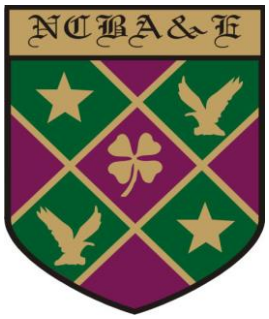
National College of Business Administration & Economics Lahore



EVAUALTING PERFORMANCE OF DISASTER RECOVERY OF CLOUDS USING FUZZY INFERENCE SYSTEM

BY

BISMA ISHTIAQ

MASTER OF PHILOSOPHY
IN
COMPUTER SCIENCE

AUGUST, 2021

NATIONAL COLLEGE OF BUSINESS ADMINISTRATION & ECONOMICS

EVAUALTING PERFORMANCE OF DISASTER RECOVERY OF CLOUDS USING FUZZY INFERENCE SYSTEM

BY

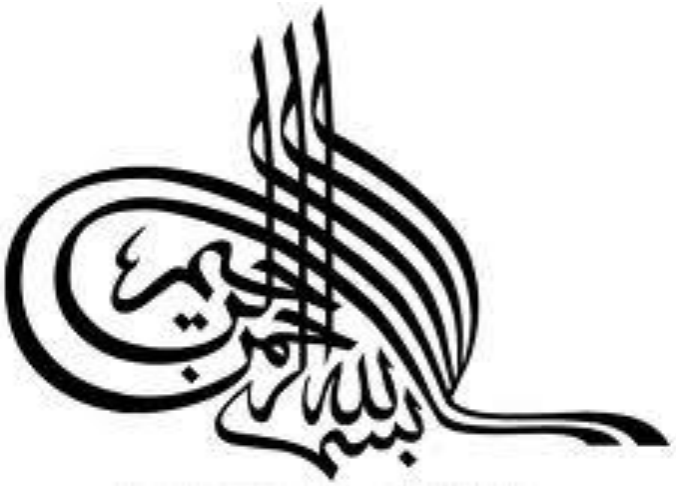
BISMA ISHTIAQ

A dissertation submitted to
School of Computer Sciences

In Partial Fulfillment oft he
Requirements for the Degree of

MASTER OF PHILOSOPHY
IN
COMPUTER SCIENCE

AUGUST, 2021



In the name of ALLAH,
The Most Beneficial,
The Most Merciful,

NATIONAL COLLEGE OF BUSINESS ADMINISTRATION & ECONOMICS LAHORE

EVAUALTING PERFORMANCE OF DISASTER RECOVERY OF CLOUDS USING FUZZY INFERENCE SYSTEM

BY
BISMA ISHTIAQ

A dissertation submitted to School of Computer Sciences, in partial fulfillment of the requirements for the degree of

MASTER OF PHILOSOPHY IN COMPUTER SCIENCE

Dissertation Committee:

_____
Chairman

_____
Member

_____
Member

_____
Director Research
National College of Business Administration and Economics

DECLARATION

It is to declare that this research work has not been submitted for obtaining similar degree from any other university/college.

BISMA ISHTIAQ
AUGUST, 2021

Dedicated
To

This dissertation and all of
My Academic achievements are
dedicated to My Parents & Siblings

ACKNOWLEDGEMENT

Praise and thanks to Allah for sustaining and helping me throughout this Endeavour. There are many individuals who performed a vital role in the completion of this research work. I would like to present my humble gratitude to my august supervisor ***Dr. Sagheer Abbas*** for his efforts. I especially thanks to ***Dr. Gulzar Ahmed*** who has guided me, inspired me, and spent a significant amount of time reviewing my work. I appreciate his encouragement and support throughout the writing of this thesis, as well as his contribution to a stimulating and enjoyable working atmosphere.

My colleagues and seniors are worth mentioning, as their presence, comments and encouragement has always given me energy to work hard and achieve my goals without fail. I'd also like to express my gratitude to my seniors for their feedback and opinions and ideas. Dr. Sagheer Abbas, Dr. Muhammad Adnan Khan are few names to whom I would want to thank them for their assistance and show my gratitude.

It is an honor to present my gratitude to my institute National College of Business Administration & Economics for providing me a knowledge platform and my employer Lahore Garrison University for giving me opportunity to excel in my professional as well as academic endeavor.

RESEARCH COMPLETION CERTIFICATE

Certified that the research work contained in this thesis entitled **"Evaualting Performance of Disaster Recovery of Clouds using Fuzzy Inference System"** has been carried out and completed by **Bisma Ishtiaq** under my supervision during her **M.Phil. Computer Science** Programme.

(Dr. Sagheer Abbas)
Supervisor

SUMMARY

This research is primarily focused on recovery of disaster in cloud computing and the spread of this technology with an enormous speed, which is sufficient to explain the need and desirability of this technology, on the other hand, same distinction is also the main challenge i.e. unplanned growth of cloud computing and relevant technologies. In past we have seen the same issues with World Wide Web, in which we have expanded to such levels that a proper governance and maintenance became near to impossible. Rapidly expanding cloud technology with conventional and emerging services is a source of generating huge volumes of data that requires to be addressed for analytics and simply for suitable storage structure.

Big data and IoT are two emerging challenges linked to cloud computing and these two areas are research focus of many scientists. In this research we have proposed a fuzzy inference system (FIS) which is a blend of cloud technology along with artificial intelligence and cognitive science. We believe that an autonomous and self-evolving intelligent environment is the solution to emerging problems related to cloud technologies. To address the issues of big data and IoT, our proposed model FIS is having the ability to analyze the heterogeneity and homogeneity knowledge structures wherein, machine learning and artificial neural networks have been proposed for semantic, property and feature analysis.

Validation of the proposed model FIS is being done through algorithm development as well as by simulating the model in MATLAB. Results have shown the positive inclination towards ecosystem relevance with overall performance and interoperability i.e. These two characteristics play a vital role in the intelligent recovery system's long-term viability, while third parameter is dynamic which may change as per the requirement e.g. reliability, security, cost etc. This research concludes that cloud technology will work better in a comprehensive cloud ecosystem with better management and service parameters for users as well as for cloud service providers, also the issues of big data and IoT are more manageable and observable in a cloud ecosystem.

LIST OF ABBREVIATION

BFT	Byzantine Fault Tolerance
CSP	Cloud Service Providers
DRBD	Distributed Replicated Block Device
DR	Disaster Recovery
DC	Data Cost
DS	Data Storage
DR	Data Reliability
DD	Data Dependency
DS	Data Security
DFD	Data Failure Detection
FCFS	First-Come-First-Served
FIS	Fuzzy Inference System
FCIP	Fiber Channel over Internet Protocol
GRM	Geographical Redundancy Method
HAIL	High Availability and Integrity Layer
HSDRT	High Security Distribution and Rake Technology Single-Multi Cloud
IGG	Inter Grid Gateway
IT	Information Technology
ISP	Internet Service Provider
IFCP	Internet Fiber Channel Protocol
IDC	Macintosh Apple Computer
IAAS	Infrastructure As a service
ML	Machine Learning
MCE	Multi-Cloud Environments
MCS	Multi-Cloud Storage
PCS	Parity Cloud Service
PAAS	Platform As a Services
SAAS	Software as a Service
SDA	Service Discovery Agent

SLA	Service Level Agreement
SAN	Storage Area Networks
SQL	Structured-Query Language
TCP	Transfer Control Protocol
RTO	Recovery Time Objective
RPO	Recovery Point Objective
RDBS	Remote Data backup server
URL	Uniform Resource Locator
VM	Virtual Machine
EPCDR	Evaluation Performance of Cloud Disaster Recovery
VSM	Virtual Shared Memory

LIST OF TABLES

LIST OF FIGURES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Data is handled, saved, and processed using a network of remote servers housed on the Internet, as opposed to using a local server or a personal computer. IT tracks services assembled by cloud providers, which raises substantial issues about the security and reliability of the services, resulting in a failure. The first step in upgrading information in the cloud is to figure out how to put together a data backup and recovery mechanism that is effective in terms of large-scale data flexibility, availability, and reliability while being cost-effective. Multiple data backup results cover is considered for single cloud preparation, but having individual copies of information may not be enough because data loss may begin to seek away capable failure during a disaster. (Shklovski et al., 2008)

Various replications on more than one remote cloud provider were occupied by additional solutions (multi cloud). Most suggested findings suggest creating at least three records models and either saving all models in different areas or sharing them over an unlimited number of remote locations to achieve a high degree of reliability. High costs, a wide storage area, high consumption, and increased network problems are all disadvantages of this strategy. This model will place a greater emphasis on factors such as data dependency, data cost, data security, data storage, and data reliability. This essay will look at the disaster recovery challenges that arise in both single and multi-cloud environments. Inquire about recent cloud-based Disaster recovery studies to see which issues cloud-based Disaster recovery experts consider are the most pressing. (Castejón et al., 2011)

Cloud computing refers to the on-demand availability of computer system resources, particularly data storage (cloud storage) and computational power, without the requirement for active management by the user. The term refers to data centers that are accessible to a huge number of people over the Internet. In today's huge clouds, functions from central servers are routinely distributed over multiple sites. If the connection to the user is sufficiently close, it can be classed as an edge server. Clouds can be restricted to a single firm (enterprise clouds) or made available to a group of enterprises (public clouds) (public cloud). Cloud computing relies on resource sharing to provide consistency and economies of scale. According to proponents of public and hybrid clouds, cloud computing allows enterprises to eliminate or minimize upfront IT technology costs. Supporters of cloud computing argue that it helps businesses get their applications up and running faster, with better manageability and less downtime,

and that it enables IT teams to more quickly adapt resources to meet fluctuating and volatile demand by delivering high computing capacity during peak demand periods.

Cloud providers frequently use pay-as-you-go methods, which might result in unanticipated operating costs if administrators are inexperienced with cloud-pricing structures. Cloud computing has grown as a result of the broad adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing, as well as the availability of high-capacity networks, low-cost processors and storage devices. Linux was the most widely used operating system, including in Microsoft products, and was thus regarded as the most powerful.(Z. N. Chen et al., 2017)

Cloud computing is gaining attention by offering a variety of services, its reliability, high-performance computing and massive data storage. Cloud users are attracting due to interoperability platforms, accessibility and elasticity. Cloud computing boosts the Emerging Enterprise Technologies in term of economics and best utilization of its service model. Due to heterogeneity structure, the large-scale organizations are converting their infrastructure into Cloud-based systems. One of the best cutting-edge benefits of cloud computing is data recovery management and increase the business by using the property of on-demand delivery. (Z. N. Chen et al., 2017)

Using Clouds, the organization can cut infrastructure cost and increase the storage cost and pay per use. Cloud computing is a metered service for their services. The main attraction of cloud computing, resource virtualization for completion of service using virtualization, the services become more attractive, when accessed by any platform. (Dubey & Bengal, 2017)

Cloud computing is giving an assortment of cloud service providers, elite and versatile information stockpiling over the internet & IoTs. The growing number of cloud users on different platforms such as desktop and window creates an incentive to adopt innovative cloud services in a cloud environment. Cloud computing, in general, can take advantage of the limitless capabilities and resources of cloud-like storage, processing, and communication.(Fernandez et al., 2016)

Variety of services, scalable data storage and high performance enlarged the field of computing and providing user need a base solution. Due to the high demand for data management by the users and big organization, cloud computing gain popularity by offering self-management, automation of cloud services and dynamic load balancing. The big organization can better control by

rented monitoring the computing resource, instead of investing huge amont of physical cost for data centres.(Botta et al., 2016)

Cloud computing is also a providing the fault tolerance system, system resilience and different types of backup system. Fault-tolerance in cloud computing increased the reliability of data and service provision. Fault detection and its recovery modes to its previous state can enhance the trustworthiness. (Castejón et al., 2011).

1.1 DISASTER

Heterogeneous clouds are made up of a variety of hardware and software, including hybrid storage and multiple discs. In cloud-based businesses, the entire firm data is saved in a cloud database. As a result, in these environments, data security, safety, and recovery are critical. Information that has been processed on the primary host but has not yet been duplicated on the backup site is referred to as data in jeopardy. As a result, improved data recovery technology in storage clouds is required in the event of a disaster. Three options for data recovery have been offered.(Alshammari et al., 2018)

a) In the case of a disaster, the fastest disk technology is used to replicate data that is in risk.

b) Changing the polluted page threshold: The amount of clean RAM pages that must be discarded to disks could be decreased.

c) Dangerous device prediction and replacement: A variety of critical variables, such as power consumption, temperature management, carbon credit usage, and the relevance of data (stored on each disc), can be measured over time. To develop a replace priority list, a mathematical equation will be created based on these factors.

Disasters and events are unpredictably changing events that are frequently identified by a mix of information abundance and availability, depending on one's relationship to the events. Despite the fact that crisis management personnel are obsessed with processing large volumes of incoming data, members of the public are frequently left with a severe shortage of timely information needed for personal decision-making and peace of mind (Alshammari et al., 2018) and Members of the public take the initiative to verify it and seek additional information utilizing social connections and tools available, frequently asking assistance from their communities. The nature of contextual knowledge has long attracted researchers in the domains of human-

computer interaction and computer-assisted cooperative work finding, as well as the ways in which it is facilitated by and influenced by information and communication technology (ICT) (Abreu et al., 2019), and military personnel have been the focus Information management in emergency and safety-critical situations has been the subject of a lot of research.

The attention has now switched to the impromptu ICT-enabled acts of citizens who are directly or indirectly affected by emergencies. This research extends on that analysis by describing how information-seeking characteristics are linked to issues of location and environment on public-side emergency response techniques that are urgent. Individuals and family groups are not the only ones affected by disasters; communities are also affected. The study of the use of information and communication technology (ICT) in community processes during times of crisis is still in its early stages. In this article, we look at how members of the group use ICT to organize in crisis situations.

1.2 DISASTER MANAGMENT

Geospatial information enables us to imagine characterized topographical regions and examine the elements and articles inside them. Today, this information assumes a significant part in the debacle the board (DM) area by empowering experts to all the more likely react to, recuperate from and plan for calamity occasions. (Abreu et al., 2019) the information can be utilized to create quick harm appraisals, design and execute search and salvage activities, survey regions inclined to danger chances, and various different exercises. The successful utilization of this information, nonetheless, necessitates that partners have the capacity to get to, oversee and share it. Inescapable web access propels in reasonable innovations and the developing accessibility of open and while free datasets have made it easier to work with these requirements, partners still face significant challenges in accessing and sharing information at all stages of the DM cycle.

As a result, this essay seeks to piece together the primary cycles, and (Abreu et al., 2019) which remain one of the most vulnerable to catastrophic catastrophes. Because of the specialized breakthroughs that have unfolded after a 7.0 magnitude earthquake struck just west of Port-au-Prince on January 12, 2010, Haiti presents a unique scenario for our investigation (Calcaterra et al., 2019) . Responders were left with a big data void for undertaking aid and recovery exercises soon after the quake, as many of the country's basic pattern databases were obsolete, missing, or simply didn't exist.

Huge inflows of information from public and private information providers, international philanthropic organizations, volunteer and specialized networks (V&TCs), and, surprisingly, the influenced populace, soon filled the gap, providing responders on the ground with greater situational awareness for the planning and coordination of their efforts.

Following the earthquake, the drives, organizations, and practices for producing and sharing geospatial datasets have had a significant impact on how various partners are accessing information for DM in Haiti today (just as in other calamity influenced States). In addition, the influx of new entertainers, the expansion of spatial information foundation (SDI) and neighborhoods boundary building, and the recognition of the growing significance and value of data for useful linked activities are all elements attempting to make new elements among partners and cycles for information sharing inside the country. These improvements were again put under serious scrutiny when (Mendonca et al., 2018).

This investigation takes its take off in the repercussions of the Hurricane, to recognize continuous cycles furthermore, it looks into the issues surrounding information sharing and how they are influencing relevant partners. The paper is based on data gathered through participatory perceptions and semi-organized meetings, as well as rational discussions that outline the use of spatial innovations and information for DM exercises in Haiti since the earthquake, as well as larger issues relating to philanthropic cycles in the country and the region as a whole. To more readily comprehend these turns of events, the article is isolated into six segments and continues as follows.

Area two provides a quick authentic overview of how information creation, access, and sharing have evolved from the time of the 2010 earthquake to the present day. The institutional and functional features of relevant entertainers working with information-related DM exercises in the country are used to lay out these progressions. Segment three characterizes the examination approach furthermore, restrictions for the examination and, from there on, area four lays out the fundamental discoveries for the examination inside three topical regions: Monetary, Technical and Legal. Segment five grows the essential discoveries into a scientific conversation which draws from reasonable subjects in a debacle grant, basic topography and enlightening administration examines, and ultimately, segment six finishes up the investigation with contemplations for the more extensive functional ramifications of the exploration.(Jain & Jain, 2017)

Respondents disclosed that preceding the quake, the absence of satisfactory SDI, slow web pages and dissipating of geospatial information

clients in the nation implied that information was principally shared through casual networks; regularly by means of outer stockpiling gadgets like USBs and Disc. Since the tremor, they noted that the SDI in Haiti had been rebuilt and enlarged, and that the generation of information and objects among individual partners had increased. (Mendonca et al., 2018) Outside sources are needed since hardly any office or organization in Haiti has the specialized or financial resources to meet all of their information needs. Respondents were featured on web geo portals to work with these cycles, as well as some of the new market administrations for the arrangement, the board, and examination of information evaluated in the past area.

1.2.1 Dynamic Provision

On-demand service is a model or technique in which we just provide the cloud users with the facility that they can get their services from service providers anytime at any place. The users can get this facility to fulfil its work or any application so the users can have this facility to engage the services on demand. The service providers provide these resources to their users at any time. On-demand self-service can be achieved through dynamic provisioning. When a user demand for more resources the in complex networked server computing environment, through automated server computing instances, the resources are provisioned. (Shaikh & Sasikumar, 2014)

Cooperate organization can reduce the cost of the resources and increase the computing resources and balancing the demand and supply resourcing. Using dynamic provision, the can reduce application and the usage cost. Distributed computing gives resources on request, i.e. at the point when the user’s needs it more as they assigned resources. This is made conceivable addition without any request and input from administration; resources are allocated. Self-benefit implies that the customer plays out every one of the activities expected to gain the administration benefits.

Dynamic resources are useful for seasonal demand and supply. The on-demandself-service is also helpful for different demand variations and meet burst demand to some extraordinary client request. To make this conceivable, a cloud service provider should clearly have the foundation setup to consequently deal with service level agreement between users and providers. (Hou et al., 2016).

1.3 MACHINE LEARNING

ML is a discipline centered on two interrelated inquiries: The investigation of machine learning is significant both for tending to these essential logical and designing inquiries furthermore for the highly functional programmed it has provided and managed across a wide range of applications.

ML is a discipline centered on two interrelated inquiries: Machine learning research is important not only for addressing these important logical and design questions, but also for the highly effective programmed it has produced and managed across a variety of applications. A learning issue can be characterized as the issue of working on some proportion of execution when executing some undertaking, through a few sort of preparing experience. For instance, in learning (Suguna & Suhasini, 2015)

The presentation metric to be improved may be the precision of this representation classifier, and the preparation experience may comprise of an assortment of authentic Visa exchanges, each named by and large as deceitful or on the other hand not. Then again, one may characterize a distinctive execution metric that relegates a higher punishment when misrepresentation is marked not extortion than at the point when not misrepresentation is erroneously marked extortion. One may likewise characterize an alternate kind of preparing Experience for instance, by including unlabeled Master card exchanges alongside marked models. An assorted exhibit of ML calculations has been created to cover the wide assortment of information and issue types displayed across various ML issues.

