Hours)**



**Figure 14: Outlook.com went Offline [42]**

This was not the first or last service interruption reported for Microsoft’s public cloud email service.

* **Google Compute Engine Outages (Date: February, 2015 Down Time Duration: 03 Hours)**



**Figure 15: Google Compute Engine Suffered Outages [43]**

Google Compute Engine is the company, which offered primary IaaS. It suffered an outage across multiple zones or sites.

* **Apple icloud Services (Date: March ,2015 Down Time Duration: 11 Hours)**



**Figure 16: Apple Icloud Services Down [44]**

In March 2015, both the Apple App Store and iTunes went down taking with iCloud Mail and other web tools. The mainly causes were determined to be internal DNS errors at Apple.

* **Verizon Service (Date:January,2015 Down Time Duration: 40 Hours)**



**Figure 17: Verizon Services Outages [45]**

Verizon brought down as its IaaS to perform routine maintenance on its own cloud infrastructure. However, customers were give warning ahead of time and service remain outages in this period.

* **Drop box (Date:Jan,2014 Down Duration: 48 Hours)**
* **Drop box drops the ball (Date: Jan. 10, 2013 Duration: Around 16 hours)**

****

**Figure 18: Dropbox service Outages [46]**

* Popular cloud storage provider Drop box suffered a global outage due a failed upgrade of its systems. Sporadic website server errors and non-syncing files ensued
* The main selling point of a service like Drop box is that you can rely on it as if it were your own local hard drive -- so when the service is unavailable for an entire day, it does not bode well for business. all client-syncing and file-uploading would be unavailable "for approximately in that period."
* **Samsung (Date:April,2014 Down Time Duration: No. of Days)**



**Figure 19: Samsung Data Centre Down [47]**

On April 2014, a massive fire incident was observe in a Samsung SDS data center in South Korea, which disrupts mobile access to data stored in the cloud globally as well as credit card services and other Samsung Smart devices’ those are cloud-dependent features.

* **Salesforce.com (Date: June, July 2012 Down Time Duration: 09 Hours)**



**Figure 20: Salesforce.com Power Loss [48]**

In June 2012 and July of 2012, both saw outages at the world’s largest cloud CRM Company. For Salesforce, a momentary power loss were observed at a third party data center

* **Amazon AWS Outage**

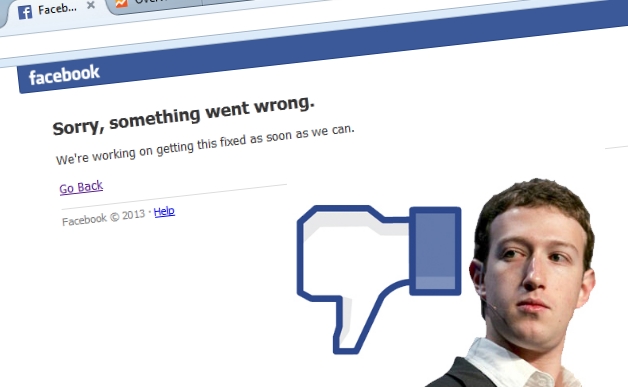
1. **(Date: April, 2011 (Service Interrupted) Down Time Duration: 04 Days)**
2. **(Date: Sept, 2015 (Service Interrupted))**



**Figure 21: Amazon AWS Outages [49]**

1. Azure suffered a massive service disruption that also took down heavily traffic to sites like Reddit, NetFlix, and Foursquare.
2. Amazon went down again, bringing with it NetFlix (again), as well as Tinder, IMDb, and Amazon.com sites down.

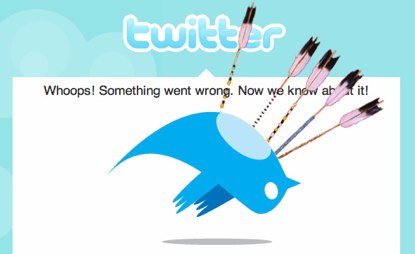
* **Facebook falls flat (Date: January, 2013 Down Time Duration: Two to three hours)**



**Figure 22: Facebook Few Hours Down Time [50]**

Facebook users also around the globe, unable to keep up with their friends' status updates As Facebook is mainly social contact way .So few hours of downtime does not go unnoticed.

