JOINT EMERGENCY DATA AND SERVICE EVACUATION IN CLOUD DATA CENTERS AGAINST EARLY WARNING DISASTER

[1] A. RACHEL, [2] MD. SALEEM, [3] S. NARASIMULU

[12]Assistant Professor, Department of IOT, Sri Indu College of Engineering and Technology, Hyderabad, Telangana-501510

[3]Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology, Hyderabad, Telangana-501510

ABSTRACT

As crucial network infrastructures for data storage and service delivery for customers worldwide, cloud data centers are greatly threatened by disasters that occur frequently around the world. It making the ability of cloud data centers to survive a crucial problem. This article examines a combination design of data and service evacuations to combat disasters because they are both desired simultaneously in a genuine crisis scenario. We take into account disasters that can provide an early warning period before they actually affect cloud data centers, and by utilizing the inherent interaction between data and service evacuations and effectively utilizing the early warning period, we propose a joint data and service evacuation scheme for emergency protection. First, we use two ideal Integer Linear Program (ILP) models to represent the joint design. Due to the early warning time constraint, it is important to note that the protection process is highly time-sensitive. To improve the sharing of network resources between data backup and service migration, two time-efficient heuristics are then designed by carefully choosing evacuated services and candidate evacuation nodes. Many numerical findings show how effective the suggested plan is at enhancing the survivability of data and services in cloud data centers. This study can assist data center operators in achieving a trade-off between data backup and service migration under a set of predetermined resource and early warning time limitations.

1. Introduction:

Large-scale disasters can severely disrupt Information Technology (IT) infrastructure, e.g., Data Centers. Earthquakes, hurricanes, tsunamis, and other natural catastrophes may lead to such a scenario. Man-made threats, e.g., a High-Altitude Electromagnetic Pulse (HEMP), can also provoke such an aftermath. In the HEMP case, however, the aftermath might include damage even to non-terrestrial IT infrastructure, such as satellites. After any disaster, it is important that critical data located in the affected region be evacuated to secure locations where it can be useful for emergency operations, mission-critical activities, rescue and relief efforts, and society and businesses in general. To minimize the time it takes to perform this evacuation, we must use all available resources as efficiently as possible. This includes using the remaining satellites to connect the affected regions of the network to the unaffected ones. Utilizing the Software-Defined Network (SDN) paradigm applied to satellite networks, we propose an algorithm that can be executed by the SDN controller [1]. This algorithm generates an evacuation plan for data located in possibly-isolated terrestrial systems, such as Data Centers, through the satellite network, towards

final destinations in the main network [2]. The evacuation plan is a transmission schedule that maximizes the amount of evacuated data. Considering the current industrial interest in mega satellite constellations, we compare how two constellations of 66 and 720 satellites perform in terms of amount of data evacuated. Our results show how the evacuation is affected by different satellite constellation configurations (i.e., buffers, inter-satellite link capacities, etc.). Since our approach allows for Traffic Engineering (TE) to be performed, we also demonstrate how it enables fair resource utilization among different affected infrastructures during data evacuation. Our illustrative examples also compare our method to an approach designed for Delay-Tolerant-Vehicle networks and show how our solution can evacuate up to 60% more data after a disaster [3].

EWS development is crucial for sustainable development and building resilience of the cities. It is therefore important to develop a EWS framework and strengthen strategies across all levels to ensure better coordination efforts for functional EWS at the city level. This must be seen as opportunity to strengthen network among institutions, foster partnerships and build the capacities of all keys stakeholders. EWS framework must be made as a functional component of the DM Plan process (national/ state/district/city). The framework must foster areas of cooperation in data sharing and impact forecasting [4]. It is widely realized that city institutions are being rather response-centric instead of being the ones that take preventive measures. The technical capacity in understanding DRR, risk assessment and EWS needs to be strengthened at the ULB level. City level hazard and vulnerability mapping capabilities need to be enhanced on priority basis. A long-term perspective on capacity development should be envisaged. There is a common challenge in the interpretation of the forecast products. Technical agencies involved in providing warning have to evolve in providing information that can either be used by a wide pool of users or create products based on user needs [5].