Thoughtfully, MI calculations can be seen as looking through a huge space of up-and-comer programs, directed via preparing experience, to discover a program that advances the exhibition metric. MI calculations fluctuate incredibly, to a limited extent by the manner by which they address competitor programs (e.g., choice trees, numerical capacities, furthermore, general programming dialects) and in part by the manner by which they search through this space of projects (e.g., advancement calculations with surely knew assembly ensures what's more, transformative pursuit strategies that assess progressive ages of haphazardly transformed projects). (Ramharuk & Osunmakinde, 2014)

Numerous calculations center around work estimation issues, where the undertaking is epitomized in a capacity (e.g., given an info exchange, yield a "fake" or "not extortion" mark), and the learning issue is to work on the exactness of that work, with experience comprising of an example of known info yield sets of the capacity. In a few cases, the capacity is addressed expressly as a defined utilitarian structure; in other cases, the capacity is certain and gotten

through a search measure, a factorization, an enhancement method, or a recreation based system. Indeed, at the point when certain, the capacity for the most part depends on boundaries or other tunable levels of opportunity, what's more, preparing relates to discovering values for these boundaries that advance the presentation metric. Whatever the learning calculation, a key logical also, commonsense objective is to hypothetically describe the abilities of explicit learning calculations also, the inborn trouble of some random learning issue: How precisely can the calculation learn room a specific kind and volume of preparing information? How powerful is the calculation to mistakes in its displaying suspicions or to blunders in the preparation information? Given a learning issue with guaranteed volume of preparing information, is it conceivable to plan a fruitful calculation or is this learning issue on a very basic level recalcitrant? (Yashodha Sambrani, 2016)

Indeed, endeavors to portray ML calculations hypothetically have prompted mixes of measurable and computational hypothesis in which the objective is to at the same time portray the example intricacy (how much information are needed to adapt precisely) what's more, the computational intricacy (how much calculation is required) and to determine how these rely upon components of the learning calculation such as the portrayal it utilizes for what it realizes. A particular type of computational examination that has demonstrated especially helpful in later a long time has been that of improvement hypothesis, with upper and (Li et al., 2017)

1.3.1 Machine Learning Types

Comprehensively speaking, Machine Learning calculations are of three sorts Supervised Learning, Unsupervised Learning, and Reinforcement Learning. Likewise, with any strategy, there are distinctive approaches to prepare AI calculations, each with their own benefits and burdens. To comprehend the advantages and disadvantages of each sort of AI, we should start by looking at the kind of information they consume. In machine learning, there are two types of data: labeled data and unlabeled data. In a completely machine-meaningful example, marked information contains both the information and yield bounds, but it still takes a lot of human effort to label the information. In a machine-intelligible structure, unlabeled information only has one or none of the boundaries. This negates the need for human labor, but it necessitates more complex structures. There are likewise a few sorts of (*Disaster Recovery in Single and Multi Cloud Using Fuzzy Orignial*, n.d.)

1.3.2 Supervised Learning

One of the most basic types of machine learning is supervised learning. The machine learning algorithm is trained on labeled data in this case. Despite the fact that precise labeling of data is required for this method to work, supervised learning can be incredibly effective when utilized under the right situations. The ML algorithm is given a short training dataset to work with in supervised learning. This training dataset is a subset of the larger dataset, and it serves to provide the algorithm with a rudimentary understanding of the problem, solution, and data points to be handled. By the end of the training, the algorithm has a good understanding of how the data works and how the input and output are related. The final dataset is then used to train this solution, which it learns from in the same way as the training dataset. This means that supervised machine learning algorithms will improve even after they've been deployed, identifying new patterns and relationships as it learns fresh data.

1.3.3 Unsupervised Learning

Unsupervised learning alludes to the utilization of Artificial Intelligence (AI) calculations to distinguish designs in informational indexes containing information focuses that are neither ordered nor marked. The calculations are in this way permitted to characterize, mark or potentially bunch the information focuses contained inside the informational indexes without having any outer direction in playing out that undertaking. All in all, unaided learning permits the framework to distinguish designs inside informational indexes all alone. In unsupervised learning, an AI framework will group unsorted data based on similitude and contrasts, even if no classifications are provided. Unsupervised learning calculations are capable of carrying out more complex errands than controlled learning frameworks. Furthermore, exposing a framework to solo learning is one method of testing AI.

1.3.4 Reinforcement Leaning

Reinforcement learning derives its inspiration from how people acquire facts in their everyday routines. It involves a computation that improves over time and gains from new situations through the use of an experimentation technique. Good yields are energized or built up, whereas poor yields are weakened or rejected. In view of the mental idea of molding, support learning works by placing the calculation in a workplace with a mediator and a prize framework. In each cycle of the calculation, the yield result is given to the mediator, which determines if the end result is positive.

If there should arise an occurrence of the program tracking down the right arrangement, the translator builds up the arrangement by giving a prize to the calculation. On the off chance that the result isn't ideal, the calculation is compelled to repeat until it tracks down a superior outcome. By and large, the prize framework is straightforwardly attached just before the adequacy of the outcome. In ordinary support culture use-cases, like tracking down the most limited course between two focuses on a guide, the arrangement is anything but a flat out esteem. Along these lines, the program is prepared to give the most ideal answer for the most ideal award.

1.4 DISASTER INCIDENT COMMAND SYSTEM

The Incident Command System was created after a series of uncontrolled wildfires scorched California's southern region more than thirty years ago (ICS). The reaction was chaotic and disconnected at the time since there was no structure in place to combine the thousands of organizations involved in dealing with such a large-scale disaster. This resulted in extraordinary operational issues. (Vanbrabant & Joosen, 2014)

The FIRESCOPE coalition worked with the Rand Corporation and the aerospace industry to create the Incident Command System, which applied then-novel systems theory principles to a crisis situation. On October 20, 2007, the wildfires in Southern California started in Malibu, CA. The Incident Command System was developed by the FIRESCOPE alliance in collaboration with the Rand Corporation and the aerospace industry, and it brought then-novel systems theory principles to a crisis situation.

We designed a system to collect empirical data using qualitative methods such as observation, interview, and online text collecting as a sort of "rapid response analysis" to capture perishable data on social phenomena that emerge in that was updated for this case sped up the logistical process (Thomas & Valvano, 1992) In the days following the onset of the fires, one researcher deployed from her home base in Southern California to conduct observations and semi-structured interviews with persons affected by the wildfires in three Southern California counties, including emergency shelters and family support centers (Thomas & Valvano, 1992).

As evacuation orders were removed by day 10, we designed an online questionnaire about ICT usage and information collection and sharing activities to capture a wide range of perspectives from persons affected by the wildfires. The questions were developed using preliminary findings from face-to-face

interviews and previous research. On the questionnaire, there were both multiple choice and free answer text fields. We sought to investigate how people utilized ICT to communicate with others during wildfire evacuations, how they looked for fire-related updates, and how they gave their time, products, or resources, including online information dissemination.

We posted it on local forums and online publications in the relevant locations, as well as suitable Craigslist, Facebook, and Flickr discussion groups, and solicited comments (Gaur et al., 2015), We asked people to forward invitations to their friends and family. From the interviews and questionnaire findings, we learned about two independent group websites, one utilized by people of San Bernardino County and the other by a community in northern San Diego County.

As a result, we contacted the sites' administrators and conducted email interviews with them, as well as monitoring action on discussion threads on the sites during and after the disasters. The information presented in this research is based on transcriptions of audio-recorded face-to-face interviews, handwritten field notes, and responses to an online questionnaire. We present the main themes here, with data examples that are copied exactly as written or spoken by responders to highlight points.

1.4.1 Secure-Distributed Data Backup (SDDB)

In (Ueno et al., 2010), a revolutionary technique for data disaster recovery was introduced. There are six steps to the data security technique:

1) After receiving data into a data centre, the data must first be encrypted.

2) Physical randomization: A positional scrambling method is used to change the order of data files.

3) Duplication of Partitioning: Partitioning is copied by splitting data files into bits, which are subsequently reproduced according to the statement of work.

4) Secondary cryptographic: Fractions are protected a final time this happens key.

5) Trundling and Transmission: A shuffling procedure is utilized to disseminate pieces into unused memory capacities in the final stage.

The controlling center will collect all data from multiple nodes in the event of a disaster and execute Decryption (2nd) sort and merge, inverse spatial encoding, and decode (1st) activities as needed.

Romulus is a disaster-resilient device built on top of the KVM hypervisor. The fact that Remus only uses one buffer to replicate writes between the primary and backup hosts is a flaw. The discs and VM states will be out of sync, and Remus' fault tolerance will be broken if this buffer breaks before the checkpoint is sent. As a result, Romulus utilizes a fresh buffer to repeat disc writes after each Check point. The second fault is that network egress traffic is not released until the check point has been completely transferred to the storage backup host, reducing device efficiency.(Suguna & Suhasini, 2015)

1) During VM execution, it consists of disc and Replication of VM state into a fresh updates queue.

2) Failover refers to a service's ability to recover from a disaster.

1.5 CLOUD SERVICE MODELS

In cloud computing, the fundamental service model consists of three combinations. These service models describe the working and integration of various models according to respective functionalities. The service models are interdependent of each other for the provision of cloud services.

The achieved a new of the analytical approach of information systems disciplines has had the most impact, but its development has an impact on the goals and content of training as well. The technological component of the methodical system of informatics disciplines has the most impact, but its development has an impact on the goals and content of training as well. Those that work in the field of information technology have the most effect. The technological component of the informatics disciplines' systematic system, but at the same time, their growth has an impact on the training objectives and content experts in information technology (Markova et al., 2019).

1.5.1 Software-as-a-Service

SaaS (Software as a Service) is a technique of distributing software in the cloud market. SaaS, commonly characterized as cloud application services, is the most popular alternative for businesses. The internet is used to offer apps to

consumers that are managed by a third-party vendor via SaaS. SaaS (Software as a Service) is a cloud computing service. In the cloud industry, Software as a Service, often known as cloud application services, is the most extensively used option for businesses. SaaS (Software as a Service) is a technique of distributing programmers to customers via the internet, which is controlled by a third-party supplier. SaaS, or Software-as-a-Service, is a cloud-based technique of delivering software to clients. SaaS consumers pay a monthly fee to use software rather than purchasing and installing it. A SaaS application can be accessed and used from any Internet-connected device. Software-as-a-Service (SaaS) is a subscription-based licensing model that allows customers to access software from third-party servers. SaaS allows users to contact with programmers through the internet rather than installing software on their computers. (Ramharuk & Osunmakinde, 2014)

1.5.2 Platform-as-a-Service

Platform as a Service (PaaS) cloud platform services are typically used for apps and provide cloud components to specific software. All servers, storage, and networking are under the control of the company or a third-party provider, but the apps are under the control of the developers. PaaS (Platform as a Service) delivers computer platforms that typically include an operating system, programming language execution environment, database, and web server, as the name suggests. Just a few examples include AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, and Apache Stratos. Platform-as-a-Service (PaaS) is a cloud computing service that includes both a computer platform and a solution stack. PaaS (Platform as a Service) is a collection of tools and services that make it easier to create and distribute programs. (Ramharuk & Osunmakinde, 2014)

1.5.3 Infrastructure-as-a-Service

Infrastructure as a service (IaaS) is a cloud computing service in which a provider makes computational resources such as storage, networking, and servers available to customers. Within a service provider's infrastructure, organizations employ their own platforms and applications. The infrastructure as a service (IaaS) layer is the cloud computing model's base. DigitalOcean, Linode, Rackspace, Amazon Web Services, Cisco Metapod, Microsoft Azure, and Google Compute Engine are just a handful of the Iaas providers. IaaS (Infrastructure as a Service) represents your office's servers and hardware, PaaS (Platform as a Service) represents the operating system, databases, and

applications, and SaaS (Software as a Service) represents the real programmers and programs. (Jin & Min, 2016)

1.6 CLOUD COMPUTING CHARACTRICTICS

- By making it easier for users to re-provision, add, or grow technological infrastructure resources, cloud computing can help organizations become more dynamic.

- Companies who provide cloud services claim to have saved money. Capital expenses (such as purchasing servers) are converted to operating expenses in a public-cloud distribution plan. This is thought to lower entry barriers because infrastructure is normally provided by a third party and does not need to be purchased for one-time or infrequently demanding computer operations. The project includes a number of articles that go into greater detail concerning cost difficulties, with the majority of them indicating that cost savings are dependent on the types of sponsored activities and the types of in-house resources available.(Gaur et al., 2015)

- Users can use a web browser to traverse systems regardless of where they are or what computer they are using (e.g., PC, mobile phone). Because the infrastructure is off-site (usually provided by a third-party) and accessible over the Internet, users can connect from anywhere.

- Because cloud computing systems do not require installation on each user's device and may be accessed from multiple locations, they are easier to maintain (e.g., different work locations, while travelling, etc.).

- Performance is tracked by the service provider's IT professionals, and network services are employed as the system interface to create reliable and loosely linked systems.

- Scalability and flexibility with fine-grained, self-service resource provisioning in near real-time (Note: VM startup time varies by VM form, venue, OS, and cloud provider), eliminating the need for users to engineer for peak demand. This allows for scaling up as the demand for resources rises or scaling down when resources are not in use. Machine learning methods are being used to propose

effective elasticity models as part of new approaches to handling elasticity.

- Security may improve as a result of data centralization, increased security-focused funding, and other factors; however, there may be concerns about the security of stored kernels and the loss of control over important data. Security is typically on par with or better than that of traditional networks because service providers may commit resources to addressing security vulnerabilities that many users cannot afford to fix or for which they lack the technological competence.

- When data is dispersed over a bigger area or over a larger number of machines, as well as in multi-tenant networks shared by unrelated users, data protection becomes significantly more complex. Access to security audit reports may be difficult, if not impossible, for users. Users' ability to maintain infrastructure leverage while avoiding losing control of information security is a driving force behind private cloud deployments.

Every consumer, from home users to professionals, wants to keep a backup of their receptive data. And large corporations who are unable to save highly developed data on their own servers choose to hand it over to a third party. Third parties have cloud service services so that they can retrieve data from the remote cloud at any time when it is required, when it is lost in their storage, or when they are unable to recover data due to natural disasters. As users store data in the cloud, they need assurance from service providers that their data is unmovable and that third parties have the right to access it. (Jain & Jain, 2017) The primary motivation for most modern businesses and organizations to use cloud computing is to reduce infrastructure costs and benefit from information technology.

This type of problem can result in the loss of services or a complete loss of data, as well as a number of systems collapsing for a period of time. When it comes to restoring missing data, data integrity is crucial. To meet all of the requirements, a well-organized data enhancement and support method is required.

The advancement of a cloud-based system cannot be embraced without taking into account the problems that can arise when only one data centre is used. Natural and human-caused disasters often include disaster recovery, which consists of a set of laws, mechanisms, and behavior to aid in the recovery or continuity of critical technology infrastructure and systems. The following

features, such as (Zheng et al., 2014)data files are computed using structural scrambling and random address technology.

To reduce the risk of a malfunction resulting in compromised privacy, to ensure service availability and data loss, providers used two or more clouds. When we use many clouds at the same time, we reduce the chances of others obtaining public cloud resources for data and apps. The three most common barriers to using cloud services are reliability, price, and security. Using a multi-cloud architecture, an enterprise can have more autonomy and flexibility in selecting which workloads should be done and where they should be done. There are several definitions and explanations for cloud computing.

Cloud computing allows users to access their data from any location and use their software programs on any device at any time. It is possible to create a private or public cloud. Anyone with an Internet connection can use public clouds to buy services. A private cloud is a network with a distinct name that hosts services for a small group of people. Cloud computing, whether public or private, aims to provide users with quick and scalable access to computer resources and information technology services.

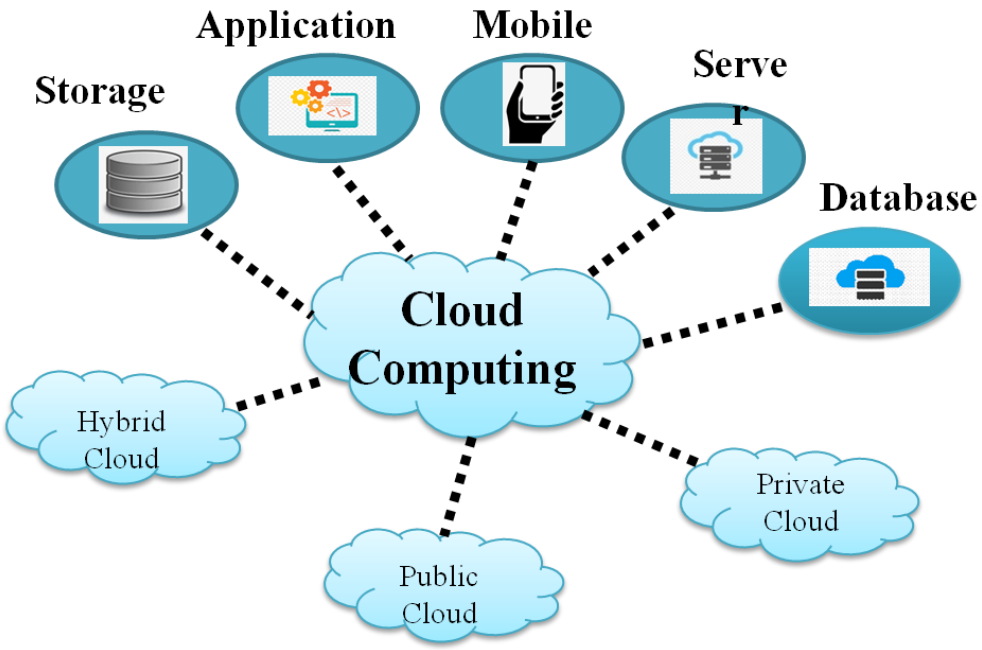


Figure 1: Cloud Computing

1.7 SINGAL CLOUD

A single cloud environment is created by using a single cloud provider to offer all software and services that the organization selects to move to the cloud. Depending on their current and future demands, single cloud settings can select between private and public clouds. For cloud providers, privacy and security should be a top priority. Customers are becoming less interested in interacting with single cloud providers due to potential challenges such as service availability failure and the risk of hostile insiders in the single cloud. A trend toward multi-cloud inter-cloud or cloud-of-clouds has evolved in recent years. (Calcaterra et al., 2019)

Protecting secret and sensitive information from attackers or unethical insiders, like as credit card numbers or a patient's medical history, is crucial. There is also research on the security challenges in single and multi-cloud cloud computing, as well as the feasibility of switching from a single cloud to a multi-cloud system. The process of shifting active transaction processing from the failed primary to the backup site is known as failover. The transition is known as a failback when the causes of the main failure have been addressed and the primary has been restored. Depending on the backup site's design and how it interacts with the primary site's functioning, a variety of options become available. The following is a typical description of the backup situation.

1.7.1 Cloud Standby

The installation of new hardware, software, and operating systems is required in this case for recovery. It could take many days for you to regain your composure. (Yashodha Sambrani, 2016).

1.7.2 Hot Standby

This necessitates the building of a second data centre capable of providing availability in seconds or minutes. If the main site goes down, a hot site will take over processing. In certain cases, the backup may include a full copy of the primary operation, eliminating the need to install the OS or the programmed. (Yashodha Sambrani, 2016).