* **Twitter (Date: June , 2013 Down Time Duration: About 45 minutes)**



**Figure 23: Twitter Service Down [51]**

There are lot of users were unable to access the services of send or read tweets. After the first 25 minutes, service returned, but remained slow for a while longer.

On the other hand, Internet services are unavailable due to different reasons in Pakistan and there are number of websites also affected by cyber attacks, which show that how much important Disaster Recovery Planning and accurate implementation in the situation of any disaster, as occurred naturally or by human error.

* **Services of PTCL telephone and internet services are disrupt and Down as PTCL is first to deliver services of Communication.**



**Figure 24: PTCL Services are Unavailable [52]**

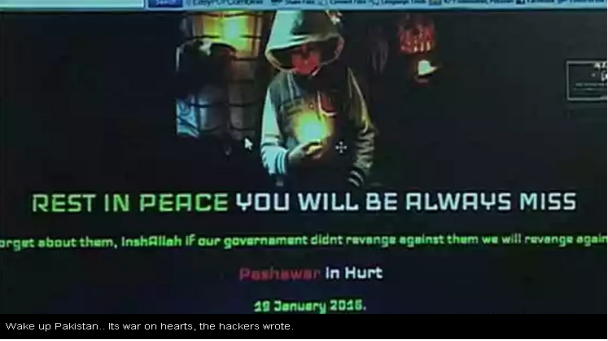
**In February 2015**, (PTCL) Edgerton Road Lahore exchange portion caught fire and services are down in Lahore, Faisalabad and Multan for several days.

**In September 2014**, a PTCL exchange (the backbone of company’s DSL services in the city) on Mall Road Lahore caught massive fire erupted again at or around fourth floor and damaged all fourth floor of PTCL Exchange, which also affected the smooth working of DSL and Telephone.

**In September 2014, floods** have destroyed a large part of the PTCL network in the flood-affected areas also. The gushing water, resulting in temporary disruption of services to the customers has also damaged Cable system.

**In August 2010,** due to flood Pakistan Telecommunication Company Limited (PTCL) suffered a loss of Rs 2.5 -13824 in different parts of the country as over 150 exchanges and 150,000 connections were damaged are reported.

* **Cyber Attack as website of Federal Health Ministry hacked and Down**

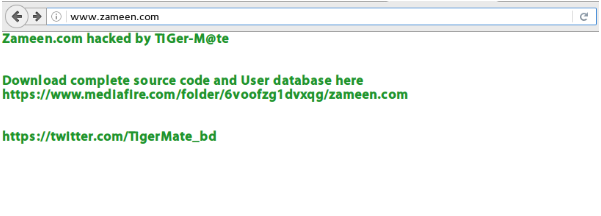
****

**Figure 25: Federal Health Ministry hacked and Down [53]**

**[31]**

In January 2016, Hackers hacked the website of federal health ministry and left message regarding Charsadda massacre as website was not available in this duration for users.

* **Cyber Attack on the web portal of Pakistani property-portal “Zameen.com”**



**Figure 26: Zameen.com hacked and Down [54]**

**[31]**

In May 2016, the web portal of Pakistani property-portal “Zameen.com” was went down for a short while, along with the entire site’s source code and the entire user database as well, which is also disturb the normal activity of zameen.com uses.

* **Allied Bank’s website hacked again in 2013 & 2015.**



**Figure 27: Allied Bank Website hacked and Down [55]**

**[31]**

In November 2015 & July 2013, the official website of Allied Bank Limited of Pakistan was hacked and user access not available. The front-end of the Allied Bank’s website was pretty much hacked and defaced to create trouble for their users.

* **Soneri Banks online banking was Hacked and website was down.**



**Figure 28: Soneri Bank Website hacked and Down [56]**

**[31]**

In March 2013, **Soneri Bank’s online banking website was hacked**twice by two separate hacking groups and hide all from users; they hide all from user to avoid any activity to perform.

