Digital Information Management in Ardent Era - A Case Study

Monika Verma, Mohit Kumar Verma and Pawan Kumar

The present study investigated the aim and implementation challenges of NIScPR Data centre, including its deployed architecture, functional components requirement and importance. We also explore applications of data centre hardware components as well as usefulness of running applications. The personnel interaction and interview method has been used to find out the essential information. In depth we found that CSIR-NIScPR has bulk of digital information resources, services, web portal, including official websites of CSIR headquarter and sister labs. Study revealed the importance of streamlining of all the NIScPR services, which running on multiple standalone servers were situated at, distinguish locations. Now, various national level services such as CSIR-IPU Unit, NKRC, ISSN, ISA, OP, NOPR, NSDL and NUCSSI are running properly and securely with effective failure management system.

Introduction

Data centres have recently received significant attention as a cost-effective infrastructure for storing large volumes of data and hosting large-scale service applications of muti-national companies like Amazon, Google, Facebook, and Yahoo!. These MNCs routinely use data centres for storage, Web search, and large-scale computations and service hosting in data centres has become a multibillion dollar business that plays a crucial role in the future Information Technology (IT) industry[1,2].

Today, most of the government organizations providing various services such as mail service, web site hosting service, social networking sites, blogs and video uploading platforms, which has more user hits i.e. multiple access in same time, all these services are routinely using data centre. Thus, it is essential that the data centres have sufficient infrastructure which works in efficient manner like provide variety of network services, secure data storage for high volume data, internet based high demand applications with uninterrupted power supply, bandwidth, latency etc.

NIScPR (National Institute of Science Communication and Policy Research) erstwhile known as NISCAIR (National Institute of Science Communication and Information Resources) is one of the premier labs of CSIR (Council of Scientific and industrial Research) out of 37 research laboratories. CSIR is funded by Ministry of Science and Technology, Government of India to pursue science which strives for global impact, technology that enables innovation driven industry and nurture trans-disciplinary leadership thereby catalyzing inclusive economic development for the people of India.[3]

In this chain NIScPR vision is to become a globally respected think-tank and resource center for undertaking Science, Technology & Innovation Policy Research and Science Communication and mission is to promote

STI (Science, Technology and Innovation) policy studies and science communication among diverse stakeholders and act as a bridge at the interface of science, technology, industry and society which is essential to a robust S&T ecosystem in the country[4].

NIScPR is the prime custodian of vast pool of digital information resources of CSIR. Therefore, the main work of NIScPR is to collect, store, publish, sale and spread S & T Information in printed and online version (through research journals, magazines and books) for different age group peoples in this high-tech era. The volume of data, being managed at NIScPR, in the form of databases and CDs (is in Tera Bytes with an exponential growth of data in this digital era). NIScPR also acts as repository of library and analytical facilities and now-a-days knowledge repositories are growing at an exponential rate, which require massive and updated capabilities for management of information resources and services including hosting and sharing. In-spite of this, NIScPR digital resources & services are dated and dis-jointed because it functioning at two separate locations. The services and data hosted on standalone servers are in an unorganized manner i.e. without any redundant infrastructure, major security and archival/ backup facility. This has significantly impacted reliability and quality of NIScPR's services.

2. Review of Literatures

Due to globalization the demand of data storage and information retrieval is increased now, including massive information transmission and sharing. In the past few years several researchers have proposed and configured data-centres, providing secure and stable infrastructure to multiple independent clients to host their applications in their data centre. The data centre service provider, depending on the service agreement, may provide a physical or virtual isolation of network, bandwidth, and network and application security. This type of arrangement is called as co-location of services and data centre may be called as shared data centre. For example, several ISPs and other web service providers host multiple unrelated web-sites on their data-centers, such differentiation becomes essential in several scenarios in a shared data-centre environment[5].

Ramroop S & Pascoe R (1999) presenting the implementation architecture of Ramroop and Pascoe's conceptual model for data integration in a Geographic Information System (GIS) environment. The model consists of a data centre and data agencies at a national level. Details of the actual processing steps followed within the Data Center are discussed and the architecture design is described. The architecture of the Virtual Data Center is presented by explaining the processes involved when integrating data sets at the National level[6].

Wen-Syan Li et al (2004) had discussed the system architecture of data center-hosted database-driven websites, data centres deploying cache portal technology, operation flow, handling secured communication protocols, handling cookies, JSP (Java serverlet pages) based dynamically assembled pages, user response time etc[7].

Curtis A R et al (2012) had discussed an algorithm for data centre network design framework. In this algorithm, they had searched a network with maximum bisection bandwidth and minimal end-to-end latency while meeting user-defined constraints and predicated cost of network[8].

