International Journal of Information Technology and Management
Vol. 20, Issue No. 1, February-2025, ISSN 2249-4510

DOI: https://doi.org/10.29070/gb9wvw60

Analysis of ICT Infrastructure of Higher Educational Institutes (HEIs) for Cost-Effective & Secured Network with the help of Simulation

Mahendrasingh G. Chauhan [1] * , Dr. Sameer P. Narkhede [2]

1. Research Scholar, School of Management Studies, Kaviyatri Bahinabai Chaudhari North Maharashtra University, Jalgaon, Maharashtra , India
mahendrasingh191@rediffmail.com ,
2. Professor & Guide, School of Management Studies, Kaviyatri Bahinabai Chaudhari North Maharashtra University, Jalgaon, Maharashtra , India

Abstract: Analyzing the ICT (Information and Communication Technology) infrastructure of higher educational institutes(HEIs) involves assessing various components that contribute to their technological capabilities. Here's a breakdown of what such an analysis might entail: Network Infrastructure: This includes evaluating the campus-wide network architecture, such as wired and wireless connectivity, bandwidth capacity, and network security measures. Assessing the reliability, speed, and coverage of the network is crucial to support the diverse needs of students, faculty, and administrative staff. Hardware Resources: Examining the hardware resources available within the institute, including servers, computers, laptops, tablets, printers, projectors, and other devices. Evaluating the age, performance, and compatibility of these devices is essential for providing a seamless technological experience. Software Systems: Learning management systems (LMS), student information systems (SIS), academic databases, collaboration tools, productivity applications, and other software systems used for academic and administrative reasons are examined. Assessing the integration, usability, and licensing of these

Keywords: Firewall, WAN, LAN, VLAN, Network Security Optical Network, VPN Switches, Network Attacks

X

INTRODUCTION

In the rapidly evolving landscape of higher education, Information and Communication Technology (ICT) infrastructure stands as the cornerstone of academic advancement and operational efficiency. Higher educational institutes worldwide are increasingly reliant on robust technological ecosystems to support teaching, learning, research, and administrative functions. The effectiveness of these institutions in delivering quality education and staying competitive in the global arena is intricately linked to the strength and adaptability of their ICT infrastructure.

The purpose of this paper is to conduct a comprehensive analysis of the ICT infrastructure within higher educational institutes. By delving into various facets of ICT, ranging from network architecture to future-readiness, this analysis seeks to shed light on the strengths, weaknesses, opportunities, and threats present in the technological landscape of these institutions. Through this exploration, we aim to provide valuable insights for policymakers, administrators, and IT professionals to strategically enhance their ICT infrastructure and bridge technological gaps for academic excellence.

The significance of ICT infrastructure in higher education cannot be overstated. In today's digital age,

students, faculty, and administrative staff rely on technology for a myriad of tasks, including accessing course materials, conducting research, collaborating on projects, and managing administrative workflows. A robust network infrastructure is essential to ensure seamless connectivity and access to online resources, regardless of the physical location of users. Furthermore, the integration of e-learning platforms, virtual classrooms, and multimedia resources has revolutionized the teaching and learning experience, enabling institutions to offer flexible and engaging educational opportunities.

However, alongside the opportunities afforded by ICT, there exist challenges and complexities that must be navigated. Issues such as data security, privacy concerns, digital divide, and technological obsolescence pose significant hurdles to the effective utilization of ICT infrastructure. Moreover, the rapid pace of technological innovation necessitates constant vigilance and adaptability to ensure that institutes remain at the forefront of technological advancements.

BACKGROUND

The landscape of higher education has been significantly transformed by advancements in Information and Communication Technology (ICT) over the past few decades. From traditional lecture halls to virtual classrooms, from physical libraries to online repositories, ICT has revolutionized the way knowledge is disseminated, accessed, and shared within academic communities. In this context, the analysis of ICT infrastructure within higher educational institutes emerges as a critical endeavor aimed at optimizing technological resources to support the diverse needs of stakeholders and enhance the overall educational experience.

The proliferation of digital technologies has led to a paradigm shift in teaching, learning, and administrative practices across higher educational institutes worldwide. Lectures are increasingly delivered through multimedia presentations and live-streamed sessions, enabling greater engagement and interaction among students and faculty. Learning Management Systems (LMS) have become ubiquitous, providing a centralized platform for course materials, assignments, discussions, and assessments. Moreover, collaborative tools and communication platforms facilitate seamless interaction and teamwork among geographically dispersed students and faculty members.