1. **Existing disaster recovery approaches**

So far, many disaster recovery approaches exists and presented. Research done by many researchers in last few years is summaries as:

**Andrea et al.** [8] as analyze the problems, issues and the challenges of off-site data replication and virtual machine migration. In particular, this research paper mainly discusses the issue of optimizing network planning to support disaster recovery and business continuity on prior basis. ILP (Integer Linear Programming) formulations for the optimization problem are present, proposed with different objective functions. Heuristics are also proposed and analyzed to taking into account for both the network cost minimization and fault recovery efficiency.

**Kruti et al.** [12] proposed a smart remote data backup algorithm that is [Seed Block Algorithm (SBA)]. The objective of this proposed algorithm is twofold accordingly; firstly it helps the users to collect information from any remote location or site of world in the absence of network connectivity and secondly to recover the files in case of the file deletion or if the cloud is destroyed due to any reason (Naturally or Manmade). Proposed SBA is also solving issues related to the time in a way such that it will take minimum or reduced time for the recovery process. Proposed SBA also prior focuses on the security issues or concept for the back-up files stored at remote server without using any of the existing encryption techniques, approaches or methods.

**T.T.Lwin et al**. [7] clustering of multiple industries standard servers together ,simultaneously to allow for share of workload and fail-over capabilities as it is a low cost method. In this paper, research presents the model of the availability through Semi-Markov Process (SMP) and analyzes the difference in downtime of these two models: the Semi-Markov Process (SMP) model and the approximate Continuous Time Markov Chain (CTMC) model.

**Muppalla et al.** [4] describes how both technologies; the virtualization and replication will protect the data from the any disaster (Naturally or Manmade) without any loss to the business and their continuity. From past 2 years, the IT department has been reducing their costs, they are meeting their services and the commitments of disaster recovery made to be successful with top level by using the hybrid cloud (composed of public & private cloud), which is comprised of two virtualized hardware.

**Gang Li et al. [13]** discusses the necessity, requirement and importance of cloud disaster recovery centers and the vital indicators of disaster recovery by analyzing the classification and selecting all the principle of cloud disaster recovery and their strategies. Developing disaster recovery strategy based on major disaster recovery strategy finally. This paper verifies and tries to approve the feasibility of the disaster recovery strategy by two specific cases of disaster recovery implementation.

**Mahitha et al**. [3] this research paper mainly focuses on a novel approach for disaster management through efficient scheduling mechanism. This paper all about to presents a Priority Preemptive scheduling (PPS) with aging of the jobs in Cloud for disaster management. The implementation results and analysis show that the jobs at any instance of time are to be given with the resources and henceforth all preventing them to enter the starvation state, which is one of the prime causes for any (natural or manmade ) disaster.

**Shalini et al.[5]** examine deeply all the factors that influences the undertaking of disaster recovery planning under the lens of the Protection Motivation Theory (PMT). Additionally, it is important to note and understand that even if there is enough motivation to undertake disaster recovery planning.(whether it is actually undertaken or not is largely dependent or dependable on the influence the Information Technology (IT) Professional is able to exert / proposed as an opinion leader within the organization). A model on disaster recovery planning is proposed and suggesting threats based on hazards and coping appraisals always as the determinants and opinion leadership of the IT Professionals proposed to be as the moderator variable.

Furthermore, there are few techniques in past like HSDRT [23], PCS [24], Linux Box [25], Cold and Hot back-up technique [26], SBBR [27],ERGOT [28] REN [29] of backup and recovery of data have addressed in detail here. Each of the technique has the complete focus and concentration on their objective of backup and recovery.

1. **High Security Distribution and Rake Technology (HS-DRT) (Proposed Year 2010)**

**(Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki, Muzai Gakuendai, Inzai-shi, Chiba, Kazuo Ichihara, proposed the innovative file back-up concept HS-DRT)**

The HS-DRT [23] is express as a proposal of an innovative file back-up concept, which makes use of an effective ultra-widely distributed data transfer mechanism, process, approach and a high-speed encryption technology.