Technical agencies/scientific institutions must also enhance the capability to deliver timely warnings with sufficient respite time so that they support DRR functions at the city level

2. Literature Survey

As pointed out above, emergency data and service evacuations are studied as two separate subproblem in existing literatures. This is mainly because they consider different design objectives. In particular, emergency data evacuation requires to back up as much data as possible within the given early warning time (i.e., maximize the amount of backup data). In contrast, emergency service evacuation considers to migrate as much service as possible (i.e., maximize the number of migrated services), in which the ability of migrated services for recovering disaster-affected connections needs to be considered [6]. However, data and service evacuations are both desired at the same time as two key processes to support a more comprehensive survivability. This motivates us to explore intrinsic interplay between the two processes, and carry out a joint design to achieve a better survivability against disasters. Joint design of data and service evacuations can also provide a flexible trade-off between the two for data center operators [7].

Existing Problem

This is mainly consider different design objectives. In particular, emergency data evacuation requires to back up as much data as possible within the given early warning time (i.e., maximize the

amount of backup data). In contrast, emergency service evacuation considers to migrate as much service as possible (i.e., maximize the number of migrated services), could be due to the complexity of the joint design problem. In general, a disaster disrupts a wide geographical range and multiple data centers. As a result, a huge amount of data and services hosted at those disaster-affected data centers should be evacuated. , our work falls into the category of emergency protection. As far as we know, it is the first work to jointly design data and service evacuation under the constraints of available network resources and the given early warning time [8].

Drawback in Existing System

- There is evidence that the prediction value of generic early warning scores suffers in comparison to specialty-specific scores, and that their sensitivity can be improved by the addition of other variables.
- They are also prone to inaccurate recording and user error, which can be partly overcome by automation

Survey 1

Title

Disaster-Aware Submarine Fiber-Optic Cable Deployment for Mesh Networks

Authors Dawson Ladislaus Msongaleli, Ferhat Dikbiyik, Moshe Zukerman, and Biswanath Mukherjee

With the increasing social and economic reliance on the Internet and the significant monetary and non-monetary societal cost associated with service interruption, network survivability is an important element in telecommunication network design. A major cause of Internet service interruption is breakage of fiber-optic cables due to man-made or natural disasters such as earthquakes. In addition to the societal cost, there is also cost of repairing damaged cables paid by the cable owner. A disaster resilient submarine cable deployment can achieve significant cost saving when disaster strikes [9]. In this study, we investigate a disaster-aware submarine fiber-optic cable deployment optimization problem to minimize such expected costs in case of a disaster. While selecting paths for the cables, our approach aims to minimize the expected cost for both cable owner and the affected society, considering that submarine fiber-optic cables may break because of natural disasters, subject to limitation of available deployment budget and other constraints. In our approach, localized disaster-unrelated potential disconnection (e.g., due to shark bites) are avoided by providing a backup cable along with primary cable. We consider a mesh topology network with multiple nodes located at different sea/ocean shores, submarine fiber-optic cables of irregular shape, and a topography of undersea environment [10]. We present an Integer Linear Program to address the problem, together with illustrative numerical examples. Finally, we validate our approach by applying it to a case study of an existing cable system in the Mediterranean Sea, and the results show that we can significantly reduce overall expected cost at a slight increase in deployment cost. The results demonstrate a potential saving of billions of US dollars for the society in case of a future disaster. In order to achieve such large savings, cable companies may require to lay somewhat longer cables to avoid potential disaster areas, which may increase deployment cost that is relatively smaller compared to potential savings in case of a disaster. Understanding such

trade-offs is important for stakeholders, including government agencies, cable industry, and insurance companies, which may have different objectives, but can work together for the overall benefit of the society [11].

Advantages

➢ Low overhead on computation and communication cost.

➢ A ranked search mechanism to support extra search semantics and dynamic data operations.

➢ It is more secure and efficient mechanism.

Disadvantages

➢ The large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need.

➢ Single-keyword search without ranking.