Bari M F et al (2013) had studied various protocols given by various researchers, related to data centre network virtualization. They told about various key points about data centre and discussed traditional TCP/ IP protocol for data centre. They had classified various aspects of proposal of researchers along with qualitative comparison of these proposals, with respect to essential key points of data centre.[9].

Sukmana H T et al (2016) mentioned that a Data centre is a place where data and applications placed and run. The data and applications saved on various server based on the function of application run such as server of database, proxy, portal, website, application, mikrotic and so on. The more vary application run, the more server types needed. There are several implications when data center encounter "server flood", where more electrical energy must be provided. There is still one problem faced by system administrators with the number of servers in the data center, the more the server to be maintained. The solution that can be done to solve this situation is by using virtualization of the servers. Virtualization, depending on the available hardware resource i.e. CPU, RAM, Storage, network etc., allows to split a physical machine in to multiple independent virtual machine (VM) and the results made are by using VM terms of energy consumption, it can provide a savings of more than 50 percent[10].

As per review, it is found that the use of data centre are growing due to vigorous increment in data at everywhere, but there are very less systematic studies are available, which were related to the real implementation of data centre and its operations issues.

3. Objectives

The main objectives of this study were:

3.1.1. To know the purpose of NIScPR data centre;

3.1.2. To study its implementation challenges;

3.1.3. To identify its application requirements;

3.1.4. To explore the main components of data centre with its deployed architecture;

3.1.5. To find out functions of main components and risk management tools of data centre;

3.1.6. To understand the usefulness and currently running services of data centre;

4. Research Methodology

All the presented information's, photographs and data have been collected from the NIScPR data centre during visits and personal interaction. The interview method has been used for the completion of presented study, which involve Head-IT and presently working data centre team. The relevant important information is collected from official websites of organisation, data centre and from annual reports.

5. Analysis and Findings

5.1. Purpose of NIScPR Data Centre

Keeping all goals in mind NIScPR team tried to established the NIScPR Data Centres to provide the uninterrupted authorized and secure access of NIScPR digital resources, assets and services among the researchers & scientific community in the centralized manner and integrated form (i.e. on remote and local platform), with fast processing of data in cost effective manner, with service level redundancy and minimum errors. It is also used for the co-location of other CSIR laboratories servers and services and being used as primary and disaster recovery (DR) site for the laboratories. In the other words, setting up NIScPR Data Centre has singular focus on setting up an integrated state-of-art facility for managing and sharing digital information resources of CSIR laboratories. The purposes of establishment of NIScPR data centre are following:

5.1.1. To host, manage and secure the digital resources and services;

5.1.2. To provide uninterrupted authorized and secure access (remote & local both) of its digital resources, assets and services to the scientific community and researchers all over the world;

5.1.3. To provide long-term scalable server and storage infrastructure;

5.1.4. To manage high volume of incoming and outgoing traffic; and

5.1.5. To streamline net-centric operations.

5.2. Challenges for Implementation of NIScPR Data Centre

Universities and colleges data centre is a system engineering data centre with high efficiency, safety and reliability can realize the unified management of data resources. The basic link of laboratory construction is the data sharing among the entire professional laboratory, thus improving the utility efficiency of teaching & research and play an active role in improving personnel training quality and efficiency. Hence, there are following kind of challenges were faced –

5.2.1 Performance interference, costs and optimization of compute, storage and network resources network resource within and across data centre;

5.2.2 Competing and emerging technologies for data centre networking, such as data centre bridging in IEEE 802, fiber channel over Ethernet (FCoE) as well as flexible network architectures and communications protocols;

5.2.3 Intra-data centre and inter-data centre network traffic characteristics, innovative traffic, engineering and routing optimization approaches;

5.2.4 Instrumentation, measurement and evaluation of data centre performance;

5.2.5 Accurate monitoring and prediction of service availabilities and qualities;

5.2.6 Migration of internet large-volume applications and distribution of large-volume data and content;

5.2.7 Risk challenges and solution of security and privacy guarantees.

5.3. NIScPR Data Centre Application Requirements

5.3.1. System Operation Platform — it used to provide a uniform foundation platform to support common OS, the application of DBMS (Database Management System), the shared system software, and general middleware and so on.

5.3.2. Data Management Platform — formulating unified data management strategy in system level using data management tools to implement unified planning and management of data, to guarantee the standardization of data management, security of data access to meet the application demand.

5.3.3. Data Disaster Recovery Backup — there is a unified data storage and disaster recovery backup system to store and retrieve data.

5.3.4. Safety Protection System — the unified safety and protection system prevent has components required to protect the application, server and equipment's form fire, invasion and unauthorized access.