1.7.3 Warm Standby

A choice between a hot or cold environment It's worth noting that the terms hot and warm can be used interchangeably. Different stages of rehabilitation are commonly described using tiers. The recovery time objective (RTO) and the recovery point objective (RPO), which are the main criteria that must be met when evaluating the optimal solution for a given total cost, are used to define tigers.(Yashodha Sambrani, 2016)

1.8 RECOVERY POINT OBJECTIVE

(Abualkishik et al., 2020) before disaster is proclaimed and action must be completed. The actions necessary to restore the backup server's transaction handling capabilities define the RPO. Advanced systems can backup tapes in less than a minute, whereas tape backups might take days. The recovery point target is the greatest amount of data that can be lost after a disaster, failure, or analogous event before data loss surpasses what is acceptable to an organization (RPO). An RPO specifies the maximum age of data or files in backup storage necessary to meet the RPO's purpose in the event of a network or computer system failure.

The recovery point objective (RPO) is a time-based indicator that specifies how much data loss a company can endure. RPO, or backup recovery point objective, is also crucial in determining whether a company's backup schedule is sufficient for disaster recovery. The recovery point goal is crucial since some data loss is unavoidable in the event of a disaster.

When large-scale failures occur, even real-time backups cannot completely prevent data loss. RPOs are typically tighter for high-priority workloads, necessitating more frequent backups. In these cases, the IT department will need to create backup systems that can meet RPOs, such as a hybrid of snapshots and replication (also known as near-continuous data protection, or near-CDP).

When the RPO is near zero, the team will combine failover services with continuous replication, commonly referred to as a continuous data protection system (CDP), to ensure that applications and data are available almost 100% of the time. The recovery point objective (RPO) and recovery time goal (RTO) are two of the most significant components of a data protection or disaster recovery plan. These goals can help with choosing the best data backup strategy, as well as identifying and analyzing potential approaches for resuming business

services in a timeframe that is close to the RPO and RTO.(Calcaterra et al., 2019)

The amount of real time that can pass before a disruption obstructs normal business operations in an undesirable fashion is referred to as RTO. The elapsed time and lost data of a real-world recovery process are always the recovery time actual (RTA) and recovery point actual (RPA), and they are usually different from these goals. Only through business interruption and crisis rehearsals can these facts be revealed. RPOs and RTOs will vary depending on the application and data priority. Continuous data replication inside failover virtual environments is the only way to ensure no data loss and 100 percent availability, therefore near-zero RPO and RTO for all applications is prohibitively expensive.

RPO is concerned with the amount of data lost following a failure. RTO is concerned with poor user experience and upset customers, but RPO is concerned with catastrophic concerns such as the loss of hundreds of thousands of dollars in consumer transactions. RTO is focused with systems and applications, which means that its (Brazdil & Soares, 2000)

1.9 RECOVERY TIME OBJECTIVE

The period of time between two consecutive backups, and hence the maximum amount of data that can be lost if a full restore is performed. Previously, the total amount was 24 hours. The RPO is essentially 0 if the backup is a synchronous mirrored device.

The time it takes for a failure, disaster, or other loss-causing event to occur is measured in RTO. The most recent backup, which is usually the point in time when your data was stored in a usable state, is referred to by RPOs. Any data alterations made before to the disaster or failure are usually saved during recovery efforts. Your loss tolerance, or the amount of data that can be lost before having a substantial impact on your organisation, is also referred to as RPOs. RPOs are often easier to implement than RTOs since data usage is typically consistent and has fewer variables.

The contrary is also true, (Bonvin et al., 2009) or week that the failure happened be capable of also distress the length of instant it takes to restore your data. RPOs are frequently required for higher-priority applications. Scheduled snapshot replication is required for four-hour RTOs, while continuous replication is required for near-zero-hour backups.

People are rarely prepared for disasters, which is one of the difficulties with them. In an ideal world, tragedies would be visible from afar, giving everyone adequate time to prepare and respond. In that environment, if your organization suffers a disaster, your data protection infrastructure will regenerate instantaneously, your data and apps would return to their previous state before the time and point of failure. It is possible to failover an application and replicate data with near-zero loss in the real world; however, these recoveries need a lot of resources.

1.10 DEPLOYMENT MODELS

Cloud computing offers various deployment models depending on the user requirement. The cloud deployment models are helpful in increasing the standardization of clouds and up-gradation. Four deployment models are explained below

1.10.1 Private Cloud

Private clouds are operated by single organization or company. In private cloud the organization uses web services that enable the cloud functionality. (NIST, 2011)

1.10.2 Public Cloud

The public clouds are owned and operated by the general public. Mostly public clouds offered their services free and assigned a quota for general public users. Public cloud service providers offer different computing resources like storage, computing power and network resources. (Castejón et al., 2011)

1.10.3 Community Cloud

Community cloud is a multi-tenant service architecture that distributes resources with a specific set of shared cloud computing resources. The community cloud could be hosted on-premises or by a third-party provider. The main goal of a community cloud is to engage community members to perform certain tasks and share the mutual goals.

1.10.4Hybrid Cloud

Hybrid cloud is acombination of exploitation model. Hybrid cloud is formed on the basis of organization's demands. Hybrid cloud can be public or private or community cloud. (Li et al., 2017) Cloud computing technology shows the cloud service models and their possible areas where they have deployed and utilized.

1.11 FIBER CHANNEL IN CLOUD

Fiber Channel is network architecture designed to link servers and storage devices in SANs (Storage Area Networks) in a fast and reliable manner. Although it was developed for use within data centers, it can be modified to be used over long distances, as shown by commercial goods currently available from major vendors. To control congestion and prevent packet losses, it uses complex link-by-link flow control algorithms. Since Fiber Channel technology is not based on the well-known TCP/IP/Ethernet suite, it is comparatively costly due to lower output volumes and the use of high-end transceivers and expensive mono modal fibers in the physical layer. As opposed to conventional network technologies like IP and Ethernet, fiber channels tend to be more difficult to handle. (Jin & Min, 2016)

It may be altered to be utilized across long distances, as seen by commercial devices currently available from major vendors. To reduce congestion and eliminate packet losses, complex link-by-link flow management techniques are used. Fiber Channel technology is comparatively expensive because it is not based on the well-known TCP/IP/Ethernet suite and requires high-end transceivers and expensive mono modal fibers in the physical layer. Traditional network technologies like IP and Ethernet are easier to manage than fiber lines.

As a result, they outperform high-end SAN topologies that use Fire Channel to send SCSI commands. Although storage virtualization can be achieved using a combination of the above technologies, application/server virtualization solutions such as XEN or VMware are mature enough to be used in mission-critical systems. (Gu et al., 2014)

Advanced mechanisms such as live virtual machine migration, for example, are now reliable and functional. This feature is highly useful for disaster recovery applications since a virtual machine can be moved between sites invisibly if a short idle period of a few seconds is used.

1.12 HIGH SECURITY DISTRIBUTION AND RAKE TECHNOLOGY SINGLE-MULTI CLOUD (HSDRT)

(Jiao et al., 2014) It's divided into the following sections: The most significant role is the Data Center, which is followed by the Supervisory Server and finally the many client nodes established by the administrator. PCs, mobile phones, Network Attached Storage, and storage services are all examples of client nodes. They are connected through a secure network to a supervisory server and the Data Center. The suggested network system's basic operation is divided into two sequences, one for backup and the other for recovery.

When the Data Centre receives data to be backed up, it scrambles it, divides it into fragments, and then duplicates it to a specific amount in order to meet the pre-determined recovery rate. At the second level, the Data Centre encrypts the fragmentations once more and distributes them to the client nodes in a random order. Simultaneously, the Data Centre sends the metadata needed to identify the component sequence.

The metadata contains encryption keys (at both the first and second stages), as well as fragmentation, replication, and delivery information. The Supervisory Server initiates the recovery cycle when such disasters occur, or on a regular basis. It collects encrypted invalidations from a number of vital clients, including the rake receiving process, and decrypts, merges, and descrambles them in reverse order before delivering the decryption at the second level.

However, this model has certain limitations, and as a result, it is unable to be declared as the ideal solution for backup and recovery. There are the following: In order to fully exploit the HS-DRT processor, web applications must first be well-adjusted to use the HS-DRT engine.

1.13 PARITY CLOUD SERVICE TECHNIQUE

The Parity Cloud Service approach is a disparity rescue subscription data recovery technique that is straightforward, easy-to-use, and convenient. A PCS has a low cost of recovery and a high probability of data recovery. PCS uses a cutting-edge data recovery technology that involves creating virtual discs in the user's environment, producing comparability groups across virtual discs, and storing the parity data of the parity group in the cloud. The Exclusive OR technique is used to create parity information in PCS methods.

1.14 CLOUD SERVICE PROVIDERS

Various computing needs are offered as a commodity in the business world. Customers' demands are met by service providers, who, for example, manage software or purchase costly hardware. Customers can get scalable servers via Amazon's EC2 service, for example. Another example is the Way of knowing for sure project, which brought together the National Science Foundation, Google, and IBM to provide access to a large-scale virtualized environment to academic institutions.

Customers can use a cloud provider for a variety of services, including scalability, pay-per-use, data storage and recovery, hacker protection, on-demand security controls, and network and infrastructure facilities. In addition to low costs, the public cloud offers reliability and availability. However, there are some concerns associated with open virtualization, the most prominent of which being data privacy and anonymity. Security would be a concern for any customer with sensitive data, such as medical records or financial details. (Stamelos et al., 2002)

Cloud computing is a significant advancement in the field of information technology development since it allows for self-service applications, source mixing, and broad network access. Cloud computing has increased in popularity around the world as a way to enable dispersed applications' speed, simplicity of combination, and low cost in a number of settings. As a result, merging services is becoming a popular technique to increase the amount of cloud computing applications available by reusing existing services.

1.15 SECURITY RISK IN CLOUD COMPUTING

Security issues play a crucial role in the cloud computing environment, notwithstanding the benefits that cloud service providers can bring to consumers. Users of internet data sharing and network services are well aware that their privacy may be jeopardized. According to a recent survey, security is the top concern for 74 percent of CIOs when it comes to cloud computing. Protecting private and sensitive information from attackers or malicious insiders, such as credit card details or patient medical records, is crucial. (Hou et al., 2016)

Data storage security, application security, data transmission security, and security tied to third-party resources are among Subashini and Kavitha most pressing security concerns. Consumers and providers have varying security responsibilities depending on the cloud service model. According to Amazon,

security management in terms of physical, environmental, and virtualized security is covered by Amazon's EC2, but users are still responsible for the security of the IT system, which includes operating systems, applications, and data. (Ölveczky & Thorvaldsen, 2006)

Users are responsible for the security of their operating systems and apps under IaaS, while cloud providers are responsible for their customers' data security. According to Ristenpartet al., the levels of security concerns in IaaS are distinct. Security concerns are more prevalent in the public cloud than in the private cloud. Any compromise of the physical infrastructure's security, or a flaw in the infrastructure's security management, for example, would cause a flood of issues.

A security risk in the cloud environment may impact the physical Data processing and storage is handled by this network. Furthermore, the path for sent data can be changed, especially when data is delivered to a large number of third-party infrastructure devices. Because cloud services are dependent on the Internet, any security risk that affects the internet will also affect cloud services. Even if the cloud provider priorities security in the cloud architecture, data is still transferred to customers across potentially insecure networks because cloud services are accessed via the Internet.

The cloud makes use of technology similar to that found on the Internet. Encryption mechanisms and stable protocols are insufficient to protect data transmission in the cloud. Hackers and cybercriminals must not be able to access cloud data through the Internet, and the cloud environment must be safe and secure for clients. We'll go over three specific security challenges that single clouds face: Referential integrity, data tampering, and service availability are all factors to consider.(Bedi et al., 2019)

1.16 SINGLE AND MULTI-CLOUD ENVOIRMENT

Methods for task scheduling can be employed in either a single cloud or a multi-cloud context. A single cloud method relies only on cloud providers because there is only one cloud server. As a result, at any time, one SaaS, PaaS, or IaaS service can be supplied. Network monitoring is simple in this environment, but if a cloud server fails, the entire system fails. The multi-cloud strategy in a cloud computing system is the simultaneous employment of two or more cloud services to lessen the risk of data loss or downtime due to a localised component failure. Software, equipment, or networking can all fail in this way.

Cloud services that are accessed by service cloud providers are referred to as multi-cloud. A multi-cloud strategy would improve overall business efficiency by avoiding vendor lock-in and employing multiple architectures to fulfil the needs of varied partners and customers. (Zhang et al., 2017)

A multi-cloud strategy can also aid an organization in reducing website load times for all types of content. Not only can a multi-cloud method provide the Redundancy in software, architecture, and equipment is required for fault tolerance, but it can also route traffic from various customer bases or collaborators through the network's fastest sections. Multiple clouds, often known as multi-clouds, can be run in four different ways:

Parallel multi-clouds: inside this process, several suppliers collaborate on a cost plan to create a correlated cloud.

Inter-clouds: in this system, clouds are grouped into sets based on common conventions like naming, identification, addressing, time zones, and trust.

Multi-cloud: Suppliers join together to establish a federation, which recommends/consumes resources through a series of phases that include resource discovery, authentication, and matchmaking.

Multi-cloud suppliers propose various facilities, such as tools, software, and networks, in this method of sky computing. By combining available resources with dynamic support for real-time requests, this architecture will provide new value-added services. The openness of a multi-cloud system is one of the most important aspects of sky computing. This architecture, in particular, gives the impression of a single cloud with an infinite pond of capital. (AlZain et al., 2012)

1.17 MULTI-CLOUD SERVICE COMPOSITION MECHANISMS

This section introduces and examines various significant multi-cloud service combination approaches. For multi-cloud scenarios, Zou et al. proposed service combination architecture. Three service composition techniques are described in order to find a suitable cloud composition with the fewest number of clouds possible. All clouds, base cloud, and smart cloud are terms used to describe this system. All clouds are included as inputs to the combination in the all clouds composition approach, which looks for all potential solutions. While this method is successful in identifying a service combination with a short

implementation time, it is unsuccessful in reducing the number of clouds in the prior service combination.

1.18 ANALYSIS OF MULTI-CLOUD RESEARCH

For a variety of reasons, moving from single clouds or inner-clouds to multi-clouds is rational and important. Single cloud services are also experiencing outages. According to the report, over 80% of corporate leaders are concerned about security risks and a lack of control over data and systems. Assumes that shifting to inter clouds is mostly for the aim of expanding what was previously available in single clouds by distributing reliability, trust, and security across multiple cloud providers. Multi-clouds could also benefit from secure distributed storage, which uses a subset of BFT techniques.

Intercloud protocols have been developed as a result of a number of recent studies in this field. For example, RACS (Redundant Array of Cloud Storage) uses RAID-like principles similar to those used by discs and file systems, but with the inclusion of multiple cloud storage. Spreading a user's data over various clouds, according to Abu-Libdeh et al., is an effective approach for avoiding vendor lock-in. This replication lowers the expense of switching service providers while also improving the tolerance for failure.

In present an inter cloud storage (ICStore) architecture that comes closer to RACS and HAIL in terms of providing a dependable service across multiple clouds. Scienceint is working on new concepts and ways to address the difficulties of cloud-based data confidentiality, honesty, consistency, and reliability. As previously reported, DepSky is a virtual storage cloud system that aggregates many clouds to create a cloud of clouds. In comparison to DepSky, Bessani et al. fix some of the shortcomings in the HAIL procedure and the RACS scheme. HAIL doesn't offer data security, requires code execution on their servers, and doesn't deal with data variances.

The RACS solution differs from DepSky in that it tackles economic failures and vendor lock-in, but not cloud storage security problems. It also lacks any means for ensuring data security or providing updates to previously recorded information. Finally, unlike previous multi-cloud studies, the DepSky technique allows for the analysis of many clouds in an experimental setting.

Several attempts have been conducted to establish consistency from untrustworthy clouds. Because Mahajan et al. believe cloud storages are dangerous, Depot, for example, boosts the flexibility of cloud storage in a similar way to DepSky. Depot, on the other hand, offers a less expensive option based on

the use of single clouds, but it will not accept data loss, and the efficiency of its service is dependent on cloud dependability.

1.19 MULTI-CLOUDS: PRELIMINARY

These concepts imply that cloud computing does not have to be limited to a single cloud. A gloomy sky, for example, mixes a variety of cloud tints and patterns, resulting in a diversity of implementations and administrative environments. Recent studies have concentrated on the multi-cloud environment, which manages numerous clouds without relying on any of them. Identify two levels in a multicloud setting: the inner-cloud at the bottom and the inter-cloud at the top.

In the interclouds, the Classical type of resistance finds a home. We'll start by going over the preceding three decades' worth of Byzantine protocols. Byzantine faults are software or hardware problems in cloud computing that typically pertain to inappropriate behavior and intrusion resistance. There are also arbitrary and crash faults in it. Classical Condition Monitoring has been the subject of extensive research since its inception (BFT). Although BFT research has received a lot of attention, it still has some functional constraints and is only deployed in a few distributed systems.

As previously stated, BFT guidelines are not unique to individual platforms. According to Vukolic, one of the disadvantages of BFT for the inside is that it, like all fault-tolerant protocols, requires a high degree of failure independence. If a cloud unit encounters Byzantine failure, it is reasonable to utilize a different technology, implementation, and hardware to prevent the failure from spreading to other cloud nodes. Furthermore, if a specific cloud is targeted, the attacker may be able to gain control of the cloud's inner-cloud infrastructure.

1.20 RESSEARCH OBJECTIVE

- Designing of a framework to evaluate Disaster in clouds.
- Designing a smart decision-making framework to disaster intelligently to achieve higher accuracy.
- Formulating a model recovery for disasters in clouds.

1.21 PROBLEM STATEMENT

Elasticity, reliability, scalability, service orientation, and availability, cloud computing has been a top trend in IT software and technology for the past years. It is an age of technology, cloud services are being monitoring in our daily life facilities and comforts. Abnormalities are linked to harmful outcomes that have direct impact on human privacy. Occupancy detection has an important job in lots of cloud applications, for example, Data Cost, Data Dependency, Data Storage, Data Security and Data Reliability. In previous system different Artificial Neural Network algorithms were applied to the dataset, taking cost, security, storage and reliability. As a result, the system reacts to any event relevant to the observed phenomenon by decision-making and derives the necessary decisions to identify events immediately. In this proposed research, a fuzzy-based recovery monitoring system is introduced to monitor disasters in clouds.

1.22 RESEARCH QUESTION

The following research questions are being introduced for this research.

- How to establish a mechanism for Disaster Recovery in clouds?
- How fuzzy logic can help in Disaster of single multi cloud?
- How to formulate categories of various factors for Data recovery, Cost effective Storage, Data Reliability, Data Dependency, Data Security?

1.23 METHODOLOGY

The above mention discussion helped in formulating the following methodology for this research;

This helped us to integrate the existing work and identify our strategy in broad manner. We made an in–depth study of Disaster recovery tools, revealing their benefits, challenges and applications. The prime focus of our study is to provide comprehensive knowledge to all users to decide which tools are better to meet their need.

1.24 THESIS STRUCTURE

In this dissertation, first chapter provides the background on cloud computing, different disaster recovery, problem statement and methodology. The second chapter provides the relevant literature of selected papers by keeping in view the problem statement. The third chapter provides the proposed methodology and proposed model while the fourth chapter provides the proposed algorithm for intelligent cloud disaster recovery. The fifth chapter provides the simulation results for intelligent cloud disaster recovery using MATLAB. Sixth chapter gives the conclusion of the dissertation. Seventh chapter highlights the limitation of this research while eighth chapter gives the future work related to this research.