Survey 2

Title: Online Virtual Machine Evacuation for Disaster Resilience in Inter Data Center Networks

Authors :Omran Ayoub, Amaro de Sousa, Silvia Mendieta, Francesco Musumeci and Massimo Tornatore

With the risk of natural disaster occurrence rising globally, the interest in innovative disaster resilience techniques is greatly increasing [12]. In particular, Data Center (DC) operators are investigating techniques to avoid data-loss and service downtime in case of disaster occurrence. In cloud DC networks, DCs host Virtual Machines (VM) that support cloud services. A VM can be migrated, i.e., transferred, across DCs without service disruption, using a technique known as “online VM migration”. In this paper, we investigate how to schedule online VMs migrations in an alerted disaster scenario (i.e., for those disasters, such as tsunami and hurricanes, that grant an alert time to DC operators) where VMs are migrated from a risky DC, i.e., a DC at risk to be affected by a disaster, to a DC in safe locations, within a deadline set by the alert time of the incoming disaster. We propose a multi-objective Integer Linear Programming (ILP) model and heuristic algorithms for efficient online VMs migration to maximize number of VMs migrated, minimize service downtime and minimize network resource occupation. The proposed approaches perform scheduling, destination DC selection and assign route and bandwidth to VM migrations. Compared to baseline approaches, our proposed algorithms eliminate service downtime in exchange of an acceptable additional network resource occupation. Results also give insights on how to calculate the minimum amount of time required to evacuate all VMs with no service downtime. Moreover, since the proposed approaches exhibit different execution times, we design an ‘alert-aware VM evacuation’ tool to intelligently select the most suitable approach based on the number and size of VMs, alert time and available network capacity [13].

Advantages

➢ Shift from a clinic-oriented, centralized healthcare system to a patient-oriented, distributed healthcare system.

➢ Reduce healthcare expenses through more efficient use of clinical resources and earlier detection of medical conditions.

Disadvantages

➢ Performance, Reliability, Scalability, QoS, Privacy, Security.

➢ More prone to failures, caused by power exhaustion, software and hardware faults, natural disasters, malicious attacks, and human errors etc.

Survey 3

Title:A Quick Survey on Cloud Computing and Associated Security, Mobility and IoT Issues

Authors :Michael Perez, Sanjeev Kumar

Major aspects of Cloud Computing are explained to give the reader a clearer understanding on the complexity of the platform. Following this, several security issues and countermeasures are also discussed to show the major issues and obstacles that Cloud Computing faces as it is being implemented further. The major part of countermeasures focuses on Intrusion Detection Systems. Moving towards Mobile Cloud Computing and Internet of Things, this survey paper gives a general explanation on the applications and potential that comes with the integration of Cloud Computing with any device that has Internet connectivity as well as the challenges that are before it [14].

Advantages

➢ Optimum combination of coding opportunity and coding validity.

➢ Improve Network Performance.

➢ To distribute the flow of data to different routing to make sure energy consumption is balanced.

➢ Connected Dominating Set (CDS) can efficiently cover the network topology, dominating nodes are a good choice to converge data flows

Disadvantages

➢ Coding collision is a severe problem affecting network performance

➢ Increase packet loss ratio.

Survey 4

Title:Blackout Resilient Optical Core Network

Authors:Zaid H. Nasralla , Taisir E. H. Elgorashi , Ali Hammadi , Mohamed O. I. Musa ,and Jaafar M. H. Elmirghani , Fellow, IEEE

A disaster may not necessarily demolish the telecommunications infrastructure, but instead it might affect the national grid and cause blackouts, consequently disrupting the network operation unless there is an alternative power source(s). In disaster-resilient networks, fiber cut, datacenter destruction, and node isolation have been studied before with different scenarios, but the power outage impact has not been investigated before. In this paper, power outages are considered, and the telecommunication network performance is evaluated during a blackout. A mixed Integer Linear Programming (MILP) model is developed to evaluate the network performance for a single node blackout under two scenarios: minimization of blocking and minimization of renewable and battery energy consumption. Insights analyzed from the MILP model results have demonstrated the trade-off between the two evaluated optimization cost functions and shown that the proposed scheme can extend the network lifetime while minimizing the required amount of backup energy [15].

Disadvantages

• It is unable to use a single computer or server to deal with the big data.

• When all the data need to be uploaded to the cloud, a large number of security risks can be arise.

Advantages

• The big data research is to process large amounts of data to obtain significant information.

• It provides high-quality cloud services via the Internet.