5.4. NIScPR Deployed Data Centre Architecture and Components

The motto of this research includes the designing and development of data centre architecture, hardware availability, proper installation and commissioning of all the related networking equipments, storage devices and high-end servers. The data centre should provide a uniform data storage, data backup, data processing, network information safety and system management services for each professional application system and in-use databases. Through the integration of the professional laboratory information resources, the data centre should provide support for information sharing, professional cooperation, public service, assistant decision and should build a unified development, application and management platform for the laboratory research.

The architecture of data centre is:

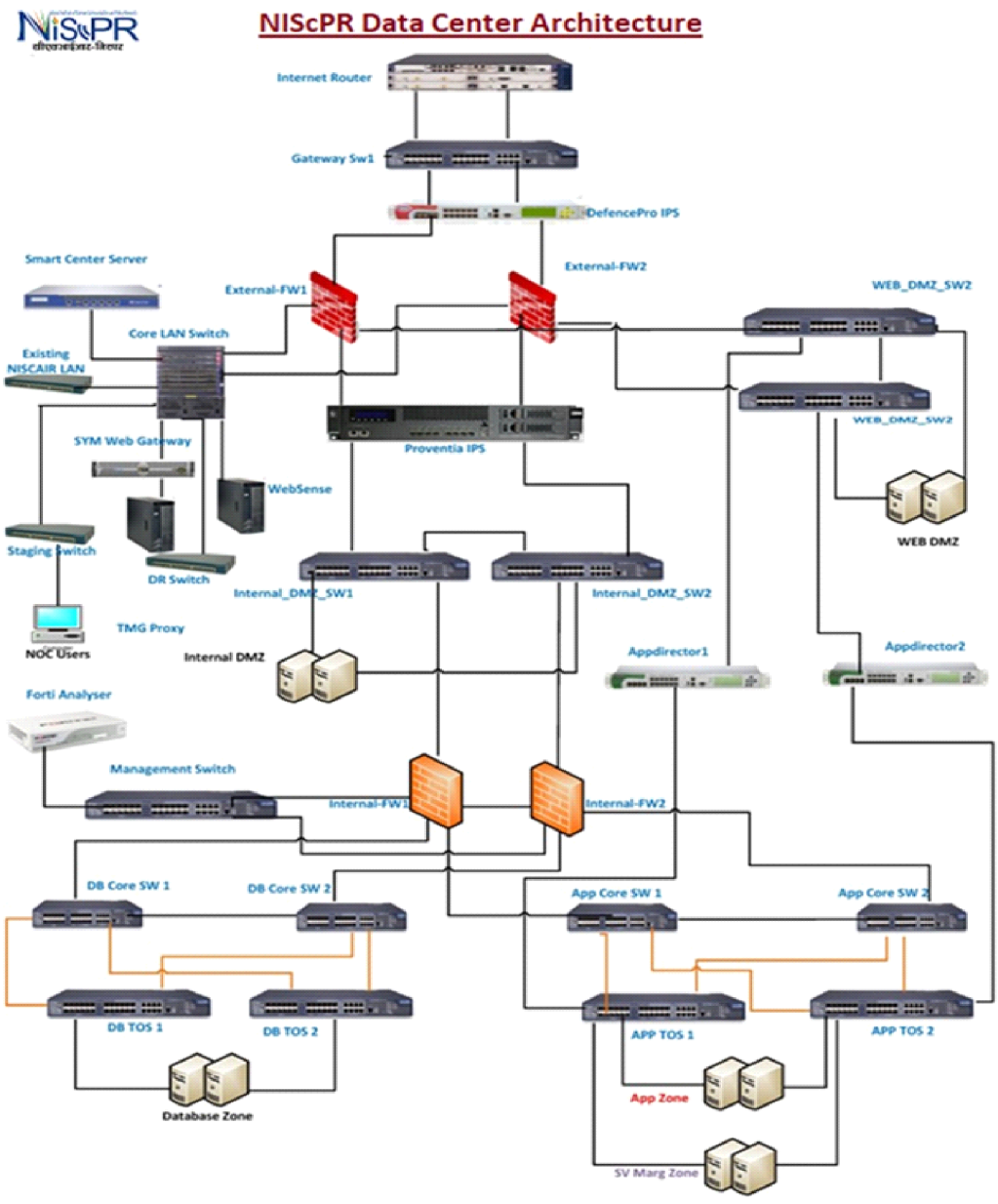

Figure 1: Deployed NIScPR data centre network architecture