1.25 CONCLUSION

In this chapter we have provided the background of numerous segments related to our research. Various cloud types and services have been discussed; similarly, the concept of disaster recovery and different types of these facts has been highlighted. Further discussion covers disaster recovery in clouds constituents along with performance criteria to understand the existing practices for disaster recovery in clouds development and maintenance. Last section of this chapter provides the research objectives, research questions and formal problem statement along with methodology.

CHAPTER 2

LITERATURE REVIEW

Disaster recovery approaches for information technology data, applications, and systems should be improved. Data and its networking, notebooks, wireless devices, servers, networks, and desktops are all part of it. The recovery time for an IT resource should be determined by the recovery time objective feature or mechanism for that IT resource. Software, hardware, data, and networking are all required components of information technology systems, and if one is missing, the system may not function properly. A data recovery plan is a vital law to follow in order to prevent a company from suffering loss and/or incurring unnecessary costs. Data recovery is the most important worry in disaster recovery, regardless of where the disaster is generated by a major catastrophe such a fire, flood, or weather, or by data theft, a human-made problem, or another power outage. A disaster recovery plan is needed so that everyone is aware of the types of steps that must be taken in the event of a disaster. (Laituri & Kodrich, 2008)

2.1 SINGLE CLOUD STRUCTUAL DESIGN

In this scientific world, storage system management is a hotly disputed topic. The introduction of new Cloud technologies has recently sparked renewed interest in the subject. Furthermore, there are currently few articles in the literature that focus on an MCS platform's data transport. In a Network Storage Environment, the investigators propose a method for simplifying file partitioning. They provide a way for distributing files efficiently inside a cluster while maintaining reliability, availability, and serviceability. They focus on the ability to divide files into blocks that can be shared across much energy storage. When a laptop is misplaced or stolen, the makers of solved the problem.(Bonvin et al., 2009)

Because it necessitates certain kernel configurations, the approach is difficult to apply to scale scenarios. The files are segmented even in this case. The replica technique based on chunk weight encouraged them to popularize the concept of "portion placement." A similar method is also discussed. The authors introduce PRESIDIO, a framework for evaluating similarity in object storage and decreasing or minimizing repetition. The authors describe a method for file partitioning optimization in a digital backup system. The model developed by

the authors shows how a partitioned network can maintain a high level of availability. (Usman et al., 2017)

Cloud computing has nothing to do with the works stated above. When it comes to huge data storage solutions in Cloud computing, the authors discuss how File sharing will provide possibilities for many organizations to handle a rising number of data. Berry Store is a decentralized offsite replication system developed for Cloud services, specifically for storing massive numbers of little data, according to the creators. Thanks to a distributed coordinated controller, the proposed system can provide stability, throughput, and failure. File blocking is one of the most critical aspects of large-scale data storage. To address file storage restrictions and parallel computing support challenges in fixed-blocking storage, the authors propose a smart-blocking file storage solution. By putting up six grouping factors, the acceptable approach may evaluate whether the file should be effectively stopped or not based on the size of the file and the consumer connectivity. The authors investigated the Cloud application requirements for supporting data-intensive applications at the Infrastructure as a Service (IaaS) level.(Mendonca et al., 2018)

After the massive penetration of Cloud Computing, an ever-increasing number of designers are considering moving their applications to the Cloud, in close connection with application relocation, an expanding number of improvement and execution stages, conveyed as PaaS arrangements are putting forth their administrations for advancement, sending, and execution of uses that are utilizing as a part of an ideal way the five attributes of the Cloud. (Lindman et al., 2016) The presentation of a brought together segment, the Cloud Governance, is fundamental maintenance in intelligence the last part ambition to empower the improvement of complex single cloud environments. This brought together part is expanding, supplementing, finishing and incorporating centre elements from the PaaS layer, such as observing provisioning, arrangement, and others, and coordinate elements of the different Cloud recovery system. (Cunningham, 2015)

2.2 MULTI CLOUDS STRUCTURAL DESIGN

The conception of a multi-Cloud backup system has been expanded beyond individual viewers to Cloud operators who want dependable storage as a service. As a result, a generic private, public, or hybrid Data center controller in need of distant storage space, dubbed Home Cloud, can rely on a theoretically endless hybrid Multi-Cloud Storage (MCS) space made up of various Cloud storage capabilities offered by multiple owners. We designed an MCS module prototype for this purpose, which allows a home Cloud to use a hybrid multi-

Cloud storage system. We tested the complete MCS system in order to make a recommendation on how to configure it. The MCS system is more difficult to set up than anticipated since several elements must be considered while distributing files. To do so, we study the MCS ecosystem as a whole, as well as the performance of individual Cloud storage providers. We investigate how Cloud storage providers' upload and download capabilities might be used to choose where data portions should be stored, as well as how de-duplication policies and synchronization activities improve system efficiency.(Gaur et al., 2015).

While there are several Cloud anthologies, the categorization of cloud Platforms is unclear, and the distinction between differing definitions is ambiguous. As a result, we believe it's critical to identify Multi Cloud from other cloud architecture.

Cloud computing, the Sensor networks, and cognitive technologies are quickly becoming the most powerful applications of our time. The author proposed an improved healthcare system. Smart clothing will be next generation healthcare system using machine intelligence. (M. Chen et al., 2017)

There are two types of methodologies in many Clouds: Federalized Computing and Multi-Cloud. The degree of coherence between the Clouds involved, as well as the users contact with the Clouds, affects the difference, according to the various Cloud vendors in the first model have agreed to share their resources, whereas there is no such agreement in the second model. The two models are classified in the same way based on the type of co - operation: voluntarily, in Federation, or not, in Multi-Cloud. In the first model, the user interacts with one Cloud and is unaware that the information or functions used belong to a different Cloud.

In the second model, the subscriber is familiar of the many Clouds and is authorized for service or resource delivery, or a third party is. The term Multi-Cloud can refer to a client's or a service's utilization of several and independent Clouds, according to the above classification and proposal. The Federated Cloud meets the needs of cloud providers. The key driving force is the necessity for N9, for the most part to attain fresh wherewithal owed to the scarcity of existing ones? Conversely, N2 and N4 can also be there causes for its use, particularly in the case of regional limits or internal cost-cutting policies. The Multi-Cloud approach meets the needs of cloud clients.

The fusion in academic institutions, Cloud is following the Grid approach by developing Community Clouds, such as Open Cirrus (opencirrus.org). Agreements between large Cloud providers, on the other hand, are difficult to

reach, especially when the external provider is expected to contribute resources and services for the internal provider's advantage.(Thomas & Valvano, 1992).

2.3 DISASTER RECOVERY IN CLOUDS

For long-term sustainability, a company must have a disaster recovery plan in place. Virtualization technology makes hardware independent of the systems it runs on, allowing operating systems, software apparatus, and companies to move data to the cloud while improving financial efficiency. The growing number of cloud service providers enables their customers to recover from disasters faster and with less downtime. Sensitive programmers, for example, are held on Amazon's cloud in different data centers around the globe. Amazon's employees have been unable to achieve a completely functional design. When a short-phase disruption occurs at one site, the consumer is notified and the program is shifted to another location automatically. Any interfaces and processes that rely on this application are protected by electrical systems. For disaster recovery to be successful, information that is critical to a company must be backed up on a regular basis and securely stored in multiple locations.(Zheng et al., 2014).

Disaster recovery systems must ensure that active applications are not disrupted and that these applications are easily restored following a disaster represent a part of the business continuity organization that oversees the recovery of information technology systems and procedures. Because of its potential to provide services that are cost efficient, reliable, and efficient, cloud computing is a significant aspect of operations for a range of enterprises. If a user wants to use these services, they must pay for them and only use them when necessary. The consumer benefits from lower costs, faster deployment, versatility, and dynamic scalability. Even so, virtualization has yet to gain widespread use regarding security concerns. Privacy and security concerns were the primary reasons for not using the cloud. The majority of these service providers have issues with their users' data. The following are the most pressing issues that a company faces while moving to the cloud: the ability to manage deployments across many Clouds is a key aspect of the Multi-Cloud. (Id, 2019).

Beyond the production-ready management tools, the research community is working hard to enable the development of novel Multi-Cloud solutions. We only name a few of them in this section. Does a more in-depth investigation. A multitude of causes can lead to vendor lock-in, including services with solid financial preservation, a scarcity of complete applicability of specifications, exclusive APIs, and so on. The issue isn't always a result of vendor preferences,

but it can be a reflection of the wide range of hardware and software stacks that are required to develop a Cloud examine.

This layout should always be defined by translating the development platform, including its subsystems and relationships, onto a variety of offerings while keeping performance, cost, and security constraints in mind. In this study, we specifically address four performance constraints that are relevant to achieving the resource requirements of 85 each instance type in terms of computational resources use don't take into account the overall application's perceived performance, which is normally measured outside requisites of reaction time and throughput. In terms of security, we're looking for a deployment option that lets us to meet existing security criteria for each individual component as well as the application 90 as a whole. Furthermore, we assume that Service Level Agreements (SLAs) be used to express the security features of both available cloud services and built components and applications (SLAs). (Gamez, 2008).

The composition of Cloud services is obligatory when a particular Cloud service unable to satisfy the user requirements. The composition includes numerous tasks like selection, checking, discovery, compatibility, and deployment; it is a difficult process because users find it hard to select the optimal one among them if all possible compositions are not available. Cloud service composition is a new challenge triggered by diversification of users, services or applications deployed through the transformation of geographical locations with different legal constraints. The crucial problem is to handle the combination of virtual resources and infrastructure to select them according to user requirements. In this research, a framework and algorithms are proposed in the cloud to simplify service composition for unqualified users. (Bangui et al., 2017).

2.4 DATA COST

The rate of data improvement is expected to be lower. According to the percentage of users, the lower the rate of data recovery, the better; this low cost is the answer magnetism in favor of the consumer. Cost is a significant thought while utilizing cloud assets. Subsequently, regardless of whether a client may essentially need to speed up an information escalated task through scaling up in the cloud, the caused cost might be restrictive. The client may hence acknowledge a more extended fruition time for brought down costs. This would regularly infer that a piece of the cloud-occupant information will be executed by neighborhood assets. The general objective for this method of execution is to limit the season of execution while remaining under a client indicated cost

requirement. It ought to be noticed that the compromise between the expense and season of execution is nontrivial for two reasons. In the first place, in most cloud conditions today, there is an expense related with recovering information for handling outside of the cloud.(Bonvin et al., 2009).

Second, the expense is subject to not just the quantity of cases utilized, yet how long they are utilized. The information proprietor rents extra room in information workers in a few server farms all throughout the planet and pays a month to month utilization based genuine lease. Each virtual hub is answerable for the information in its vital reach and ought to consistently attempt to keep information accessibility over a specific least degree of certainty while limiting the related expenses (for example dormancy and cost). To this end, a virtual hub can be accepted to go about as an independent specialist for the information proprietor to accomplish these objectives. Time is thought to be parted in ages.

At every age, a virtual hub might recreate or relocate its information to another worker or self-destruction (for example erases its information copy). It additionally pays a virtual lease, which is characterized later in this segment and it is an intermediary of the conceivable genuine lease, to the worker where its information is put away. These choices are made dependent on the question rate for the virtual hub, the leasing costs and the upkeep of high accessibility upon disappointments. There is no worldwide coordination and each virtual hub acts freely. The virtual lease of every worker is reported at a board and is refreshed toward the start of another age.(Badhel & Chole, 2015).

IoT based disaster recovery can cost big processing cost. In this paper, author highlighted the recovery and performance requirements for damage devices. Data processing applications over IoT and big data using machine learning algorithms for data processing through network cost and increased processing demand using devices raspberry Pi and Intel base server. During the evaluation, on both devices can be processed the data more efficiently to achieve better energy and performance using machine learning algorithms. (Cui et al., 2017).

2.5 REMOTE DATA BACKUP SERVER (RDBS)

With one important exception, remote backup software works similarly to regular data backup software. Backup online backup software provides backups to your online backup server, which is safely offsite, rather than a tape drive as well as other mainstream press connected to the machine being backed up, over the Internet or other network connections. It does this (typically) at night when no one is using the computer. On-demand backups are also possible

at any moment. It's entirely automated. It's possible that you'll forget it's on. (Badhel & Chole, 2015).

Using a virtual, software-defined architecture, providers can build a large storage pool and then share it among their clients. They can not only manage the entire commodity right to the node level, but they can also use multi-tenant systems to keep client accounts separate so that data from one client does not "bump" into that of another. If your backup provider allows you to choose a third-party storage destination, you'll see that many of them also offer infrastructure as a service (IaaS), such as Amazon Web Services. While you still can build servers and use them as restoration destinations in these clouds, the majority of them have dedicated storage services that appear as network drives to users and software. That's great for flexibility, but bear in mind that the cost of these services, as well as the cost of safeguarding data stored there, should be incorporated into your overall secondary budget estimates.

In addition, if the main cloud's network access is unavailable, they will collect data from a remote cloud. The following criteria must be met by remote backup services.(Kanwar et al., 2019).

2.6 DATA INTEGRITY

In backup and recovery services, data integrity is crucial. It is concerned with the server's complete state and structure. It verifies the information so that it is unchanged during transmission and collection. It's a metric for how trustworthy and dedicated the information on the server is. Data respectability involved to the unwavering quality and dependability of information all through its lifecycle. It can depict the condition of information e.g., substantial or invalid—or the method involved with guaranteeing and safeguarding the authority and correctness of information. Data integrity refers to the quality and stability (significance) of evidence during its tenure. It seems, organizations have little use for compromised data, let alone the hazards associated by sensitive data loss. As a result, many business security solutions place a high focus on data integrity. The integrity of data can be harmed in a variety of ways. Data should be duplicated or moved in such a way that it is unaffected by subsequent changes. Error checking methods and validation procedures are often employed to preserve the integrity of data that is transferred or reproduced without the intent of tampering.

In case to take a well-organized cloud service, it can be meet the user's privacy safety demand and trust. This article preferred a cloud service assessment model based on privacy- up to date and trust. The model launches

the time failure factor to explain the problem that the trust passage changes extra, proceed into account independent deal amount given independent weights, it maps the straight trust determining process based on combining weights and service attributes, revolving the straight trust timeliness, coherence. Simultaneously, the model takes a Standard cloud model of a technique for privacy data safety, in case the user can select authentically, trusted operation to interact. (Wagle et al., 2016)(Manzoor et al., 2016).

2.7 DATA CONFIDENIALITY

User data files must always be kept private; File formats that are personal to a single client must be smart enough to hide from those other clients on the clouds when accessed, even if a large number of users are using the cloud at the same time. Data Confidentiality manages securing against the disclostire of data by guaranteeing that the information is restricted to those approved or by addressing the information so that its semantics stay available just to the individuals who have some basic data (e.g., a key for sorting out the enciphered data). A critical component of privacy is that it helps assemble trust. To have their data shared isn't just a break in protection; however, it will annihilate representative trust, certainty and unwaveringness. It will likewise cause a misfortune in efficiency. Severe information insurance rules should be followed while overseeing private data.

In this paper, author proposed a trust management structure for network vitalizing environments. The proposed framework aids differentiate between the infrastructure contributor based on their response and past skills from service contributor. The author highlighted the major elements included in gathering the response and organizing the repute data. In proposed trust system, the idea of degree of Involvement of an infrastructure contributor regarding connections and nodes are discussed. Pretending output assures the efficiency of proposed to the trust management system in improving the service of contributor to achievement and decreasing the selection of infrastructure contributors that don’t complete their Service Level Agreement (SLA). As well as trust management system, service contributor is inspired to work only with highly reputable infrastructure contributors for VN determined. (Ecurity, 2017)

2.8 COST EFFICIENCY

Recovery should be less expensive. The bigger proportion of users, lower the cost of recovery. Cost efficiency is the act of saving money by altering a product or process to work more efficiently. This is done to improve the

financial position of the company by cutting procurement costs and enhancing operational productivity. Businesses must find the best potential return on every dollar they spend in order to compete successfully, obtain the resources they need to expand and develop, and generate a healthy bottom line. Finding ways to attain and improve cost-efficiency is a critical component of any long-term business plan. Cost efficiency approaches, being one of the most widely employed business efficiency tactics today, may be used effectively by enterprises of all sizes and sorts.(Shaikh & Sasikumar, 2014)

Cost-cutting methods, when combined with the correct software and digital technologies, may help businesses make more strategic decisions that drive innovation, transform procurement into a value-creation centre, and lower operating costs while enhancing operational efficiency and profitability. In a commercial cloud computing environment, wireless carriers have their own priced systems for billing consumers. The three basic categories comprising cloud resources are computation, storage, and bandwidth.

2.9 CONCLUSION

This chapter has provided a detail review of research conducted by other scientists in relevant domains like cost efficiency, data integrity and remote data backup system. From distributed networks to the role of agency in cloud computing is covered along with emerging trends and challenges in the domain of disaster recovery or more precisely intelligent cloud computing. Existing work has shown the interest and efforts done by many researchers in the domains related to problem statement, there are various solutions proposed for disaster recovery in terms of storage, intelligence, and service management and performance measurement. All these segments give directions to establish a model for an evolvable and disaster recovery in clouds.

CHAPTER 3

PROPOSED EVALUATING PERFORMANCE OF DISASTER RECOVERY USING FUZZY INFERENCE SYSTEM

Fuzzy memory is a type of logic in fuzzy mathematics where the actual value can be a real number between 0 and 1, inclusive. It's being worn to arrangement with half-truth, wherein the true value can range from absolutely true to absolutely false. However, in Boolean logic, a variable's true value can only be the input variables 0 or 1. However, fuzzy logic had been studied as infinite-valued logic since the 1920s, primarily by UKasiewicz and Tarski. Fuzzy logic is founded on the assumption that decisions are made focused on inelegant

These approaches can identify, define, modify, analyze, and utilize ambiguous and unreliable relevant data. From systems engineering to artificial intelligence, fuzzy logic has been employed in a range of applications. Fuzzy logic is a type of processing that uses "levels of validity" instead of the usual "true or false" (1 or 0) Boolean logic that currently underpins computers. Consider fuzzy logic to be the true essence of thinking, and basic, or Logical, reasoning to be a component of that as well.

3.1 CAPABILITY OF PROPOSED FUZZY SYSTEM

The suggested Platform's capabilities include determining the categorization of services supplied by server less computing providers, managing the variety of various operations offered by various recovery vendors, and classifying readily available cloud goods through the network, management of versatility of different services offered by various recovery vendors and classified readily available cloud products over the network.

- A wide range of AI systems and technologies employ fuzzy logic. Examples include machine navigation, consumer electronics, medicine, software, chemicals, and aerospace. In automobiles, fuzzy logic is used to choose gears, and it is affected by factors such as engine load, traffic environment, and driving approach.
- In dishwashers, fuzzy logic is used to determine the washing approach and produce a quality, which seems based on factors such as the type of dishes and the amount of food residue on the dishes.
- In fax machines, fuzzy logic is utilized to modify the drum voltage based on variables such as humid, visual frequency, and altitude.