Survey 5

Title: Load Balancing in Data Center Networks: A Survey

Authors: Jiao Zhang , Member, IEEE, F. Richard Yu , Fellow, IEEE, Shuo Wang , Tao Huang, Zengyi Liu, and Yunjie Liu

Data center networks usually employ the scale-out model to provide high bisection bandwidth for applications. A large amount of data is required to be transferred frequently between servers across multiple paths. However, traditional load balancing algorithms like equal-cost multi-path routing are not suitable for rapidly varying traffic in data center networks. Based on the special data center topologies and traffic characteristics, researchers have recently proposed some novel traffic scheduling mechanisms to balance traffic. In this paper, we present a comprehensive survey of recent solutions for load balancing in data center networks. First, recently proposed data center network topologies and the studies of traffic characteristics are introduced. Second, the definition of the load-balancing problem is described. Third, we analyze the differences between data center load balancing mechanisms and traditional Internet traffic scheduling. Then, we present an in-depth overview of recent data center load balancing mechanisms. Finally, we analyze the performance of these solutions and discuss future research directions [16].

Advantages

• It maximizes the potential for energy savings through fine-grained code offload while minimizing the changes required to applications.

• It achieves the benefits by using several properties of today's managed code environments.

• MAUI offers significant energy and performance benefits to mobile applications.

Disadvantages

• During runtime offloading such as timely triggering of adaptive offloading.

• Selection of an application partitioning policy.

3. Proposed System

The objective of the proposed model is to maximize the amount of backup data under the constraints of available network resources, the given early warning time and the number of services that are expected to be migrated. The second one is with the objective of maximizing the number of migrated services under the constraints of available network resources, the given early warning time and the amount of backup data (called SMDB). To meet the stringent requirement of emergency evacuations and time sensitivity due to the limited early warning time, two time-efficient heuristics are designed to provide fast solutions, where evacuated services and candidate evacuation nodes are carefully selected to better share network resources between data backup and service

migration. Data center and content placement problem by taking no uniform distribution of potential disasters into account. Submarine fiber-optic cable deployment is investigated for mesh networks against disaster [17].

- Primary and backup data centres and paths are set for connection requests to minimize loss of network operators under disaster.
- Proposes a backup computing and transmission resource allocation model with a probabilistic protection for virtual networks against multiple facility node failures to minimize backup computing and transmission capacity.

A heterogeneous data backup scheme against early warning disasters is proposed in with fairness considerations for different types of data. In our project we are proposed the system is Rescue Management Server (RMS). This server collects the data automatically from the weather application. Rescue Manager Details are stored in CRMS server. Capacity First (CF) method is designed to deal with the service capacity constraint in the migration Bandwidth First (BF) method is provided to sort the disaster-affected services in ascending order according to the overall required bandwidth of all connections requestingIf any changes occurred in weather Disaster Management Server, it sends the disaster notification and location for registered android mobile users through the Cloud Rescue Management Server (CRMS). Cloud Rescue Management Server checks the disaster and rescue manager's locations. We have planned in future to implement the project is automatically detect the disaster and get the notifications for all type of mobile users.

Advantages

- Cost Reduction. It's a basic financial principle that profit comes from making more money than you spend.
- To reduce the downtime.