The main components of a data centre are classifie1d into two main parts-

5.4.1. IT Components

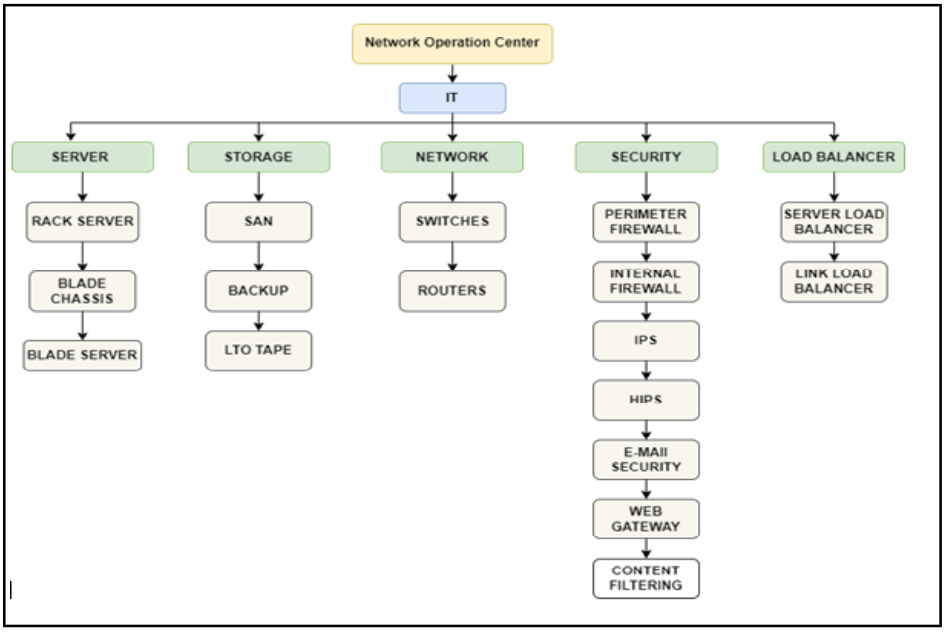

Figure 2: Major IT components and their sub-units.

5.4.2. Non-IT Components

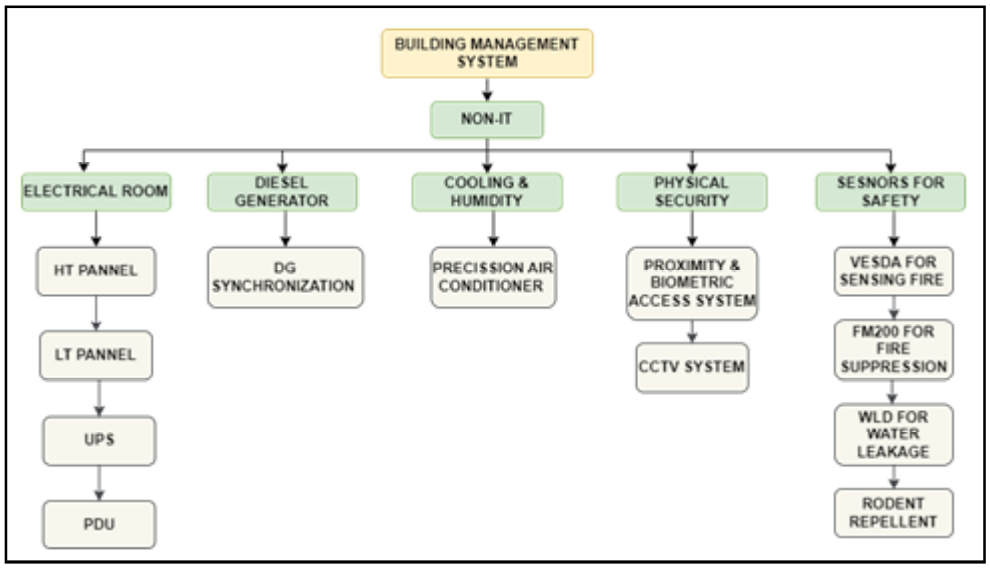

Figure 3 : Major non-IT components and their sub-units

5.5. Functions of Main Components

5.5.1. Network Security

5.5.1.1. Two Tier Security — the data centre is equipped with two tier security with heterogeneous solution from multiple vendors, which helps to eliminated possible security breach.

5.5.1.2. Perimeter Intrusion Prevention System (IPS) — is placed on the top of the network. IPS protects the data centre network from security threats, providing auto signature based protection and examines all inbound connection for suspicious characteristics like modified frame, packets, DDoS attacks etc. and only authorised traffic is allowed.