- In the aircraft industry, fuzzy logic is utilized to govern satellite and spacecraft altitude control based on environmental parameters.
- Fuzzy logic is worn in natural language processing to detect semantic relationships between words and other linguistic characteristics.
- Fuzzy logic regulates output in environmental control systems like air conditioners and heaters based on factors like present temperature and goal temperature.

Fuzzy logic can be utilized in a business rules engine to speed up decision-making based on specified criteria. The truth value of variables in a fuzzy inference system can be any real number between 0 and 1, which is a sort of many-valued logic. It's used to deal with partial truth, in which the truth value can be somewhere between true and false. As a result, we can define fuzzy inference as a method for interpreting the values in an input vector and assigning responsibilities to the output vector using a set of rules. In fuzzy logic, the truth of any sentence becomes a matter of degree.

3.2 EVALUATING THE PERFORMANCE OF DISASTER RECOVERY IN CLOUD MODEL

The proposed model for evaluating the performance of disaster recovery in cloud consists of following five major modules

- Data Cost
- Data Security
- Data Reliability
- Data Dependence
- Data Storage

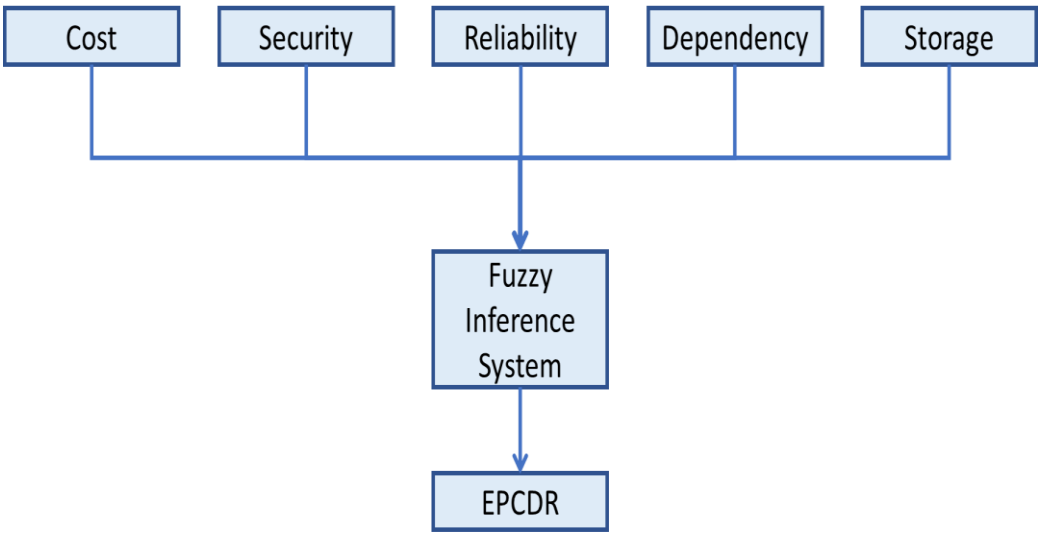


Figure 2: Proposed Model for Evaluating EPCDR

3.2.1 Data Cost

The rate of data improvement is expected to be lower. According to the percentage of users, the lower the rate of data recovery, the better; this low cost is the answer magnetism in favor of the consumer. Cost is a significant thought while utilizing cloud assets. Subsequently, regardless of whether a client may essentially need to speed up an information escalated task through scaling up in the cloud, the caused cost might be restrictive. The client may hence acknowledge a more extended fruition time for brought down costs. This would regularly infer that a piece of the cloud-occupant information will be executed by neighborhood assets. The general objective for this method of execution is to limit the season of execution while remaining under a client indicated cost requirement. It ought to be noticed that the compromise between the expense and season of execution is nontrivial for two reasons.

In the first place, in most cloud conditions today, there is an expense related with recovering information for handling outside of the cloud. Second, the expense is subject to not just the quantity of cases utilized, yet how long they are utilized. The information proprietor rents extra room in information workers in a few server farms all throughout the planet and pays a month to month utilization based genuine lease.

3.2.2 Data Dependency (DD)

Users of cloud services have no control over the structure or content of their data. The need for a reliable service provider is a major red flag for businesses considering moving to the cloud. Application Dependencies happen when innovation parts, applications, and workers depend on each other to give a business arrangement or administration. Understanding underlying cloud architecture and as well as possible disaster situations. Getting hold on your app's API connections and consumer interactions. On the basis of these requirements, develop a comprehensive monitoring strategy. At the point when engineers construct arrangements, they would so with a specific innovation stack in care.

3.2.3 Data Storage (DS)

When the use of cloud computing grows, so does the number of records that must be stored. As a result, cloud once-over provider's data storage security is at menace of crash along with a specific storage location. Point mists are regularly named being scanty or thick relying upon the point thickness utilized in addressing the objective article. With respect to their capacity in any case, point mists are data wise thick Maybe than meager, which would suggest many missing qualities. A lot of various characteristics or properties are related to each point in a point cloud. Other than the XYZ arranges and the RGB shading esteems, there are for example extra credits identified with the occurrence laser beat (e.g., power, check point and return-related information) just as some semantic information, which is commonly a whole number worth that orders the designated object. By and by, we can expect that the complete number of properties will stay much of the time well under 50. In this regard, point mists can be described as being upward limited. As a difference, in Reference the creators use the term 'wide' for datasets that comprise of hundreds if not of thousands of various properties.

The capacity of point cloud documents, tremendous as they might be in their number of focuses, should introduce forget about it, for circle stockpiling can be viewed as basically free. Moreover, the slow expansion of glimmer based strong state-drives (SSDs), which have no moving parts, implies that the aggregate arbitrary access idleness (i.e., the look for time + the rotational dormancy) will be insignificant. This infers that getting quick reaction times from a point cloud question basically requires diminishing the information move time; that is, the time needed to stack the information from plate into memory.

All the more exactly, what is required is an effective ordering plan to rapidly find the ideal focuses. With a point cloud, the list is involved the XYZ organizes, which unexpectedly additionally convey the primary data.

As to nature of point mists, we share the view proposed by in that since point mists have some normal attributes with both raster information and vector information, it is helpful to consider them as a class separated. We note that has brought up in Reference, since point cloud information isn't related with a normal network, it tends to be named unstructured information. Moreover, point mists can be described as being generally static informational collections once handled and cleaned, there is little requirement for adjusting or refreshing them. This shortfall of a dynamic dataset implies that the information handling needs of point mists are altogether different from a serious exchange based handling including heaps of updates.

3.2.4 Data Security

Disaster recovery services should consider the security of important documents as well as rapid data recovery. There are two types of disasters: human-caused and natural disasters. The remote server's ultimate requirement is to provide complete security to the customer's information.

Deploying data bases to massive data centers introduces a slew of security difficulties, including virtualization flaws, openness flaws, security and control issues associated with data accessed from the outside, credibility, confidentiality, and data loss or robbery. Present some key security challenges, such as data storage security, application security, and data transmission security. The security obligation between clients and suppliers varies depending on the cloud administration type.

A security risk might have an impact on the actual framework that is responsible for information handling and storage in the cloud. Additionally, the manner in which the communicated information is conveyed might be impacted, specifically when the information is conveyed to some external framework gadgets.

Each virtual hub is answerable for the information in its vital reach and ought to consistently attempt to keep information accessibility over a specific least degree of certainty while limiting the related expenses (for example dormancy and cost). To this end, a virtual hub can be accepted to go about as an independent specialist for the information proprietor to accomplish these objectives. Time is thought to be parted in ages. At every age, a virtual hub might recreate or relocate its information to another worker or self-destruction (for example erases its information copy).

3.2.5 Data Reliability (DR)

If various unnecessary sites are used, it is modernized, resulting in fine measured cloud computing that is acceptable for business unity and disaster recovery. Administration accessibility is another major concern in cloud administrations. Amazon mentions in its authorising agreement that the help may be unavailable from time to time. If any client's records violate the distributed storage method, the client's web administration may be terminated at any time. Similarly, if any harm occurs to any Amazon online administration and the administration falls short, the Amazon Organization will not be held liable for the failure.

These features protect customers against Amazon data breaches as well as programmers who may have gained access to their email or stolen their secret word. It additionally pays a virtual lease, which is characterized later in this segment and it is an intermediary of the conceivable genuine lease, to the worker where its information is put away. These choices are made dependent on the question rate for the virtual hub, the leasing costs and the upkeep of high accessibility upon disappointments. There is no worldwide coordination and each virtual hub acts freely. The virtual lease of every worker is reported at a board and is refreshed toward the start of another age.

In aggressive fill material, only the pivot order, which is at the top of the waiting list, is given a reservation. Other requests can advance in the queue as long as they don't cause the pivot to be delayed. Using selective backfilling, reservations are provided to requests that have waited long enough in the queue.

The Selective-Differential-Adaptive approach, presented by Srinivasan et al., permits the XFactor threshold to represent the average slowness of previously completed requests. The accompanying policy sets are evaluated for scheduling requests that arrive at the organization's cluster:

a) Naive

The desires are scheduled using conservative backfilling by both the Site and Cloud schedulers. When each job arrives at the site, the redirection algorithm is run. If a request cannot be started immediately by the site scheduler, the redirection algorithm determines whether the request can be started right away using Cloud resources. The request is forwarded to the Cloud if it can be launched on Cloud services; else, it is queued on the web.

b) Shortest Queue

Jobs are scheduled on a first-come, first-served (FCFS) basis, with aggressive reseeding at the cluster. The redirection method determines the ratio of virtual machines required by queued requests to the number of processors available when each job comes or completes, similar to how work is done. If the Cloud's ratio is lower than the clusters, the redirection algorithm loops through the list of outstanding requests, redirecting them until both ratios are equal.

c) Weighted Queue

This method is a variant of the Shortest Queue method. Waiting requests on the cluster cause the scheduler to determine the virtual machines required, as well as how many virtual machines are in use on the Cloud when each job arrives or completes. The site scheduler then calculates num vms as the difference between the rate of VMs requested by the platform's responses and the Cloud's VM cap, and redirects requests to the Cloud unless num vms is fulfilled.

d) Selective

The selective backfilling scheme listed earlier is used at the local site. The scheduler test which requests can be started and then begins them when each job arrives or complete. If the ratios vary, the algorithm iterates through the list of pending requests, checking the XFactor for each one. If the expansion factor for a waiting request reaches the threshold, the algorithm tests the request's possible start time next to mutually the Cloud and the location.

In above discussion the standard way of recovery property and matrix process for measuring service to define a recovery property. It describes the result of the measurement only not explain how the measurement is performed. The matrix explains the knowledge about the property and observation can result in formulating or estimate the recovery property results. Recovery property can define a statement, idea and an event can resultin metric and fully understood and assessed in context. The context of recovery property defines the conditions and the rules for performing the measurement in cloud computing. Service interface for cloud computing using matrices can be divided into three major areas;

- Service Selection
- Service Verification
- Service Agreement

Metrics can perform an important role in cloud procurement process and can help for best suited to find out the requirement of the business model.

Metrics can also help to cloud vendors to communicate their cloud service properties for measurable and can facilitate their customers for providing service level agreement. In cloud computing, standards for measurements can be achieved for many purposes like different layers' hardware layers, software-defined layer, monitoring layers and service delivery layers. Matrices can also be helpful in procurement, audit and operation level of the cloud computing services life cycle.

e) Conservative

To plan requests, both the local site and the cloud utilize conservative require a substantial. The scheduler looks over each request to see if the site can make the deadline. If the deadline is not met, the scheduler looks for availability on the Cloud. If the Cloud will meet the request's timeline, the request is booked on Cloud services. If the request deadline is not met, the scheduler redirects it to a local site with a faster opening time than the Cloud. If this is not the case, the request is sent to the Cloud.

f) Aggressive

Both the content and skills and the cloud employ a lot of reseeding to plan requests. The scheduler constructs a tentative timetable for presently pending requests in the same way that it constructs a tentative schedule for currently waiting requests as each request comes. For generating the preliminary schedule, the scheduler sorts the requests using an Earliest Deadline First scheme and verifies if the approval of the arriving request would break any request deadlines. If there are no potential deadline breaches, the request is planned locally; otherwise, a tentative schedule for Cloud services is created. If the approach does not conflict with the constraints of other Cloud-based requests, it is served with Cloud-based services. If the request deadline is not fulfilled, the scheduler uses the local site's resources instead of the Cloud's if they have a faster start time. Aside from that, Cloud services are employed to complete the order.

g) System Design in Single and Multi Cloud

This section briefly describes the Inter Grid Gateway (IGG), which is comparable to the scheduler and is used to implement virtual machine leases issued to users. The names of the components were inspired by our past work on the interconnection of computational Grids. The conditions under which IGGs can borrow resources from one another are referred to as peering relationships. These peering relationships explain how an IGG analyses a request for resources from another IGG when it wishes to use those resources.

The center of the IGG is the Scheduler, which is responsible for satisfying user requests, managing reservations, and organizing the start and stop of virtual machines when jobs are planned. In order to meet the demands of scheduled requests, the scheduler keeps track of resource availability and communicates with the Virtual Machine Manager (VM Manager) to construct, start, and stop virtual machines. The IGG does not directly share physical resources, instead abstracting them through virtualization methods.

The IGG's repository contains all of the available models. Users who want to request VMs must currently decide which templates they want to use from the repository. IGGs must agree on templates in order for one IGGS to request VMs from another. We assume that each template offered at the organization's cluster in this study has a matching template at the Cloud provider.

The VM Manager deploys virtual machines on physical resources when the IGG requires it. The scheduler of the IGG provides the scheduling mechanisms that govern when and which virtual machines are started or shut down. The VM Manager uses a VIE for installing and maintaining VMs; the most recent implementation uses Open Nebula as a VIE for vitalizing a physical cluster infrastructure. Additionally, the VM Manager can manage virtual machines (VMs) deployed on cloud platforms such as Amazon EC2. Message transmission is handled by the Communication Module. This module gathers messages from other organizations and distributes them to the appropriate components that have been designated as listeners. Message-passing loosens the coupling between gateways and allows for more fail-safe communication protocols.

3.3 PROPOSED EVALUATING PERFORMANCE OF DISASTER RECOVERY USING FUZZY INFERENCE SYSTEM MODEL (EPCDR)

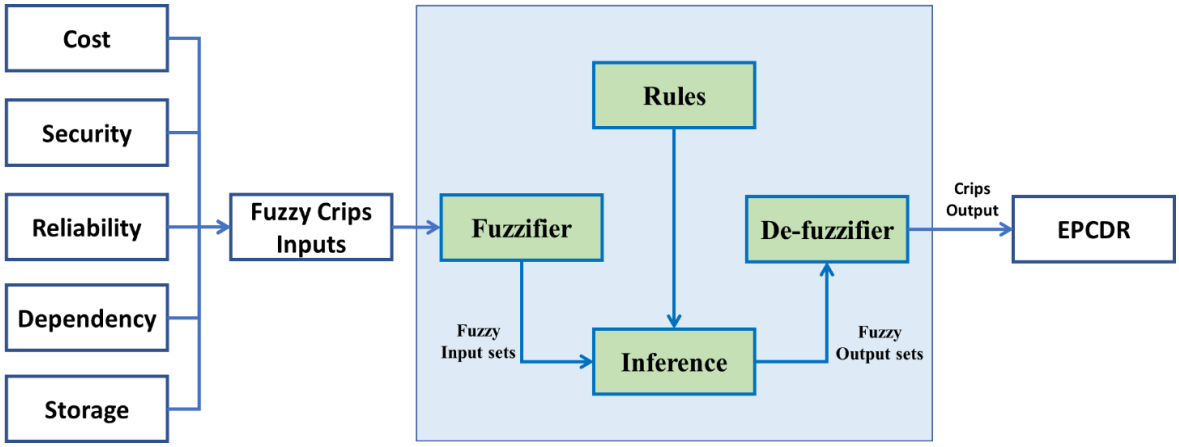


Figure 3: Proposed Model for Evaluating EPCDR 2

Figure 3: shows the proposed ***EPCDR*** *model* which depends on five parameters which are Cost, security, Reliability, Dependency, and Storage. The Parameters contains various input like Data Cost, Data Storage, Data Reliability, Data Dependency and Data Security which get the values from parameters and pass these values through rules and store in a device known as database. Input sets are the types of data that Fuzzifier receives. It could store data that is missing or noisy. As a result, it is referred to as raw data. The next batch of Fuzzy inputs is sent to the inference system, which is a critical layer in which we manage missing values using moving average and normalization to eliminate noisy data. Following this, the Inference System's Fuzzy output sets are transferred to the Defuzzifier layer. If the input parameters are relevant, they are fuzzifier and transformed into fuzzy crisp inputs in the Defuzzifier layer. Fuzzifier takes a crisp set of input data and converts it to a fuzzy set utilizing fuzzy linguistic variables, fuzzy semantic words, and membership functions. The fuzzy advances are then passed to a Fuzzy Inference engine in the next level. Fuzzy inference is the process of converting a given input to an output using fuzzy logic, and then converting the fuzzy set attributes to a crisp set in a defuzzifier. In most fuzzy control frameworks, it is required.

In the processing stage, a specific number is turned into a fuzzy linguist variable (fuzzification), each applicable rule (or data) is triggered, and a result is generated for each, and then the results are merged (inference). Finally, the combined result is turned back into a specified control output value in the output step (defuzzification).

3.4 SCENARIO IN SINGLE AND MULTI CLOUD

A discrete-event simulator is used to test the strategies. We utilize simulation because it allows us to run repeatable trials, which would be prohibitively expensive if we used real infrastructure. To record information on resources available for running virtual machines, the scheduler utilizes a data structure based on a red-black tree, whose nodes hold the list of resources accessible at the start or completion of leases. The tree is given a double-linked list that connects the sibling nodes. This list makes it easy to identify different time slots when dealing with advance reservations or searching for possible start times for requests. The availability profile idea is employed in some conservative backfilling systems, and this data structure is based on it.

We mimic the San Diego Super Computer Blue Horizon machine since work traces obtained from this supercomputer are publicly available1 and have been investigated previously. In the Blue Horizon machine, there are 144 nodes. The maximum number of virtual computers on the site is the same as the number of nodes. Furthermore, the maximum number of virtual machines that the Cloud

provider can operate at any given time is the same as the maximum number of virtual machines that may be hosted in the local cluster for this project. We wish to loosen this assumption in future work. To assess the cost of using Cloud services, we use the amounts paid by Amazon to host simple virtual machines on EC2.

The studies only look at the cost of running virtual machines, but Amazon also charges for other services such as network and storage. Other costs are not included in this analysis because they are reliant on the applications' contact and data standards. Although a virtual machine's operating system takes a few seconds to a few minutes to boot, Amazon starts billing users as soon as the VM process starts. As a result, the experiments assume that the request length already includes the booting time. Furthermore, the tests account for maximum hours of usage; for example, if a request consumes a VM for 30 minutes, the cost of one hour is considered.

a) Need Backup in Cloud

Consumers and users can access services on demand thanks to cloud computing. Resource management is required for each and every client/user. This type of management covers a wide range of aspects of resource utilization. As tools, any hardware or software can be employed. Software includes, for example, any application programming interface, application development kit, and any type of data file. Various implementations offer a number of methods for backing up data and maintaining its security among multiple users. Because cloud computing must be dependable, users must be able to upload crucial and essential data. When it comes to cloud installation, cost-effectiveness is the most crucial factor to consider.