It consists of three components, which are brief below:

1. The main functions are Data Centre.
2. Supervisory server
3. Various client nodes specified by admin.

The client nodes are composed of different moveable clients such as PCs, smart phones, Network Attached Storage and storage devices or services. The all client’s nodes are link / connected with a supervisory server in addition to the Data Centre via a secure network.

The basic procedure is follow in the proposed network system is in this sequence, “There are two sequences which are

1. Backup sequence (Data in backup sequence is receive, which is need to be back up).
2. Recovery sequence (As this is the recovery process, the supervisory server starts the recovery process as disaster is occurred).

As a result of these processes, the Supervisory Server can recover the original data in an original shape that should be backed-up”.

Always remember this model or method is not to be declaring as a perfect technique for Cloud Back-up and recovery services due to some limitations are impose at their best. The main disadvantages is about this model show that the data recovery cost is comparatively increased and also there is increased redundancy always, instead this model can be used for movable clients such as laptops Smart phones etc.

1. **Parity Cloud Service (PCS) (Proposed Year 2011)**

**(Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, have proposed a novel data recovery service framework for cloud infrastructure, the Parity Cloud Service (PCS) provides a privacy-protected personal data recovery service)**

Parity Cloud Service technique (PCS) [24] is a very simple, reliable data recovery at a low cost and easy to use and more convenient for data recovery, which is based on parity recovery service. In this proposed framework, there is no need for user data to be uploading on to the server for data recovery. A Parity Cloud Service (PCS) has low cost for recovery and can recover data with very high probability. For data recovery, Parity Cloud Service (PCS) uses a new technique in this ways as generating virtual disk in user system for best data backup, make parity groups across virtual disk, and store parity data of parity group in cloud. The algorithms for PCS work as follows by using the Exclusive–OR for creating Parity information.

* **Initial parity generation**
* **Parity Block Update**
* **Data Block Recovery**

1. **Efficient Routing Grounded on Taxonomy ERGOT (Proposed Year 2010)**

**(Giuseppe Pirr´o, Paolo Trunfio, Domenico Talia, Paolo Missier and Carole Goble proposed Efficient Routing Grounded on Taxonomy (ERGOT) which is fully based on the semantic analysis and does not focus on time and implementation complexity)**

Efficient Routing Grounded on Taxonomy (ERGOT) [25] .This system is based on the Semantics that provide support for Service Discovery in cloud computing.

This model is built upon three component or its building components are :

1. A DHT (Distributed Hash Table) protocol
2. A SON (Semantic Overlay Network)
3. A measure of semantic similarity among service description

Main reason to focus on this technique as it is not a simple back-up technique rather it provides retrieval of data in an efficient and effective way, The main priority to this technique as this technique is totally based on the semantic similarity between service descriptions and service requests. ERGOT proposes a semantic-driven query answering in DHT-based systems by building a SON over a DHT, but it does not working well according to requirements with semantic similarity search models. The main drawback or disadvantages of this model is an increased in time complexity and implementation complexity both.

1. **Linux Box (Proposed Year 2011)**

**(Vijaykumar Javaraiah introduced a mechanism for online data backup technique for cloud along with disaster recovery)**

Linux Box [26], is a technique in which author has used Linux box approach. The proposed approach is simple, cost effective and protects data from disaster. It also makes the process of migration from one cloud service provider to other very easy .It is affordable and acceptable to all consumers and Small and Medium Business (SMB) because all were not dependent on the service of cloud provider or Internet Service Provider. This solution mainly eliminates consumer’s dependency on the Internet Service Provider (ISP) and its associated backup cost.

A simple hardware box can do all these at little cost with full protection named as simple Linux box [26], which will synchronize up the data at block/file level from the cloud service provider to the consumer. It incorporates an application on Linux box that it will perform backup of the cloud onto the local drives. The application will interface with cloud on a secured channel, check for updates and synchronization them with local storage. The data transmission in this technique will be secure and encrypted on top level.

Furthermore, mainly this model contribution is unable to take the complete backup from the server due to minimal availability of bandwidth which is mainly a drawback of this technique.