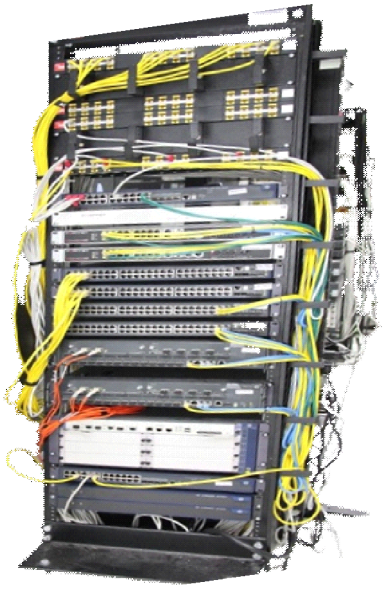

Figure 4 : Network Rack

Figure 5: Firewall

5.5.1.3. External Firewall — is the second layer security, restricting the external user access to data centre. It also provides secure connections to the multiple Host/User to access data centre applications from internet, including stateful inspection features, which helps to reduce the session hijacking possibilities and protects the IP spoofing threats. This firewall is deployed in high availability (N+1 fashion) to eliminate the chances of hardware failure.

5.5.1.4. Web Gateway — provides the Application/Content based security to prevent malicious traffic (malware, viruses, etc.) from internet While users do the browsing then, web gateway blocks the executables sites or files to be downloaded from internet.

5.5.1.5. Internet Firewall — provides zone based security and zone to zone firewall policies provide additional security to database and application zone.\

5.5.1.6. Internal IPS — is the second layer IPS security because its place behind the external firewall and restricting the SPAM/Intruders/Hackers etc. with latest security signatures from both Internet/ Intranet traffic.

5.5.1.7. Host Based Intrusion Prevention System (HIPS) — is providing host based security to protect servers from attacks and manage compliance with monitoring, recording, auditing.

5.5.1.8. Mail Security — CISCO IronPort appliance enhances the security to Mail Server, so that malware/ Spam mail traffic can be discarded. It reviews sender reputation, examine the complete context of a message, filter more accurately then the traditional spam screening techniques.

5.5.2. Load Balancing

5.5.2.1. Server Load Balancer — is deployed for high availability, improves performance of web applications by distributing the incoming traffic across application servers.

5.5.2.2. Link Load Balancer — is deployed to ensure high availability for internet connections utilizing dual link and distribute the traffic based on bandwidth and link availability.

5.5.2.3. Availability — all devices are in high availability (N+1 fashion), to eliminate break down of services due to hardware failure. this ensure 99.999 % access of data centre services.

5.5.2.4. Storage Backup — the data centre have SAN (Storage Area Network) of 30 TB, expandable to 50 TB with backup features, which capable to taking backup on the fly and transforming this into LTO 5 tape cartridge.

5.5.3. Power Backup

5.5.3.1. Uninterruptible Power Supply (UPS) — All devices are connected through the dual 60 KVA UPS supply for consistent and uninterrupted power supply with the help of Power Distribution Unit (PDU).

5.5.3.2. Two Digital Generator (DG) — These set are being used for power back up. DG operation is being managed by DG synchronization panel. During the power failure, the DG set starts automatically and power supply remains interact. When the power resumes the DG sets stops automatically and the system runs normally.

Figure 6: UPS

Figure 7: Power Distribution Unit (PDU)

5.5.3.3. Diesel Generator (DG) Synchronization panel: In case of power failure, DG panel starts automatically and if main power restore the DG stop automatically. DG synchronization panel controls the operation of two DG sets and synchronise the operation and based on the load one DG or both DG may work.

Figure 8: Digital Generator

Figure 9: DG Synchronized Panel

5.5.3.4. Low Tension Distribution Panel (LT) — LT panel distribute the received three phase to UPS, PAC, and other ancillary units. The LT uses circuit breakers to protect the devices from overvoltage and surges. Based on the input electrical requirement, single and three phase output is proved to devices. (UPS, works in three phase IT equipment work on single phase input).

5.5.4. Building Management System (BMS)

It is a suite of many devices and application controlled from BMS for monitoring and securing data centre premises.

5.5.4.1. Proximity Access Card — the card access control system is issued only for authorised persons only. The doors are automatically locked and unlock only with the proximity access cards. The most critical areas (such as server room and electrical room) are secured with the two level access control (biometric and card based) access.

5.5.4.2. CCTV Monitoring — A total of -09 CCTV cameras are used for surveillance of complete data centre, to prevent any unauthorized movement.

Figure 10: Access Card and Biometric System

Figure 11: PAC

5.5.4.3. Smoke and Water Leakage Detector — these detectors are used in the data centre to detect the smoke, fire and any kind of water leakage in any area of the data centre to prevent damages. The smoke detection systems known as VESDA system.

5.5.4.4. Rodent Repellent System — it works as an intelligent system, which helps in keeping the rodent away from the protected area with high frequency ultrasonic sounds, which is not audible by human being.

5.5.4.5. Fire Extinguisher — there are CO2 cylinder for fire safety and specialised FM 200 gas based fire suppression is being used for server farm area also.