The importance of robust ICT infrastructure in higher education extends beyond the realm of pedagogy to encompass administrative functions and institutional operations. Student enrollment, course registration, grading, and financial transactions are now predominantly managed through digital platforms, streamlining administrative workflows and enhancing efficiency. Moreover, research activities heavily rely on ICT infrastructure for data collection, analysis, and dissemination, enabling scholars to collaborate across disciplines and geographical boundaries.

However, while ICT has undeniably revolutionized higher education, it has also brought forth a myriad of challenges and complexities. Issues such as digital divide, cybersecurity threats, technological obsolescence, and data privacy concerns pose significant hurdles to the effective utilization of ICT infrastructure. Moreover, the rapid pace of technological innovation necessitates continuous investment in upgrading infrastructure, training personnel, and adapting policies to keep pace with evolving trends and emerging technologies.

Against this backdrop, the analysis of ICT infrastructure in higher educational institutes assumes paramount importance. By systematically evaluating network architecture, hardware resources, software systems, data management practices, support services, budget allocations, accessibility measures, and readiness for future technologies, institutes can identify strengths, weaknesses, opportunities, and threats within their technological ecosystem. Such insights inform strategic decision-making and resource allocation aimed at optimizing ICT infrastructure to meet the evolving needs of stakeholders and foster academic excellence.

In summary, the analysis of ICT infrastructure within higher educational institutes represents a crucial endeavor in the quest to harness the transformative potential of technology for educational advancement. By addressing the opportunities and challenges inherent in ICT adoption, institutes can cultivate a technologically empowered environment conducive to learning, innovation, and excellence in the 21st century.

Analyzing the ICT infrastructure of higher educational institutes can reveal several drawbacks or challenges that institutions may face. Here are some common drawbacks:

1. Digital Divide: One of the most significant drawbacks is the exacerbation of the digital divide. Students from low-income families may not have access to computers or fast internet, even though information and communication technology infrastructure has great promise for improving educational possibilities. This has the potential to worsen inequality in educational opportunities and resources, and to increase existing gaps in educational achievement.

2. Cyber security Risks: With the increasing reliance on digital platforms for academic and administrative purposes, higher educational institutes face heightened cybersecurity risks. Information such as student records, research data, and financial transactions are particularly vulnerable to data breaches, hacking attempts, malware assaults, and phishing scams, all of which compromise the availability, confidentiality, and integrity of the data. Inadequate cybersecurity measures can compromise institutional reputation, financial stability, and stakeholder trust.

3. Technological Obsolescence: ICT infrastructure is subject to rapid technological advancements and obsolescence. Hardware and software systems may become outdated or incompatible with emerging technologies, leading to inefficiencies, compatibility issues, and increased maintenance costs. Institutes must invest in regular upgrades and technology refresh cycles to ensure that their ICT infrastructure remains current and effective in meeting evolving needs.

4. User Resistance and Skill Gaps: The successful adoption and utilization of ICT infrastructure depend heavily on the digital literacy and willingness of users, including students, faculty, and administrative staff. Resistance to change, lack of training, and insufficient support resources can impede the effective utilization of technology, leading to underutilization of ICT infrastructure and suboptimal outcomes. Institutes must prioritize digital skills training and user support initiatives to empower stakeholders to leverage technology effectively.

5. Budgetary Constraints: Implementing and maintaining robust ICT infrastructure requires substantial financial investments in hardware, software, network infrastructure, cybersecurity measures, and personnel. However, many higher educational institutes face budgetary constraints and competing priorities, which

may limit their ability to allocate sufficient resources to ICT initiatives. Striking a balance between fiscal responsibility and strategic investments in ICT infrastructure is essential to maximize the return on investment and achieve long-term sustainability.

6. Accessibility Challenges: Ensuring equitable access to ICT infrastructure for individuals with disabilities presents significant challenges. Digital platforms, software applications, and online resources must adhere to accessibility standards and guidelines to accommodate diverse needs and ensure inclusivity. Failure to address accessibility challenges can hinder the participation and academic success of students with disabilities, violating principles of equal opportunity and social justice.

Addressing these drawbacks requires a multifaceted approach involving policy reforms, strategic investments, capacity-building initiatives, and stakeholder engagement. In order to promote inclusion, creativity, and quality while improving teaching, learning, research, and administrative operations, higher educational establishments must proactively tackle these difficulties and use the transformational potential of ICT infrastructure.