Solution & Technical Architecture

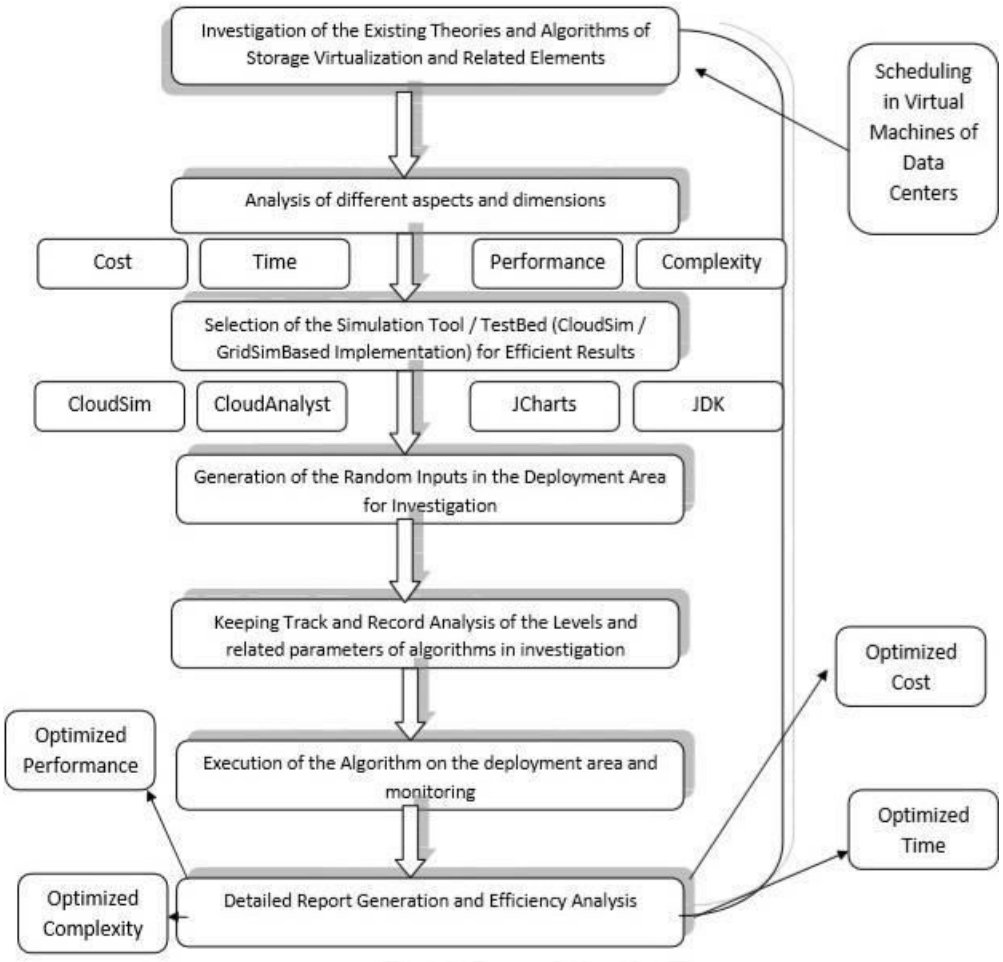

Figure 1.Flow of Process

Step1: Initialization: The initial population of candidate solutions is usually generated randomly across the search space.

Step2: Evaluation: Once the population is initialized or an offspring population is created, the fitness VM values of the candidate solutions are evaluated.

Step3: Selection: Selection allocates more copies of those solutions with higher fitness values and thus imposes the survival-of-the-fittest VM mechanism on the candidate solutions.

Step4: Mutation: While recombination operates on two or more parental chromosomes, mutation locally but randomly modifies a solution [18].

Step5: Replacement: The offspring population created by selection, recombination, and mutation replaces the original parental population

4. Implementation

1 Prover

The node who needs to collect location proofs from its neighboring nodes. When a location proof is needed at time t, the prover will broadcast a location proof request to its neighboring nodes through Bluetooth. If no positive response is received, the prover will generate a dummy location proof and submit it to the location proof server.

2 Witness

Once a neighboring node agrees to provide location proof for the prover, this node becomes a witness of the prover. The witness node will generate a location proof and send it back to the prover.

3 Location Proof Server

As our goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history records of the location proofs. It communicates directly with the prover nodes who submit their location proofs. As the source identities of the location proofs are stored as pseudonyms, the location proof server is un trusted in the sense that even though it is compromised and monitored by attackers, it is impossible for the attacker to reveal the real source of the location proof.

4 Certificate Authority

As commonly used in many networks, we consider an online CA which is run by an independent trusted third party. Every mobile node registers with the CA and pre-loads a set of public/private key pairs before entering the network. CA is the only party who knows the mapping between the real identity and pseudonyms (public keys), and works as a bridge between the verifier and the location proof server. It can retrieve location proof from the server and forward it to the verifier.