5.5.4.6. Precision Air Conditioning (PAC) — N+2 PAC system of capacity of 8 tons each are being used in server farm area to maintain temperature (21 Celsius and necessary humidity (70 %) to avoid heating of equipments.

5.5.5. Physical Infrastructure

5.5.5.1. Blade centre H Chassis –

5.5.5.1.1. There are 14 server bays in a single chassis which can pack up to 112 eight-core processors into an industry-standard 9 U rack space;

5.5.5.1.2. Innovative design reduces cables by up to 80 percent compared to rack servers, helping you save on installation time and cable cost.

5.5.5.2. Server/Blade Servers (IBM H series) –

5.5.5.2.1. Unmatched flexibility to meet changing workload demands;

5.5.5.2.2. Populated with dual Quad Core Intel CPU, 16 GB Ram and 2x600 GB SATA Drive for RAID;

5.5.5.2.3. Balanced systems for virtualisation, database and enterprise workloads;

5.5.5.2.4. Provide greater performance and utilisation at lower total cost;

5.5.5.2.5. Easy-to-own, simplified power and systems management with energy –smart design and remote access.

Figure 12: Blade Chassis **Figure 13 : Servers**

5.5.5.3. Storage (IBM DS 5100) –

5.5.5.3.1. Populated with 30 TB of usable data storage expandable upto 50 TB with RAID-5 to prevent data losses form disk failure and dual controller for redundancy;

5.5.5.3.2. Provide balanced performance – up to 700,00 input/output operations per second (IOPS) well-suited for virtualization and consolidation;

5.5.5.3.3. Support high availability with hot-swappable components and non-disruptive firmware upgrades.

5.5.5.4. Back up (IBM Tivoli)–

5.5.5.5. Provides a modular, scalable tape library which capable to taking backup on the fly and transforming this into LTO 5 tape cartridge.

5.5.5.5.1. Delivers optimal data storage efficiency with high cartridge density using standard or write once, read many (WORM) Linear Tape-open (LTO) Ultrium data cartridges;

5.5.5.5.2. Doubles the compressed cartridge capacity and provides over 40 percent better performance compared to 5th generation LTO Ultrium Drives.

5.5.5.6. SAN Switch –

5.5.5.6.1. Dual switch with up to 48 ports of 8 GBPs line-rate ports in a compact one RU are installed to support multipathing and eliminate single device failure;

5.5.5.6.2. Support Redundant power supplies, fans and other availability features help minimize downtime and improves business resiliency;

5.5.5.6.3. Built-in management, operational and configuration tools, with plug-and-play features that support quick deployment and easy end-to-end SAN management;

5.5.5.7. KVM (Keyboard, Video and Mouse) Switch –

5.5.5.7.1. Enhanced capabilities of KVM over IP switches also include: a Message Board, Panel Array Mode, Mouse Dynamic Sync and Adapter ID;

5.5.5.7.2. KVM is used to access and manage the server by NOC users and administrator over LAN

5.5.6. Virtualized Infrastructure

Virtualization enables to quickly create a virtual server and custom template may be used while creating a virtual server which allow installation of software, patch upgrade, attachment of storage, network and security policies.

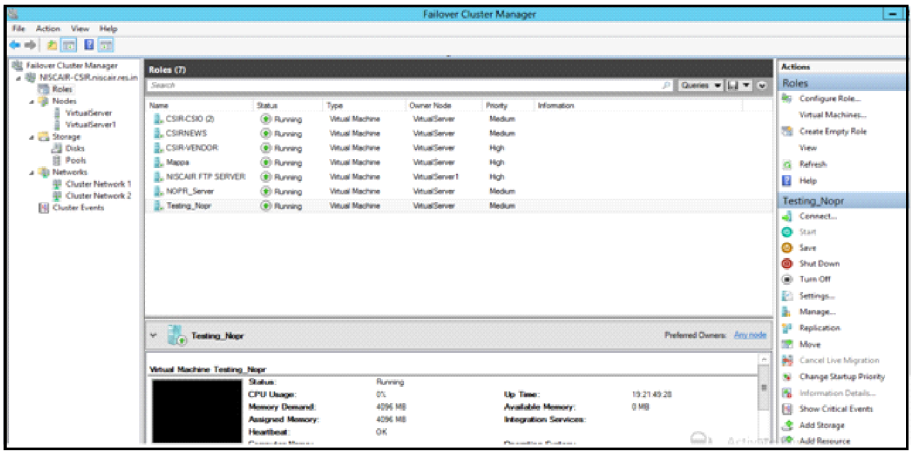

Figure 14: Hyper-V Sever Cluster for Virtualization.