We identified a number of advantages while researching cloud computing. In terms of advantages, we learned that the cloud is capable of securely storing enormous volumes of data from a variety of customers, allowing an Internet Service Provider (ISP) to provide a customer a big amount of cloud storage. Users can also upload sensitive and confidential information to the main cloud. At the same time, we discovered a critical flaw in this storage: if some of the client's data files go missing or vanish for any reason, or if the cloud is damaged due to a natural disaster (such as a flood, earthquake, or other natural disaster), the consumer/client must rely on the service provider for backup and recovery, which means the data must be stored on the server. If the main cloud fails to give the users' data, the client must be able to connect a backup server where private data is stored with great dependability. These approaches must be low-cost to use as a recovery solution, and they must be capable of promptly restoring data after a disaster. Cloud computing necessitates

backup and recovery strategies due to the vast volume of data kept by its customers. After the knowledge pattern is derived from the candidate module, it is passed through the relevance module for further processing.

Consumers and users can access resources on demand thanks to cloud computing. Resource management is required for each and every client/user. This sort of management covers a wide range of resource usage areas. As resources, any hardware or software can be employed. Software can be anything from an application programming interface to an application development kit to a data file. Numerous implementations offer a number of alternatives for backing up data and maintaining its security among various users. Because cloud computing must be dependable, users must be able to input sensitive and critical data. When it comes to cloud installation, cost-effectiveness is the most crucial factor to consider.

We identified a number of advantages while researching cloud computing. We observed that the cloud is capable of securely storing enormous volumes of data from a variety of clients, allowing an Internet Service Provider (ISP) to provide a user with a big amount of cloud storage. Users can also upload sensitive and confidential information to the main cloud. An effective data backup and recovery mechanism is necessary to handle the problem of such a scenario, so that the client may reach a backup server where private data is stored with high reliability whenever the main cloud fails to supply the user's data. As a solution to the recovery dilemma, these solutions must be low-cost to implement and capable of promptly restoring data after a disaster. Cloud computing necessitates backup and recovery solutions due of its clients' massive storage.

b) Scheduling and Redirection Strategies

The research methodologies focused into how the scheduler manages lease scheduling and when it borrows resources from the Cloud. The scheduler is separated into two sub-scheduler modules, one of which controls request scheduling on local cluster resources and is known as the Site Scheduler, and the other of which is known as the Cloud Scheduler and manages request scheduling on Cloud resources. A scheduling strategy is a method or algorithm for scheduling leases, and a redirection strategy is a method or algorithm for determining when the scheduler borrows Cloud resources and which requests are diverted to Cloud resources. A strategy set is a collection of strategies for scheduling and redirection. A redirection technique may be utilized at different times in distinct strategy sets (for example, upon work arrival or completion).

Once the enhanced property sub-module grouped the similar patterns of recovery, new properties and features also appear and these new characteristics are more strong and unique in the implementation. These new characteristics are optimized to make them ready for the new recovery category. The patterns that are collected in relevance module are of similar nature that is why the disaster is of recovery nature means when the combination of different disaster takes place to form cloud recovery network, they are combined on the basis of the similar properties. When two or more cloud properties are evaluated with their properties, then new features are also evolved. For example, all the storage cloud services must be offered in the platform of software as service. Building a storage related recovery, all the properties of storage are evolving and for a sub evaluating performance of disaster recovery of storage.

3.5 CONCLUSION

In this chapter we have proposed Intelligent Evaluating performance of disaster recovery in cloud model and elaborated different modules from connectivity and processing perspective. As per our research objectives, this model is designed to provide autonomous self-evolving mechanism as explained in learning module and memories. On the other hand, it is also capable of analyzing the recovery properties and categorizes it according to evaluation performance as discussed in relevance and disaster modules. Machine learning module has been explained to expose the potential and possibilities to address big data or IoT problems by having an intelligent cloud recovery performance. An important module is performance analyzer which perform evaluation of candidate clouds with dynamic parameters – as it is presumed that emerging technology is changing swiftly therefore, fixed / certain parameters may fulfill the requirements of this research but may not be able to cope up with future demands. The overall model provides the modular explanation of a cloud evaluation performance of disaster recovery which may act as a central platform for various cloud services along with autonomy and self-evolving features.

CHAPTER 4

DESIGN FOR EVALUATION PERFORMANCE OF DISASTER RECOVERY OF CLOUDS

4.1 DESIGN CHALLENGES

The autonomous cloud service discovery, validation, verification, and cloud service classification is a complex task due to heterogeneous structure of cloud system. Designing cloud services classification, different types of challenges in order to collect the desired datasets.

4.1.1 Multi Cloud Services

The word of intercloud and cloud-of-cloud which are similar to multi-cloud. These concepts imply that cloud computing does not have to be limited to a single cloud. In their example, a gloomy sky combines numerous hues and patterns of clouds, resulting in a variety of implementations and administrative worlds. Recent research has focused on the multi-cloud environment, which handles multiple clouds without relying on any one of them. In a multicloud environment, there are two layers: the inner-cloud at the bottom and the inter-cloud at the top. In the interclouds, the Byzantine fault resistance finds a home. We'll start by going over the preceding three decades' worth of Byzantine protocols. Byzantine faults are software or hardware problems in cloud computing that typically pertain to inappropriate behavior and intrusion resistance. There are also arbitrary and crash faults in it. Byzantine Fault Tolerance has been the subject of extensive research since its inception (BFT).

4.1.2 Standardization Issue of Multi Cloud

Furthermore, many people think of BFT as a cloud service that is only of academic interest. This lack of interest in BFT contrasts sharply with the degree of interest in crash fault tolerance mechanisms used in large-scale systems. As previously stated, BFT protocols are not suitable for single clouds. According to Vukolic, one of the disadvantages of BFT for the inner-cloud is that it, like all fault-tolerant protocols, requires a high degree of failure independence. If a cloud node encounters Byzantine failure, it is reasonable to utilize a different operating system, implementation, and hardware to prevent the failure from

spreading to other cloud nodes. Furthermore, if a specific cloud is targeted, the attacker may be able to gain control of the cloud's the inside equipment.

4.1.3 Scalability

Cloud services are gaining popularity due to its versatile nature and efficient delivery over the internet. A large amount of web and cloud services over the World Wide Web can heavily affect the searching of desired cloud service. Cloud crawler engine’s performance is subject to optimize the computing cost in the large-scale web.

4.1.4 Exploring New Multi Cloud Recovery Services

Different cloud service providers offer different cloud recovery services with a different name, but their functionality will be same and cloud recovery services are gaining popularity due to its versatile nature and efficient delivery over the internet. A large amount of web and cloud recovery services over the World Wide Web can heavily affect the searching of desired cloud recovery service. Cloud crawler engine’s performance is subject to optimize the computing cost in the large-scale web.

4.2 CONCLUSION

As in previous chapter, we have provided the detail functionality and connectivity of our proposed model EPCDR. This chapter covers the validation of our thought and arte fact. We have proposed a detail algorithm to explain the functionality and different criterion in our proposed recovery system for member evaluation performance. Visualization explains the flow and the interactivity of the algorithm which starts from the first phase of EPCDR model.

CHAPTER 5

SIMULATION FOR EVALUATION PERFORMANCE OF DISASTER RECOVERY IN CLOUDS (EPCDR)

5.1 CLOUD EVOLUTION MANAGEMENT

In intelligent evaluation performance of disaster recovery in cloud system, automation of cloud services according to service model can result in cloud evolution. Cloud services management performing clustering the cloud services within service model and helpful for categorization/classification of cloud services. The evaluation performance of disaster recovery in cloud system is interconnected with cloud resources, different cloud services, seller, reseller and applications for cloud users. The evaluation performance of disaster recovery in cloud system may include big data application hubs, big data cloud plug-ins, big data analytical tools and different big data resources.

Due to evaluating structure of cloud services, many parameters can be used for cloud management in the evaluation performance of disaster recovery in cloud system. Selecting different parameters based on user preferences can reflect the dynamism in the cloud. Evaluation performance of disaster recovery in cloud system is a broader term where many stack holders can take part in defining the homogeneous and heterogeneity properties within different categories of cloud services. Within evaluation performance of disaster recovery in cloud system, the following parameter can be used to define the progress of a certain part of the evaluation performance of disaster recovery in cloud system.

- Data Cost
- Data Reliability
- Data Dependency
- Data Storage
- Data Security

The above mention parameters can be used individually for measuring the cloud security, their performance and reliability management in clouds. Different features enable parameters like cost, interoperability and scalability also take part in measuring performance.

Storage is one of the most essential components in the cloud recovery system due to the greater scope of the evaluation performance of disaster recovery in cloud systems. The performance and ranking of the aforementioned component are evaluated in this thesis utilizing a fuzzy inference method. For validating the suggested system, there is a distinct scenario. Performance and interoperability are significant parameters in evaluating disaster recovery in cloud systems in this thesis. These parameters have more significant in evaluation performance of disaster recovery in cloud system and can emerging impact on current research era. For sustainability to remain in evaluation performance of disaster recovery in cloud system, the cloud service providers have high-performance cloud services and technology-oriented features.

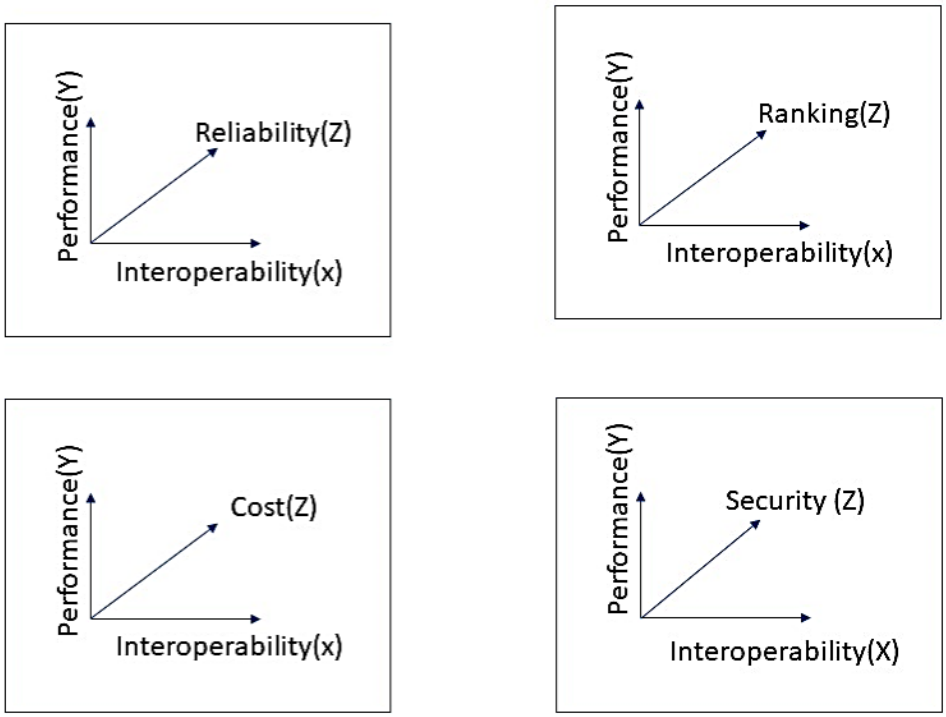


Figure 4: Proposed Model for Evaluating Different Visualization of Selected Parameter

Using the above mention parameters, different visualization of cloud management can be achieved. Interoperability (X) and Performance (Y) remain the static and Z is dynamic and can be implemented using fuzzy inference system. As mentioned before that generalization of proposed EPCDR model is only possible through dynamism that can evolve according to the emerging technologies, therefore, we have taken interoperability and performance as our core parameters while all other cloud properties can be used for processing. As in mentioned visualization we are showing reliability, cost, ranking and security. In section below, we have taken only ranking and variant of performance to explain the simulation because all other parameters mentioned before are the

constituents of ranking that is why we have taken only ranking and variants of performance for simulation purposes. On these lines we have developed various cases which are explained in following section.

In the first case, the performance of storage cloud cluster has been evaluated through fuzzy inference system. In the Second case, the ranking of cloud services has been evaluated using fuzzification. In the third case, the performance of cloud services of selected parameters has been evaluated using the different parameter. In the fourth case; the overall performance has been evaluated using the output of case 2 and case 3 as shown in fig.2.

5.1 IMPLEMENTATION: PERFORMANCE MEASUREMENT OF DISASTER RECOVERY

For performance measurement of storage service area having a parameter of Security, Cost, Dependency, Reliability, and Storage, Fuzzy inference system (FIS) were used. In simulation phase, first determine the performance of cloud security, and then we calculated the ranking of the given services.

a) Input Fuzzy Sets

This system's membership function provides curve output values ranging from 0 to 100, as well as a mathematical function that generates numerical parameters for input and output variables. The first layer (Data Dependency, Data Cost, Data Security, Data Storage, and Data Reliability) considered as level 1, rest of layer is correspondence.

Table 1
Input Variable Range

Sr #	Input Parameters	Ranges	Semantic Sign
1	**Data Cost**	[0 0 25 30] [25 30 70 75] [70 75 100 100]	Low Average High
2	**Data Dependency**	[0 0 20 30] [20 30 70 80] [70 80 100 100]	Weak Normal Strong
3	**Data Reliability**	[0 0 20 30] [20 30 70 80] [70 80 100 100]	Low Average High
4	**Data Security**	[0 0 15 25] [15 25 75 85] [75 85 100 100	Public Semi Public Private
5	**Data Storage**	[0 0 20 30] [20 30 80 90] [80 90 100 100	Incapable Moderate Capable

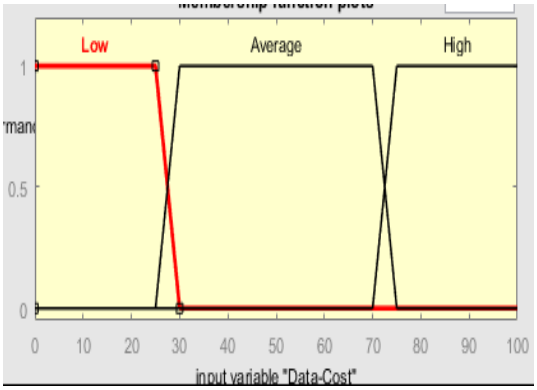
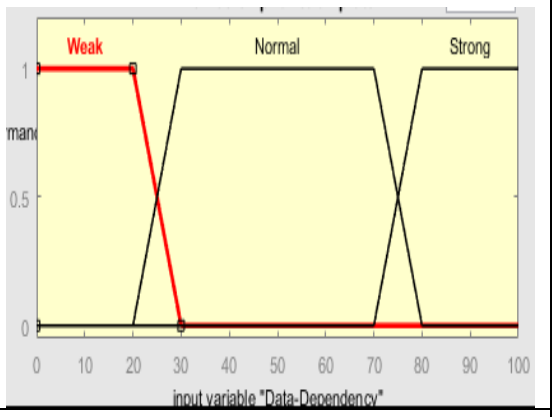
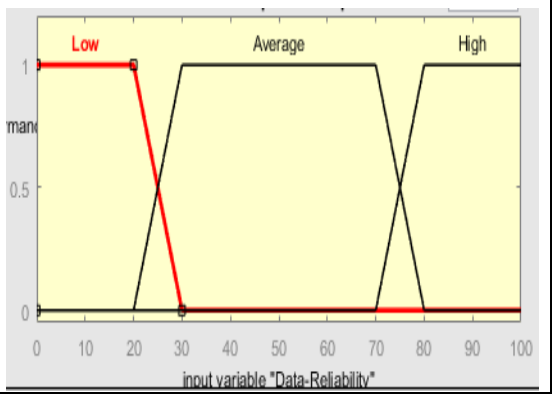
b) Rule based

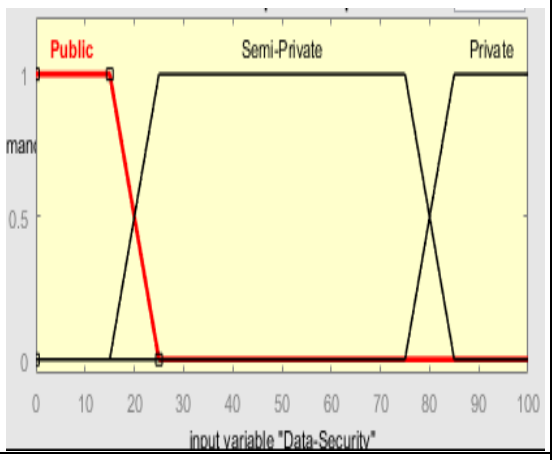
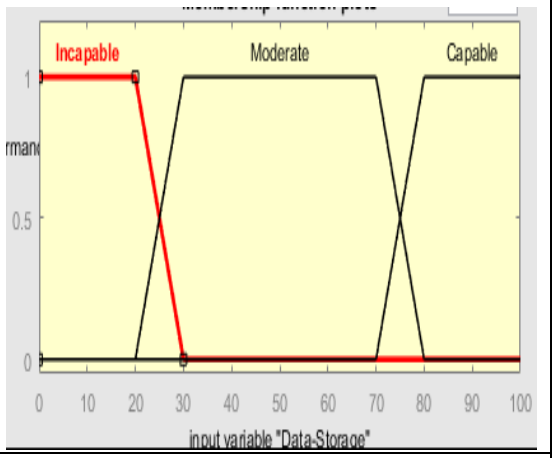
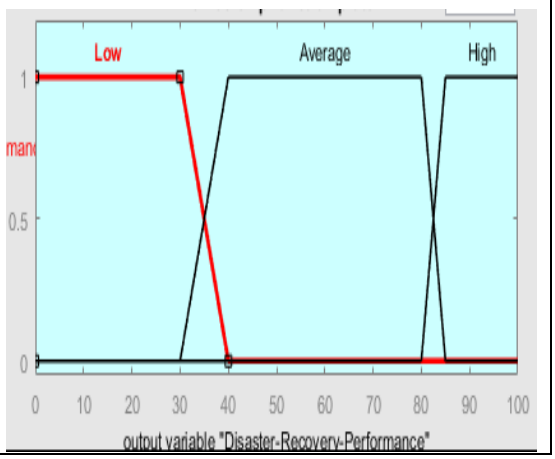
In FIS, I/O Rules play a crucial role. These rules are used to create the fuzzy inference system (FIS). I/O rules are generated in this chapter using a lookup table, which may be found in Table II. Below is a proposed I/O rule that is dependent on FIS.

c) Membership Function

Membership function represents the curve values that are range between 0 and 100. It is a mathematical notation of input and output variables. FIS Input/output Variables with Graphical & Mathematical representation of the Proposed **EPCDR** system in table 1 for layer 1. FIS Input/output Variables of layer 2 with Graphical & Mathematical representation of the Proposed **EPCDR** system in table 1. In table 1 first five rows represent the input member function while for row 6 represent the output member function.