5. Results

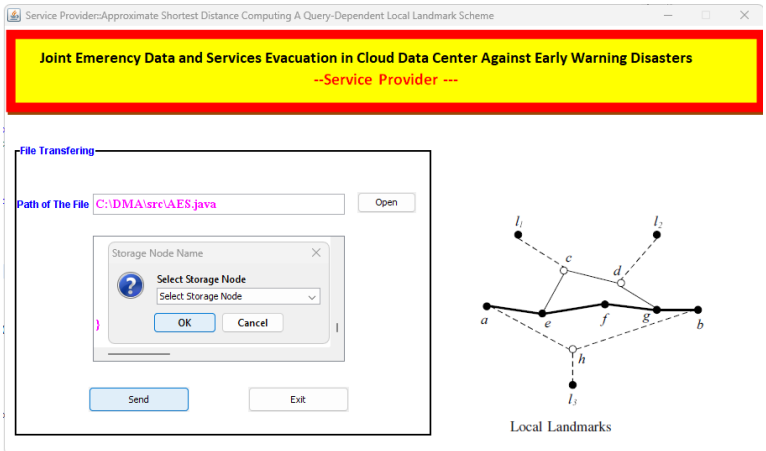

Figure 2 Service Provider

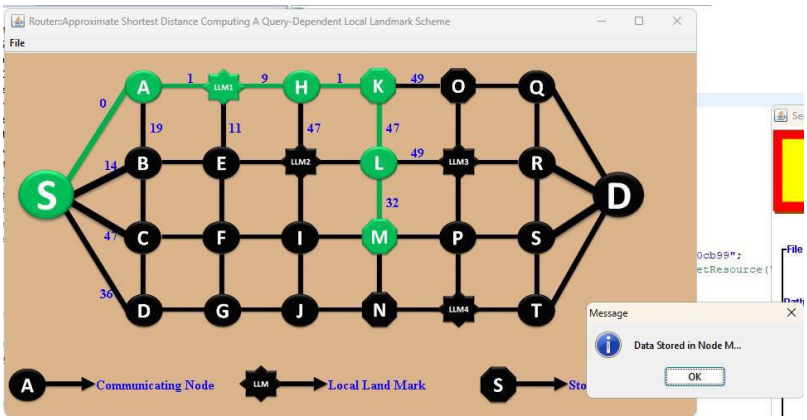

Figure 2 Query Router

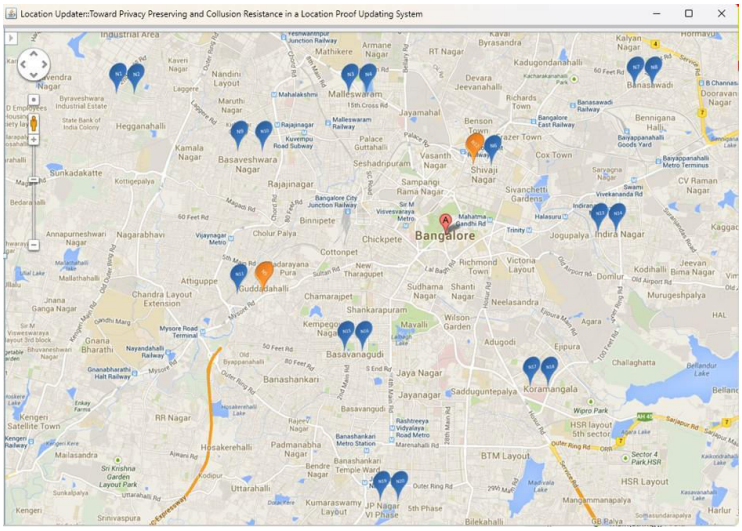

Figure 4 Location Updater

6. Conclusion

Under a given early warning time constraint, we proposed a joint emergency data and service evacuation scheme in cloud data centers against disasters to achieve a comprehensive survivability, as well as a flexible tradeoff between data backup and service migration. Our work includes two optimal Integer Linear Program (ILP) models and efficient heuristics. The former provides optimal solutions for migrated services and backup data. The latter renders fast and time efficient solutions to meet the stringent time constraint in the disaster scenario, and achieves high protection performance with improved survivability and tradeoff flexibility. This gives data center operators a guide to determine the amount of data and services that should be evacuated for survivability improvement. Numerical results showed that the proposed joint design is efficient to fight against early warning disasters.

References

[1]. T. Adachi, Y. Ishiyama, Y. Asakura, and K. Nakamura,(2011) 'The restoration of telecom power damages by the Great East Japan Earthquake', in Proc.IEEE 33rd Int. Telecommun. Energy Conf., pp. 1–5.