Microsoft Hyper-Virtualization software is installed on Two Dell R530 Server (20 CPU Core and 32 GB ram each) for virtual infrastructure. The virtual infrastructure provides a total 40 CPU core and 64 GB RAM. The storage for data is attached form the existing IBM storage. This virtual infrastructure helped in reducing power and cooling requirement. Also, virtualization setup enables NIScPR to fast provision the services and reduced maintenance window.

5.6. Services of NIScPR Data Centre

Our team monitor applications running in data centres and the collecting link-level and network–level performance. After analyzing some issues can lead to a variety of advancements, reduce loss rates within data centres, mechanism for improved quality-of service and even techniques for consumption. The major services, those are currently managed by data centre are following:

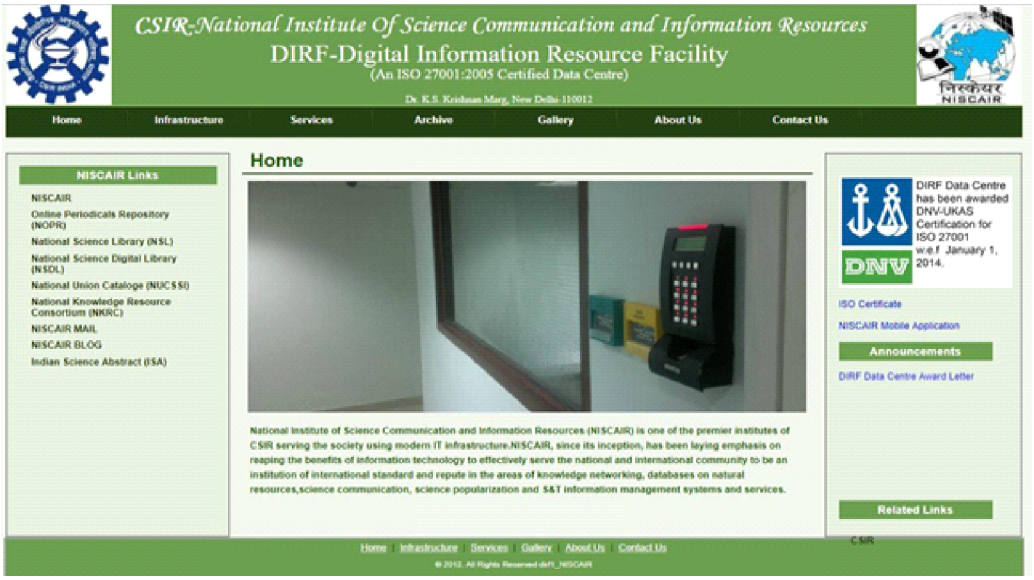

Figure 15: NIScPR data centre official website

5.6.1. CSIR-Innovation Protection Unit (IPU): this is a portal for protecting all types of intellectual property generated in CSIR that includes patents, trademarks, design and copyrights; this is hosted by NIScPR data centre.

5.6.2. CSIR-HQRS: hosting primary web-site of CSIR headquarter (new and old both) as well as CSIR vendor registration portal.

5.6.3. CSIR Finance Portal: hosting accounting software for finance & account of CSIR and its Labs.

5.6.4. CSIR-CDRI: hosting recruitment portal and disaster recovery site.

5.6.5. CSIR-CRRI: hosting primary web-site, recruitment portal and domain services of Central Road Research Institute.

5.6.6. CSIR-NPL: hosting official website and research archival data of National Physical Laboratory.

5.6.7. CSIR-CSIO: manage co-location of primary web site of Central Scientific Instruments Organisation.

5.6.8. CSIR-NIScPR: hosting primary web site, Online Publication (OP) NIScPR online publication Repository (NOPR), NKRC, ISA, NSDL, Science Reporter Portal, CSIR-News Portal, recruitment portal and other services:

5.6.8.1. NIScPR Online Periodicals Repository (NOPR): 'Online publishing @ NIScPR (OP)' has been implemented for automation of editorial process for NIScPR research journals. It is based on open source publishing software 'Open Journal Systems (OJS)' which has been customised as per NIScPR requirement.

5.6.8.2. Online Publishing (OP): This system is available at http://op.niscair.res.in for NIScPR 17 research journals, 03 magazines and 01 natural product repository. It is used basically for capturing, distributing and preserving research articles, reviews, short communications, technical reports etc.

5.6.8.3. National Knowledge Resource Consortium (NKRC): it used to provide world class e-journals, patent databases, standards, bibliographic databases and other important kind of indexes to all CSIR labs and DST (department of Science & technology) labs.

5.6.8.4. National Science Library (NSL): NSL whole website is hosted by DIRF now.

5.6.8.5. National Union Catalogue of Scientific Serials in India (NUCSSI): This is a data repository of a large number of unique journal titles and library holdings belonging to major universities, S&T institutions, R&D units of industries, higher institutes like IISc, IITs and professional institutes spread all over the country. (Total Journals: 45632, Total Holdings: 26788, Total Libraries: 572 and Total Visitors: 665870).