Table 2
Input/output Variables Membership Functions Proposed EPCDR

Input/ output	Membership Function	Graphical Representation of MF
D $= \mu_{D,c}(c)$	$\mu_{D,c}(C) = \{max(\left(1, \frac{30-dc}{5}\right), 0)\}$ $\mu_{d,c}(C)$ $= \{max(\left(\frac{dc-25}{5}, 1, \frac{75-dc}{5}\right), 0)\}$ $\mu_{d,c}(C) = \{max(\left(\frac{dc-70}{5}, 1\right), 0)\}$	
D $= \mu_{D,D}(D)$	$\mu_{D,D}(D) = \{max(\left(1, \frac{30-dd}{10}\right), 0)\}$ $\mu_{d,c}(C)$ $= \{max(\left(\frac{dd-20}{10}, 1, \frac{80-dd}{10}\right), 0)\}$ $\mu_{D,D}(D) = \{max(\left(\frac{dd-70}{10}, 1\right), 0)\}$	
R $= \mu_{D,R}(r)$	$\mu_{D,R}(r) = \{max(\left(1, \frac{30-r}{10}\right), 0)\}$ $\mu_{D,R}(r)$ $= \{max(\left(\frac{dr-20}{10}, 1, \frac{80-dr}{10}\right), 0)\}$ $\mu_{R,Out}(r)$ $= \{max(\left(\frac{dr-70}{10}, 1\right), 0)\}$	

Input/ output	Membership Function	Graphical Representation of MF
S $= \mu_{D,S}(S)$	$\mu_{D,S}(S) = \{max(\left(1, \frac{25-s}{10}\right), 0)\}$ $\mu_{d,c}(C)$ $= \{max(\left(\frac{ds-15}{10}, 1, \frac{85-ds}{10}\right), 0)\}$ $\mu_{D,S}(s) = \{max(\left(\frac{S-75}{10}, 1\right), 0)\}$	
DS $= D, S$ (d, s)	$\mu_{D,S}(ds) = \{max(\left(1, \frac{30-ds}{10}\right), 0)\}$ $\mu_{d,s}(C)$ $= \{max(\left(\frac{ds-20}{10}, 1, \frac{80-dc}{10}\right), 0)\}$ $\mu_{D,S}(DS) = \{max(\left(\frac{ds-70}{10}, 1\right), 0)\}$	
DRP $= \mu_{drp}$ (DRP)	$\mu_{D,R,P}(drp)$ $= \{max(\left(1, \frac{40-drp}{10}\right), 0)\}$ $\mu_{D,R,P}(drp)$ $= \left\{\left(\left(\frac{drp-30}{10}, 1, \frac{80-dc}{10}\right), 0\right)\right\}$ $\mu_{D,R,P}(drp)$ $= \{max(\left(\frac{drp-80}{10}, 1\right), 0)\}$	

d) Output Variables

Table 3
Output Variable Ranges

Sr #	Output of EPCDR	Ranges	Semantic sign
1	Performance	[0 0 30 40] [30 40 80 85] [80 85 100 100]	Low Average High

e) Inference Engine

One of the most important components of a FIS is the inference engine.

If (Data-Cost is Low) and (Data-Security is Public) and (Data-Reliability is Low) and (Data-Storage is Incapable) and (Data-Dependency is Weak) then (Disaster-Recovery-Performance is Low).

If (Data-Cost is Low) and (Data-Security is Public) and (Data-Reliability is Low) and (Data-Storage is Incapable) and (Data-Dependency is Normal) then (Disaster-Recovery-Performance is Low).

If (Data-Cost is Low) and (Data-Security is Public) and (Data-Reliability is Low) and (Data-Storage is Incapable) and (Data-Dependency is Strong) then (Disaster-Recovery-Performance is Low)

.
.
.

243. If (Data-Cost is high) and (Data-Security is Semi-Private) and (Data-Reliability is Low) and (Data-Storage is Incapable) and (Data-Dependency is Normal) then (Disaster-Recovery-Performance is high).

5.3 DE-FUZZIFIER

One of the significant procedures of a fuzzy inference system is the de-fuzzifier. De-Fuzzifiers come in a variety of shapes and sizes. The centroid type of De-Fuzzifier is utilised in this article. The De-Fuzzifier graphical representation of the fuzzy inference system is shown in Figure 5.

f) FIS Defuzzification for Case-1

Figure 5: Represent the 3D view of Surface of Proposed Rule EPCDR based on Data Security and Data Cost. It observed that EPCDR Good (Yellow shade), and EPCDR, Weak or Poor (Bluish Shade) and Satisfactory results (Greenish shade).

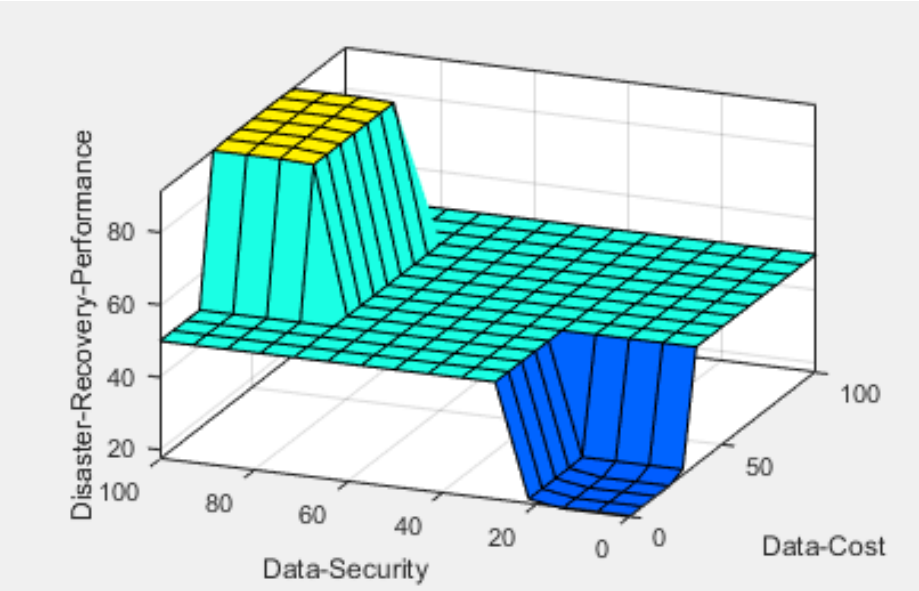


Figure 5: Surface of Proposed Rule EPCDR based on Data Security along with Data Cost

g) FIS Defuzzification for Case-2

Figure 6: Represent the 3D view of Surface of Proposed Rule EPCDR based on Data Security and Data Cost. It observed that EPCDR Good (Yellow shade), and EPCDR, Weak or Poor (Bluish Shade) otherwise Satisfactory results (Greenish shade).

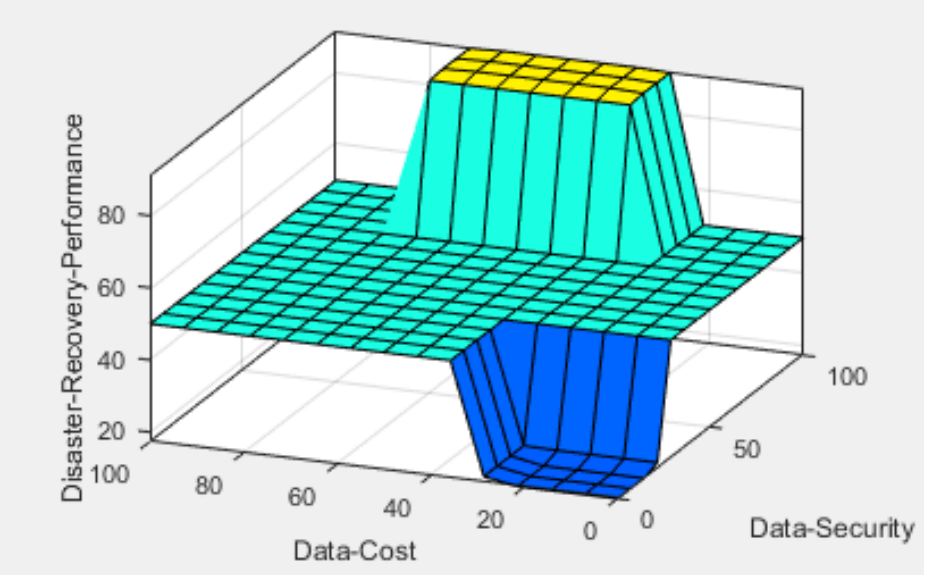


Figure 6: Surface of Proposed Rule EPCDR based on Data Security along with Data Cost

h) FIS Defuzzification for Case-3

Figure 7: Represent the 3D view of Surface of Proposed Rule EPCDR based on Data Security and Data Cost. It observed that EPCDR Good (Yellow shade), and EPCDR, Weak or Poor (Bluish Shade) otherwise Satisfactory results (Greenish shade).

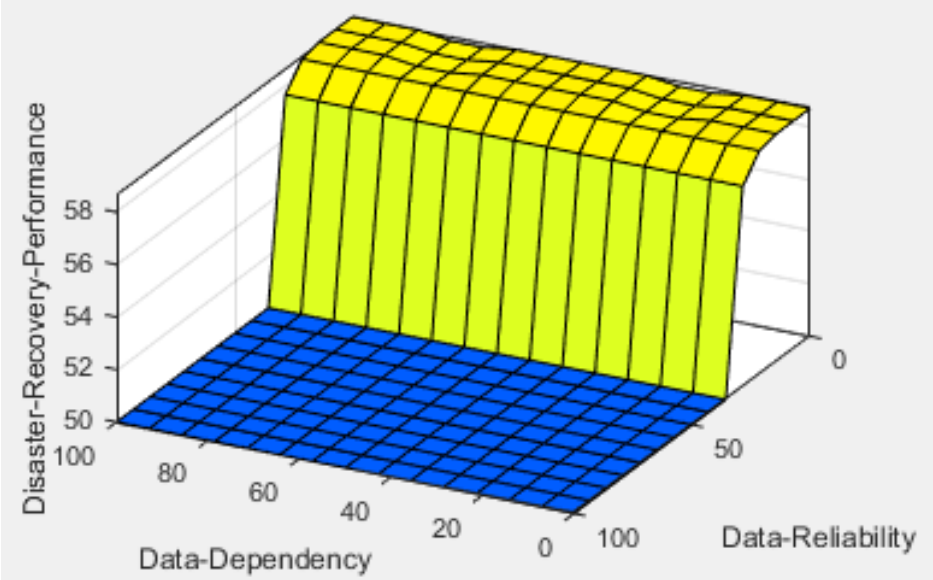


Figure 7: Surface of Proposed Rule EPCDR based on Data Dependency along with Data Reliability

i) FIS Defuzzification for Case-4

Figure 8: Represent the 3D view of Surface of Proposed Rule EFCDR based on Data Security and Data Cost. It observed that EPCDR Good (Yellow shade), and EPCDR, Weak or Poor (Bluish Shade) otherwise Satisfactory results (Greenish shade).

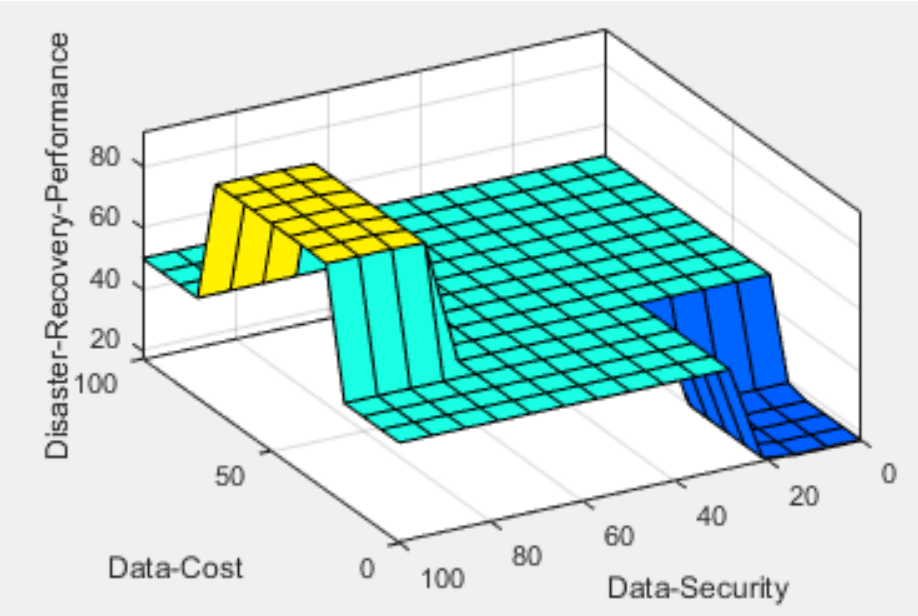


Figure 8: Surface of Proposed Rule EPCDR based on Data Cost along with Data Security.

j) FIS Defuzzification for Case-5

Figure 9: Represent the 3D view of Surface of Proposed Rule EFCDR based on Data Security and Data Cost. It observed that EPCDR Good (Yellow shade), and EPCDR, Weak or Poor (Bluish Shade) otherwise Satisfactory results (Greenish shade).

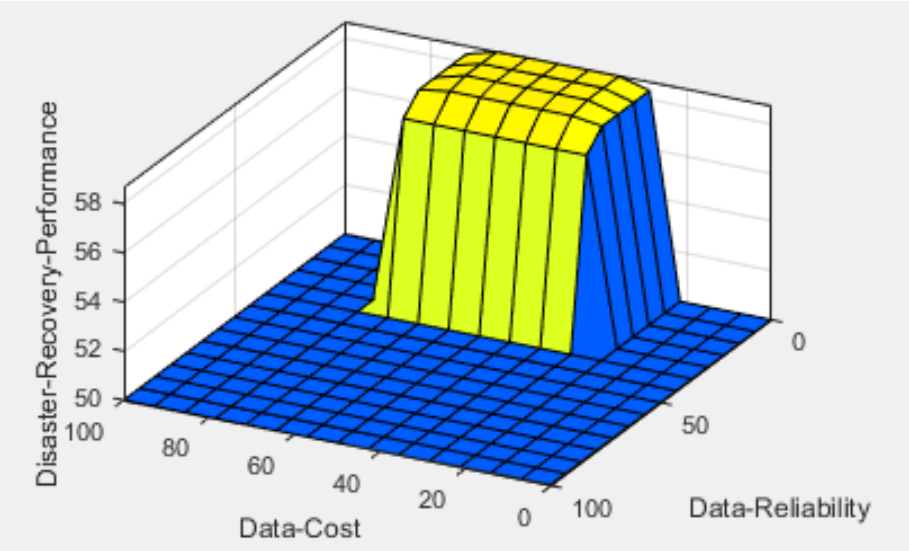


Figure 9: Surface of Proposed Rule EPCDR based on Data Cost along with Data Reliability

5.4 SIMULATION AND RESULTS

MATLAB 2019 is used to generate simulation results. MATLAB is also used in modeling, simulation, algorithm development, prototyping, and a variety of other industries. Three data inputs and one output parameter are used to reproduce the results. The proposed Fuzzy based EFCDR in this article not only identifies output, but also illustrates many sorts of output, such as EFCDR. Based on the rules presented in the lookup, a lookup rules diagram is built using Fuzzy Logic design.

a) Lookup Diagram for case 1

Figure 10: demonstrates that if the cost of data is low, Data Security is low, Data Reliability is low, Data Storage is incapable, Data Dependency is weak, and then Disaster Recovery Performance is Low.

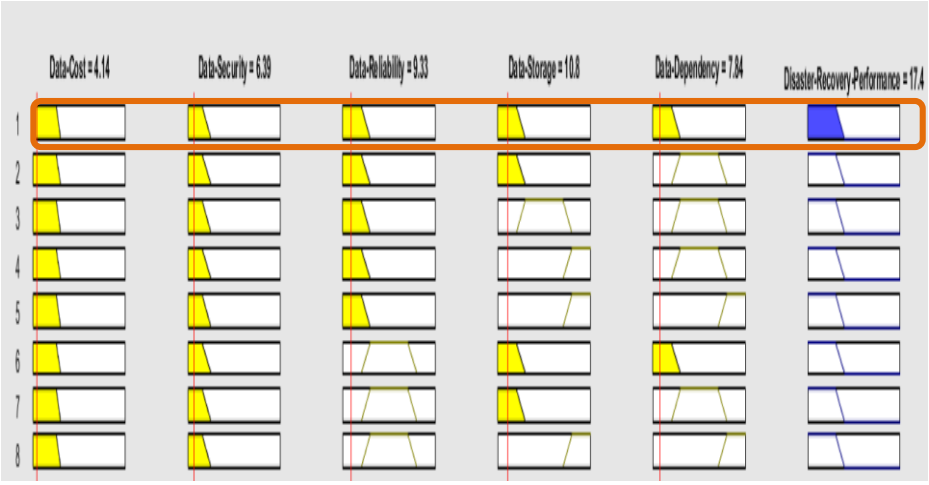


Figure 10: Layer 2 Lookup diagram for proposed EPCDR (Low)

b) Lookup Diagram for case 2

Figure 11: shows that if the Data Cost is Average, Data Security is semi-public, Data Reliability is Average, Data Storage is Moderate, Data Dependency is Normal, and then Disaster Recovery Performance is Average.

Figure 11: Layer 2 Lookup diagram for proposed EPCDR (Average)

c) Lookup Diagram for case 3

Figure 12: Shows that if the Data Cost is High, Data Security is Private, Data Reliability is High, Data Storage is capable, Data Dependency is Strong, and then Disaster Recovery Performance is high

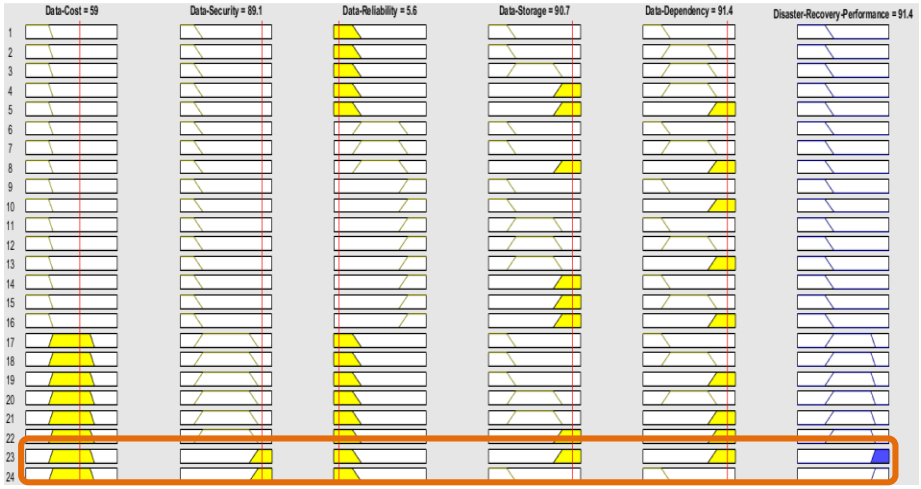


Figure 12: Layer 2 Lookup diagram for proposed EFCDR (High)

5.3 CONCLUSION

This chapter provides the details on validation process of ICE which splits into two parts i.e. algorithm and simulation. The algorithm part has been discussed in previous section, while simulation is spread over four different cases to analyze the proposed model ICE.As ecosystem is an environment, therefore, the main target is to provide such environment to the ecosystem members in whom they can perform to the optimum level. Validation cases are focused on performance phenomenon and ranking (which again is a representation of performance). Fuzzy inference has been used to test the scenarios; results are significant and shows positive inclination in favor of problem statement and hypotheses.

CHAPTER 6

CONCLUSION

Cloud computing and infrastructure is a rapidly growing technology at individual and corporate level. This fast pace desired the establishment of such measures which can regularize the expansion i.e. instead of a mushroom growth like world wide web, it is important to provide a central platform to cloud services for better management and governance. The cloud platform, storage, and network are all part of the environment. Infrastructural and security issues that develop as a result of Single-Cloud provider manage both apps and data. Sensitive information, such as medical records, is uploaded for safekeeping. Users, on the other hand, on the cloud, they have no control over their data. It's impossible to know if the data is being misappropriated. In a Single-Cloud setting, data owners are unable to access their data. Ensure that the data is secure.