[2]. O. Ayoub, A. D. Sousa, S. Mendieta, F. Musumeci, and M. Tornatore, (2021) 'Online virtual machine evacuation for disaster resilience in inter-data center networks', IEEE Trans. Netw. Service Manag., vol. 18, no. 2, pp. 1990–2001,.

[3]. N. H. Bao, M. F. Habib, M. Tornatore, C. U. Martel, and B. Mukherjee, (2015) 'Global versus essential post-disaster re-provisioning in telecom mesh networks,' IEEE/OSA J. Opt. Commun. Netw., vol. 7, no. 5, pp. 392–400,.

[4]. M. Bari et al.,(2013) 'Data center network virtualization: A survey,' IEEE Commun. Surveys Tuts., vol. 15, no. 2, pp. 909–928, 2nd Quart.,.

[5]. C. Colman-Meixner, C. Develder, M. Tornatore, and B. Mukherjee,(2016) 'A survey on resiliency techniques in cloud computing infrastructures and applications,' IEEE Commun. Surveys Tuts., vol. 18, no. 3,pp. 2244 –2281, 3rd Quart.,.

[6]. C. N. Da Silva, L. Wosinska, S. Spadaro, J. C. W. A. Costa, C. R. L. Francˆes, and P. Monti,(2016) 'Restoration in optical cloud networks with relocation and services differentiation,' IEEE/OSA J. Opt. Commun. Netw.,vol. 8, no. 2, pp. 100–111,.

[7]. F. Dikbiyik, M. Tornatore, and B. Mukherjee,(2014) 'Minimizing the risk from disaster failures in optical backbone networks,' J. Lightw. Technol., vol. 32, no. 18, pp. 3175–3183,.

[8]. S. Ferdousi et al.,(2020) 'Joint progressive network and datacenter recovery after large-scale disasters,' IEEE Trans. Netw. Service Manag., vol. 17, no. 3, pp. 1501–1514.

[9] K. Bhargavi. An Effective Study on Data Science Approach to Cybercrime Underground Economy Data. Journal of Engineering, Computing and Architecture.2020;p.148.

[10] [21] M. Kiran Kumar , S. Jessica Saritha. AN EFFICIENT APPROACH TO QUERY REFORMULATION IN WEB SEARCH, International Journal of Research in Engineering and Technology. 2015;p.172

[11] K BALAKRISHNA,M NAGA SESHUDU,A SANDEEP. Providing Privacy for Numeric Range SQL Queries Using Two-Cloud Architecture. International Journal of Scientific Research and Review. 2018;p.39

[12] K BALA KRISHNA, M NAGASESHUDU. An Effective Way of Processing Big Data by Using Hierarchically Distributed Data Matrix. International Journal of Research.2019;p.1628

[13] P.Padma, Vadapalli Gopi,. Detection of Cyber anomaly Using Fuzzy Neural networks. Journal of Engineering Sciences.2020;p.48.

[14] Kiran Kumar, M., Kranthi Kumar, S., Kalpana, E., Srikanth, D., & Saikumar, K. (2022). A Novel Implementation of Linux Based Android Platform for Client and Server. In A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems (pp. 151-170). Springer, Cham.

[15] Kumar, M. Kiran, and Pankaj Kawad Kar. "A Study on Privacy Preserving in Big Data Mining Using Fuzzy Logic Approach." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 11.3 (2020): 2108-2116.

[16] M. Kiran Kumar and Dr. Pankaj Kawad Kar. "Implementation of Novel Association Rule Hiding Algorithm Using FLA with Privacy Preserving in Big Data Mining". Design Engineering (2023): 15852-15862

[17] K. APARNA, G. MURALI. ANNOTATING SEARCH RESULTS FROM WEB DATABASE USING IN-TEXT PREFIX/SUFFIX ANNOTATOR, International Journal of Research in Engineering and Technology. 2015;p.16.

[18]. M. F. Habib, M. Tornatore, M. D. Leenheer, F. Dikbiyik, and B. Mukherjee, (2012) 'Design of disaster-resilient optical datacenter networks,' J. Lightw. Technol., vol. 30, no. 16, pp. 2563–2573.