5.6.8.6. Indian Science Abstract Journal (ISA): ISA journal is the semi-monthly abstracting journal covered more than 4 lakh records i.e. online version of ISA journal and database management software.

6. Conclusion

NIScPR have a tier-II secured data centre with high performance servers, those are managing in centralized ICT services and information resources, which play vital role in planning the better intellectual future of large segment of researchers. Now, the digital information resource of the institute is widely accessible among the academic community at national and international level. This data centre addresses gaps and

loopholes of existing system and beneficiary for CSIR & its laboratories, in web hosting and in seamless integration of their databases and services in secured environment at present and in future also.

References

1. Amazon Elastic Compute Cloud (Amazon EC2), Available at https://aws.amazon.com/cloudcomputing/ec2(Accessed on 20/8/2022).

2. D Carr, "How Google Works," July 2006. Available at https://computer.howstuffworks.com/google-apple-cloud-computer.htm (Accessed on 20/8/2022).

3. https://www.csir.res.in/about-us/vision-and-mission

4. https://niscpr.res.in/# (erstwhile http://www.niscair.res.in/)

5. Balaji, P. Narravula, S. Vaidyanathan, K. Jin, H. W. & Pand, D. K. On the provision of prioritization and soft qos in dynamically reconfigurable shared data-centers over infiniband. Available at https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.2263&rep=rep1&type=pdf (Accessed on 20/8/2022).

6. Ramroop, S. & Pascoe, R. (1999). Implementation Architecture for a National Data Center. Proceedings of the International Conference on Interoperating Geographic Information Systems, INTEROP 99, Zurich, Switzerland, 10th-12th March, 1999. Vol. 1580 of Lecture Notes in Computer Science, (pp. 65-74), Springer. Available at https://researchr.org/publication/RamroopP99 (Accessed on 20/8/2022).

7. Wen-Syan, L. Candan, K. S. & Huan, W. K. (2004). Acceleration and Monitoring of Data Center-hosted Distributed Database-driven Web Applications, Concurrent Engineering: Research and Applications, vol. 12 (3). (pp. 205-220). Available at https://journals.sagepub.com/doi/10.1177/1063293X04046190 (Accessed on 20/8/2022).

8. Curtis, A. R. Carpenter, T. Elsheikh, M. Lopez-Ortiz, A. & Keshav, S. (2012). Rewire: an optimization-based framework for unstructured data center network design. Proceedings of the IEEE INFOCOM. 2012. (pp. 1116-1124). DOI:10.1109/INFCOM.2012.6195470. Available at https://www.semanticscholar.org/paper/REWIRE%3A-An-optimization-based-framework-for-data-Curtis-Carpenter/d3ffe3303a3735bb34b18cd2b8e771d6d8ee908d (Accessed on 20/8/2022).

9. Bari, M. F, [et. al]. (2013). Data Center Network Virtualization: A Survey, IEEE Communications Surveys & Tutorials, Vol. 15 (2) (pp. 909-928). DOI:10.1109/SURV.2012.090512.00043. Available at https://ieeexplore.ieee.org/document/6308765 (Accessed on 20/8/2022).

10. Sukmana, H. T. Ichsani, Y. & Putra S. J. (2016). Implementation of Server Consolidation Method on a Data Center by using Virtualization Technique: A Case Study, Proceedings of International Conference on Informatics and Computing (ICIC). APTIKOM. Available at https://repository.uinjkt.ac.id/dspace/handle/123456789/42981 (Accessed on 20/8/2022).

11. http://www.niscair.res.in/facilities/dirf

12. https://niscpr.res.in/facilities/dirf

13. http://dirf.NIScPR.res.in/Gallery.aspx

Keywords: Digital Library Management; Digital Infrastructure; Data centre; NIScPR; CSIR; Server; Backup

About Authors

Ms. Monika Verma
Assistant Librarian
Central Sanskrit University, Ganganath Jha Campus, Prayagraj -211002 (Uttar Pradesh)
Email: monikavara48@gmail.com

Mr. Mohit Kumar Verma
Scientific Officer
Mahamana Pandit Madan Mohan Malaviya Cancer Centre (MPMMCC), Varanasi -221005 (Uttar Pradesh)
Email: ganeshamkv99@gmail.com

Mr. Pawan Kumar
Technical Officer
IT, Departmen, CSIR -National Institute of Science Communication and Policy Research (NIScPR), Dr. K. S. Krishnan Marg, New Delhi -110012
Email: pawankum.in@gmail.com