1. **Cold and Hot Backup Service Replacement Strategy (CBSRS) (Proposed Year 2011)**

**(Lili Sun, Jianwei An, Yang, Ming Zeng, suggested a technique in which there is a gradual increase in cost with the increase in data)**

In Cold Backup Service Replacement Strategy (CBSRS) [27] recovery process, it is always be triggered upon the detection of the service failures and it will not to be triggered when the service is available. In Hot Backup Service Replacement Strategy (HBSRS) [27], a transcendental recovery strategy for service composition in dynamic network is applied. According to the availability and the current state of service composition before the services interrupt, it restores the service composition dynamically. During the implementation of service, the backup services always remain in the activated states and then the first returned results of services would be adopt on priority to ensure the successful implementation of service composition. On Comparing HBSRS with the CBSRS, it reduced a maximum service recovery time. However, backup services and original services are to be executing simultaneously then recovery cost increases accordingly.

1. **Shared backup router resources (SBBR) (Proposed Year 2011)**

**(Eleni Palkopoulouy, Dominic A. Schupke, Thomas Bauscherty, proposed one technique that mainly focuses on the significant reduction of cost and router failure scenario)**

This technique focuses on the significant cost reduction and router failure scenario i.e. (SBBR) [28]. It main concerns with IP logical connectivity that remains unchanged even after a router failure and the most important and prior factor as it provides the network management system via multi-layer signaling .However, it concerns with the cost reduction concept, as there exist some inconsistencies between logical and physical configurations and addresses that may lead to some performance problem. Additionally, it represents how service imposed maximum outage requirements that have a direct effect on the setting of the significant cost reduction and router failure scenario (SBRR architecture). However, this was a drawback to be notice; it is not possible for this technique to includes optimization concept with cost reduction

1. **Rent Out the Rented Resources**

Below proposed models revolves around the concept “Rent out the Rented Resources” All concept were presented by different Researchers as their own.

1. **(Sheheryar Malik, Fabrice Huet, proposed the lowest cost point of view a model “Rent out the Rented Resources” ...Proposed Year 2011)**

Architecture of this Virtual Cloud [29] is a client-server model and it’s consist of two main components, those are

1. Virtual Cloud Manager (VCM)
2. Host Manager (HM).

Firstly, Virtual Cloud Manager is mainly a server type component as this is functioning on the cloud vendor’s infrastructure.

On the other hand, Host Manager is a component, installed at each host machine and this instance of Host Manager is always install only on rented virtual cloud vendor (host machines) of cooperating ventures.

This model revolves around the concept of “rent out the rented resources” mainly and all focus of concept and aims to provide low cost cloud services to the all clients by reducing the infrastructure cost for the cloud vendor and after giving some monetary benefits to the cooperating ventures. In case of Virtual Cloud, service quality should be slightly down or degraded as compare to the traditional clouds. However, one thing is in notice, the services are available at a cheaper price.

1. **( A. Celesti, F. Tusa, M. Villari, A. Puliafito “How to Enhance Cloud Architectures to Enable Cross-Federation”.. Proposed in 2010)**

This technique also has done some work in the area of cross-cloud federation [30] . They authors have proposed a three phase model for cross-cloud federation. These three phases are propose into as

1. Discovery
2. Matchmaking
3. Authentication.
4. **(K. Keahey, M. Tsugawa, A. Matsunaga, J. Fortes, “Sky Computing”..Proposed Year 2009)**

This technique is introducing the concept of Sky Computing [31], This is based on the concept, to interconnect the different infrastructure as a service cloud.

1. **(Bernstein, E. Ludvigson, K. Sankar, S. Diamond, M. Morrow, “Blueprint for the Intercloud Protocols and Formats for Cloud Computing Interoperability”.. Proposed in Year 2009)**

This proposed model is for the intercloud architecture [32]. The proposed model of Virtual cloud is also revolves around the concept of “rent out the rented resources”. In this model, the main theory is; cloud vendor rents the resources from some cooperating venture(s) and after performing virtualization, rents it to the clients in form of cloud services as their requirements.