The cloud is completely under your control provided by the service provider developing a relationship of trust with a cloud service the choice of a provider is crucial in deciding whether or not to relocate cloud. There are a number of other variables that could put distrust taking place the protection of the system. Employees who may or may not be trustworthy are among the sources of data in the cloud. Employees that are interested and may compete with or upset the company owner of the data Employees of cloud service companies and several cloud tune providers cloud service companies have tampered with confidential information.

The data is kept during cloud. A single cloud setup may perhaps furthermore experience significant management costs for big amounts of data, as well as data loss issues. Data security is ensured by distributing data and applications over multiple clouds. This multi cloud design ensures soaring records accessibility while also corresponding tons, managing resources, and securely storing data. The records holder possibly will have faith in the cloud owner ability to protect their numbers. This framework also facilitates the integration of private and public clouds, resulting in increased transparency, flexibility, and resource management efficiency. Homomorphism-based encryption and decryption are necessary in this idea. The management layer is

an essential component of a Multi-Cloud system's design, allowing for data and application sharing, integration, load balancing, and other functions. Each cloud was only a few inches in diameter. It is in charge of the process' execution. If sensitive data is to be stored on the cloud, security is essential. be safeguarded prevent appropriation or other types of disruption Data owners who upload sensitive data to the cloud must employ cloud properties like scalability and device mobility with caution. Two advantages are independence and remote access. The data of cloud users is protected by the cloud service provider, who may or may not be a trustworthy third party with a direct involvement.

In a single cloud setup, data stealing can occur when any aspect of the cloud is compromised, therefore security must always be questioned. Data theft does not occur when encrypted data is distributed across numerous clouds since a single-cloud architecture is insufficient for a bad influence to access all data. As a result, a Multicloud design provides the essential data protection in the cloud. High Availability: In a Service Level Agreement (SLA), uptime is an important statistic for service quality. When one section of the network becomes delayed in a Multicloud architecture Even when a DRP is in place and staffs have been trained to use it, disaster recovery poses various problems. It's possible that DR won't go as planned. After a calamity, they may out to be insufficient. The A natural disaster's enormity cannot be predicted at any same time, an organization may face multiple disasters. It's nearly impossible to plan for this situation. As a consequence, there will be some data loss. DR necessitates collaboration amongst multiple departments; simple sharing it may be difficult to share accurate information among organizations. It is difficult to maintain communication before, during, and after a disaster. Communication is difficult during and immediately after a conflict. In some circumstances, knowledge becomes obsolete fast, while in others, communication channels may collapse. For these reasons, DRPs frequently include test procedures in which various levels of disasters are simulated; the study of the outcomes can aid in the plan's refinement. More serious recovery concerns develop when backups are damaged or the backup process fails. Several firms that encounter large-scale data damage and/or disruption discover that recovery does not deliver the desired answers because the media are unusable or the data cannot be restored. Setting up a procedure that retrieves data from the backup medium, restores it, and reviews it on a regular basis is the simplest method to deal with this danger. This approach should investigate the causes of any test failures in

order to identify and correct backup problems. The eight stages of the DR process for resolving defects are recognise, react, recover, restore, return to normal, rest and relax, reevaluation, and re-documentation. The goal and boundaries of a healing process should be investigated initially. This step should encompass employee safety and critical business functions (CBFs). When a disaster is declared, all required personnel should be alerted, and a disaster recovery plan should be implemented. Management and the staff in charge of disaster recovery should lead the response to the incident. They determine the course of action to be taken, and then key systems should be restored.

At this stage, if necessary, migration to another institution may be initiated. The systems that had been identified beforehand are then restored. After the exercise is completed, the entire process should be evaluated to establish an organization's strengths and shortcomings in the event of a disaster.

CHAPTER 7

LIMITATION

One of the limitations of this research was the disaster structure of cloud computing. Evaluation performance of disaster recovery in cloud has a broader scope due to the large-scale vendor, providers, seller, reseller, brokers and users. During the validating phase; testing for whole Evaluation performance of disaster recovery in cloud is simply not possible. Due to the different naming convention of cloud services, non-availability of cloud service level agreements details, non-standardization mechanism makes the crawling process difficult. The proposed framework for the intelligent cloud service management that is being provided by storage cloud services from cloud service providers worked for one cluster of the Evaluation performance of disaster recovery in cloud.

The structure of single-cloud environment, which are integrated sets of cloud services. The cloud platform, storage, and network are all part of the environment. Infrastructural and security issues that develop as a result of Single-Cloud provider manage both apps and data. Sensitive information, Medical records, for example, is uploaded for safekeeping. On the other side, users have no control over their data while it is stored on the cloud. It's impossible to tell if the information is being misused. d. Data owners in a Single-Cloud environment are unable to access their data. Ensure that the data is secure. The cloud is completely under your control provided by the service provider developing a relationship of trust with a cloud service the choice of a provider is crucial in deciding whether or not to relocate cloud. There are a number of other variables that could put doubt on the security of the system. Employees who may or may not be trustworthy are among the sources of data in the cloud. Employees that are interested and may compete with or upset the company owner of the data Employees of cloud service companies and Some cloud service providers have tampered with personally identifiable information. The information is stored in the cloud. For large amounts of data, a Single-Cloud system may incur significant administration costs, as well as data loss risks.

Data and application security is assured by dispersing them across several clouds. This multi-cloud architecture offers high data availability while balancing loads, managing resources, and storing data securely. Because no Single-Cloud architecture has enough knowledge to decrypt data without access to other parts of the data in other clouds, a service provider's trustworthiness in this system may be less important. The data owner may have faith in the cloud provider's ability to keep their information safe. This paradigm also facilitates

the integration of private and public clouds, resulting in increased transparency, flexibility, and resource management efficiency. In this concept, homomorphism-based encryption and decryption are required. The management layer is an essential component of a Multi-Cloud system's design, allowing for data and application sharing, integration, stack corresponding, along with added functions.

Workload Manager, an earlier implementation of a Multi-Cloud architecture, did not spread process load across several clouds. Each cloud had a diameter of only a few inches. It is in charge of carrying out the procedure. Security is critical when storing sensitive data in the cloud. be protected from misuse or other types of tampering Data owners who upload sensitive data to the cloud must employ cloud properties like scalability and device mobility with caution. Two advantages are independence and remote access. The data of cloud users is protected by the cloud service provider, who may or may not be a trustworthy third party with a vested interest. Data security must always be questioned in a Single Cloud configuration, as data theft can occur when any aspect of the cloud is attacked. Data theft does not occur when encrypted data is distributed across numerous clouds since a single-cloud architecture is insufficient for a bad influence to access all data.

As a result, a Multicloud design provides the essential data protection in the cloud. High Availability: In a Service Level Agreement (SLA), uptime is an important statistic for service quality. When one section of the network becomes delayed in a Multicloud architecture, the multi cloud Management Layer shifts the process to another cloud, ensuring that the service level agreement is met. Even when a DRP is in place and staffs have been trained to use it, disaster recovery poses various problems. It's possible that DR won't go as planned. After a calamity, they may out to be insufficient. The A natural disaster's enormity cannot be predicted at any same time; an organization may face multiple disasters. It's nearly impossible to plan for this situation. As a consequence, there will be some data loss. DR necessitates collaboration amongst multiple departments; simple sharing it may be difficult to share accurate information among organizations.

It is difficult to maintain communication before, during, and after a disaster. It is difficult to communicate during and immediately after a crisis. In some circumstances, knowledge becomes obsolete fast, while in others, communication channels may collapse. For a DRP to be successful, it requires knowledge and authority, which can be difficult to maintain. For these reasons, DRPs frequently include test procedures in which various levels of disasters are simulated; the study of the outcomes can aid in the plan's refinement. More serious recovery concerns develop when backups are damaged or the backup

process fails. Several firms who encounter large-scale data damage and/or disruption discover that recovery does not deliver the desired answers because the medium is unusable or the data cannot be restored. Setting up a procedure that retrieves data from the backup medium, restores it, and reviews it on a regular basis is the simplest method to deal with this danger. This approach should investigate the causes of any test failures in order to identify and correct backup problems. The eight stages of the DR process for resolving defects are recognise, react, recover, restore, return to normal, rest and relax, reevaluation, and re-documentation.

The aim of a healing process, as well as its boundaries, should be investigated first. Staff safety and Critical Business Functions should be included in this step (CBFs). When a disaster is declared, all necessary staff should be notified, and the disaster recovery plan should be put in place. Management and the staff in charge of disaster recovery should lead the response to the incident. They determine the course of action to be taken, and then key systems should be restored. At this stage, if necessary, migration to another institution may be initiated. The systems that had been identified beforehand are then restored. A controlled return to normal operations should occur when the support systems and utilities have been restored. After the exercise is completed, the entire process should be evaluated to establish an organization's strengths and shortcomings in the event of a disaster.

CHAPTER 8

FUTURE WORK

As future work, development of cloud-based components and API could be used for the autonomous service discovery, cloud ranking for user preference. Using the proposed framework, cloud crawler can automatically crawl the cloud service information from different providers and can categorize according to their functionality. After categorization of cloud services into their subcategory, crawling performance, as well as ranking, can be improved.

REFERENCES

1. Abreu, T., Moreira, J. R., Minussi, C.R., Lotufo, A.D.P. and Lopes, M.L.M. (2019). Short-Term Multinodal Load Forecasting Using a Fuzzy-ARTMAP Neural Network. *2019 IEEE PES Conference on Innovative Smart Grid Technologies, ISGT Latin America*, 1–6.

2. Abualkishik, A.Z., Alwan, A.A. and Gulzar, Y. (2020). Disaster recovery in cloud computing systems: An overview. *International Journal of Advanced Computer Science and Applications*, 11(9), 702–710. https://doi.org/10.14569/IJACSA.2020.0110984

3. Alshammari, M.M., Alwan, A.A., Nordin, A. and Al-Shaikhli, I.F. (2018). Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges. *4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS*, 1–7. https://doi.org/10.1109/ICETAS.2017.8277868

4. AlZain, M.A., Pardede, E., Soh, B. and Thom, J.A. (2012). Cloud computing security: From single to multi-clouds. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 5490–5499. https://doi.org/10.1109/HICSS.2012.153

5. Badhel, S.P. and Chole, V. (2015). An efficient and secure remote data back-up technique for cloud computing. *International Journal of Computer Science and Mobile Computing*, 4(6), 361-369.

6. Bangui, H., Buhnova, B., Rakrak, S. and Raghay, S. (2017). Smart mobile technologies for the city of the future. *In 2017 Smart City Symposium Prague (SCSP)* (pp. 1-6). IEEE.

7. Bedi, R.K., Singh, J. and Gupta, S.K. (2019). MWC: an efficient and secure multi-cloud storage approach to leverage augmentation of multi-cloud storage services on mobile devices using fog computing. *Journal of Supercomputing*, 75(6), 3264–3287.

8. Bonvin, N., Papaioannou, T.G. and Aberer, K. (2009). Dynamic cost-efficient replication in data clouds. *In Proceedings of the 1st Workshop on Automated Control for Datacenters and Clouds* (pp. 49-56).

9. Botta, A., De Donato, W., Persico, V. and Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, 56, 684-700.

10. Brazdil, P.B. and Soares, C. (2000). A comparison of ranking methods for classification algorithm selection. *In European conference on machine learning* (pp. 63-75). Springer, Berlin, Heidelberg.

11. Calcaterra, D., Cartelli, V., Di Modica, G. and Tomarchio, O. (2019). A Comparison of Multi-cloud Provisioning Platforms. *In CLOSER* (pp. 507-514).

12. Castejón, H.N., Gavras, A., Gonçalves, J.M., Moiso, C., Undheim, A. and Zoric, J. (2011). Towards a dynamic cloud-enabled service eco-system. *In 2011 15th International Conference on Intelligence in Next Generation Networks* (pp. 259-264). IEEE.

13. Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y. and Youn, C.H. (2017). Wearable 2.0: Enabling Human-Cloud Integration in Next Generation Healthcare Systems. *IEEE Communications Magazine*, 55(1), 54–61.

14. Chen, Z.N., Chen, K., Jiang, J.L., Zhang, L.F., Wu, S., Qi, Z.W., Hu, C.M., Wu, Y.W., Sun, Y.Z., Tang, H., Sun, A.B. and Kang, Z.L. (2017). Evolution of Cloud Operating System: From Technology to Ecosystem. *Journal of Computer Science and Technology*, 32(2), 224–241.

15. Cui, W., Kim, Y. and Rosing, T.S. (2017). Cross-platform machine learning characterization for task allocation in IoT ecosystems. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference*, CCWC 2017, Ml, 0–6.

16. Cunningham, P. (2015). $) Udphzrun Iru D & Rvw (Iilflhqw & Orxg (Frv \ Vwhp.

17. Disaster recovery in single and multi cloud using fuzzy orignial. (n.d.).

18. Dubey, A. and Pal, S. (2017). Dynamic service composition towards database virtualization for efficient data management. *In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 519-526). IEEE.

19. Choo, K.K.R., Rana, O.F. and Rajarajan, M. (2017). Cloud Security Engineering: theory, practice and future research. *IEEE Transactions on Cloud Computing*, 5(3), 372-374.

20. Fernandez, E.B., Yoshioka, N., Washizaki, H. and Syed, M.H. (2016). Modeling and security in cloud ecosystems. *Future Internet*, 8(2), 13. https://doi.org/10.3390/fi8020013

21. Gamez, D. (2008). Progress in machine consciousness. *Consciousness and cognition*, 17(3), 887-910.

22. Gaur, A., Scotney, B., Parr, G. and McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia Computer Science*, 52(1), 1089–1094.

23. Gu, Y., Wang, D. and Liu, C. (2014). DR-Cloud: Multi-Cloud based disaster recovery service. *Tsinghua Science and Technology*, 19(1), 13-23. https://doi.org/10.1109/tst.2014.6733204

24. Hou, Z., Gu, J., Wang, Y. and Zhao, T. (2016). An autonomic monitoring framework of web service-enabled application software for the hybrid distributed HPC infrastructure. *Proceedings of 2015 4th International Conference on Computer Science and Network Technology*, ICCSNT 2015, Iccsnt, 85–90.

25. Jain, H. and Jain, R. (2017). Big data in weather forecasting: Applications and challenges. *Proceedings of the 2017 International Conference On Big Data Analytics and Computational Intelligence, ICBDACI* 2017, 138–142.

26. Jiao, L., Lit, J., Du, W. and Fu, X. (2014). Multi-objective data placement for multi-cloud socially aware services. *Proceedings - IEEE INFOCOM*, 28–36. https://doi.org/10.1109/INFOCOM.2014.6847921

27. Jin, Y. and Min, S. (2016). Stadam: A new SLA trust model based on anomaly detection and multi-cloud. *2016 1st IEEE International Conference on Computer Communication and the Internet, ICCCI* 2016, 396–399. https://doi.org/10.1109/CCI.2016.7778951

28. Kanwar, N., Goswami, A.K. and Mishra, S.P. (2019). Design Issues in Artificial Neural Network (ANN). *Proceedings - 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, IoT-SIU 2019*, 1–4. https://doi.org/10.1109/IoT-SIU.2019.8777337

29. Laituri, M. and Kodrich, K. (2008). On line disaster response community: People as sensors of high magnitude disasters using internet GIS. *Sensors*, 8(5), 3037–3055.

30. Li, X., Liu, Y., Kang, R. and Xiao, L. (2017). Service reliability modeling and evaluation of active-active cloud data center based on the IT infrastructure. *Microelectronics Reliability*, 75, 271–282.

31. Lindman, J., Kinnari, T. and Rossi, M. (2016). Business Roles in the Emerging Open-Data Ecosystem. *IEEE Software*, 33(5), 54–59. https://doi.org/10.1109/MS.2015.25

32. Manzoor, S., Taha, A. and Suri, N. (2016). Trust validation of cloud IaaS: a customer-centric approach. *In 2016 IEEE Trustcom / BigDataSE / ISPA* (pp. 97-104). IEEE.

33. Markova, O.M., Semerikov, S.O., Striuk, A.M., Shalatska, H.M., Nechypurenko, P.P. and Tron, V.V. (2019). Implementation of cloud service models in training of future information technology specialists. *CEUR Workshop Proceedings*, 2433, 499-515.

34. Mendonca, J., Lima, R., Matos, R., Ferreira, J. and Andrade, E. (2018). Availability analysis of a disaster recovery solution through stochastic models and fault injection experiments. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2018-May, 135–142. https://doi.org/10.1109/AINA.2018.00032

35. NIST. (2011). NIST Cloud Computing Reference Architecture: Recommendations of NIST. National Institute of Standard and Technology, Special Pu, 1–35.

36. Ölveczky, P.C. and Thorvaldsen, S. (2006). Formal modeling and analysis of wireless sensor network algorithms in real-time maude. *20th International Parallel and Distributed Processing Symposium, IPDPS*, 2006. https://doi.org/10.1109/IPDPS.2006.1639414

37. Ramharuk, V. and Osunmakinde, I. (2014). Cloud robotics: A framework towards cloud-enabled multi-robotics survivability. *ACM International Conference Proceeding Series*, 28-Septemb, 82–92. https://doi.org/10.1145/2664591.2664602

38. Shaikh, R.A.R. and Sasikumar, M. (2014). Dynamic parameter for selecting a cloud service. *International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC*, 32-35.

39. Shklovski, I., Palen, L. and Sutton, J. (2008). Finding community through information and communication technology in disaster response. *Computer Supported Cooperative Work*, 9.

40. Stamelos, I., Angelis, L., Oikonomou, A. and Bleris, G.L. (2002). Code quality analysis in open source software development. *Information Systems Journal*, 12(1), 43–60.

41. Suguna, S. and Suhasini, A. (2015). Overview of data backup and disaster recovery in cloud. *2014 International Conference on Information Communication and Embedded Systems, ICICES* 2014, 978. https://doi.org/10.1109/ICICES.2014.7033804

42. Thomas, J.A. and Valvano, M.A. (1992). tolQ is required for cloacin DF13 susceptibility in Escherichia coli expressing the aerobactin/cloacin DF13 receptor IutA. FEMS Microbiology Letters, 91(2), 107–111. https://doi.org/10.1016/0378-1097(92)90668-E

43. Usman, M., Ahmad Jan, M. and He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences*, 387, 90–102.

44. Vanbrabant, B. and Joosen, W. (2014). Configuration management as a multi-cloud enabler. *In Proceedings of the 2nd International Workshop on CrossCloud Systems* (pp. 1-3).

45. Wagle, S.S., Guzek, M., Bouvry, P. and Bisdorff, R. (2015). An evaluation model for selecting cloud services from commercially available cloud providers. *In 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)* (107-114). IEEE.

46. Sambrani, Y. Rajashekarappa. (2016). Efficient data backup mechanism for cloud computing. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(7), 92-95.

47. Zhang, S., Li, X., Zong, M., Zhu, X. and Wang, R. (2017). Efficient kNN classification with different numbers of nearest neighbors. *IEEE transactions on neural networks and learning systems*, 29(5), 1774-1785.

48. Zheng, P., Qi, Y., Zhou, Y., Chen, P., Zhan, J. and Lyu, M.R. (2014). An automatic framework for detecting and characterizing performance degradation of software systems. *IEEE Transactions on Reliability*, 63(4), 927–943. https://doi.org/10.1109/TR.2014.2338255