Here's a summary of the types of network attacks mentioned:

1. Passive Attack: Involves monitoring of communications without altering them, aiming to gather information covertly.

2. Active Attack: Involves actively altering or disrupting network traffic, potentially causing damage or unauthorized access.

3. Distributed Attack: Utilizes multiple compromised systems to launch a coordinated attack, often overwhelming the target network.

4. Insider Attack: Conducted by individuals within the organization, exploiting their access privileges for malicious purposes.

5. Close-in Attack: This occurs when an attacker gains physical proximity to the target network or device to exploit vulnerabilities.

6. Phishing Attack: Includes deceitful endeavors to acquire confidential information (such as login credentials or bank account details) by impersonating a reliable source.

7. Hijack Attack: Seizes control of an ongoing network session, allowing the attacker to intercept or manipulate data.

8. Spoof Attack: Involves falsifying information to masquerade as a legitimate user or device, aiming to gain unauthorized access.

9. Buffer Overflow: Exploits a software vulnerability to overflow a buffer and execute malicious code, potentially leading to system compromise.

10. Exploit Attack: Targets specific vulnerabilities in software or systems to gain unauthorized access or cause disruption.

11. Password Attack: Involves various techniques such as brute force or dictionary attacks to guess or

obtain user passwords, allowing unauthorized access to accounts or systems.

These types of attacks represent a diverse range of tactics employed by threat agents, from individual hackers to sophisticated nation-state actors, highlighting the importance of robust security measures to defend against them.

Some network assaults, especially Denial of Service (DoS) attacks, are broken out here in the real-time data:

A) Denial of Service (DoS)

- Ø A denial of service assault may temporarily or permanently disable a service by damaging or otherwise disrupting the system.
- Ø Some examples include physically cutting off the infrastructure, running out of memory, or corrupting a computer's hard drive.
- Ø The presented information shows a live feed of data from a campus network that is protected by a Fortinet firewall.
- Ø Upon implementing Firewall and VLAN configurations to counteract DoS assaults, the following attacks were detected.

Table 1: Flood Attack

Attack Type	Source		Destination	
	Applied	Traffic	Applied	Traffic
TCP Flood	No	0	No	0
UDP Flood	Yes	4180	No	0
SYN Flood	Yes	4200	No	0
ICMP Flood	Yes	32	Yes	583

This data illustrates the types of DoS attacks detected and the effectiveness of the configured security measures in mitigating these attacks.

B) ARP Spoofing Attack:

- In ARP spoofing, fake Address Resolution Protocol (ARP) packets are sent across a local area network.
- The outcome is that a valid computer or server's IP address becomes associated with the attacker's MAC address.
- The attack takes use of the fact that the stateless ARP protocol is susceptible to manipulation due to its lack of authentication.

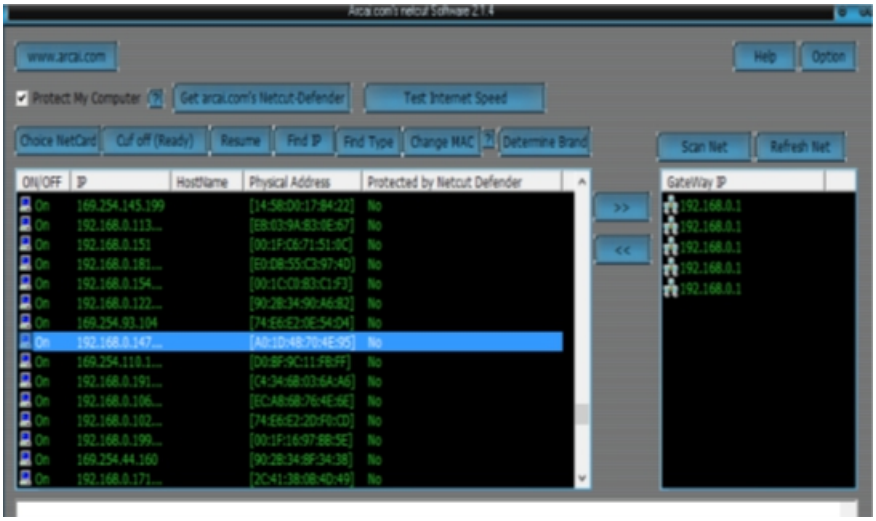

Figure 1. ARP Spoofing Attack in Campus Network

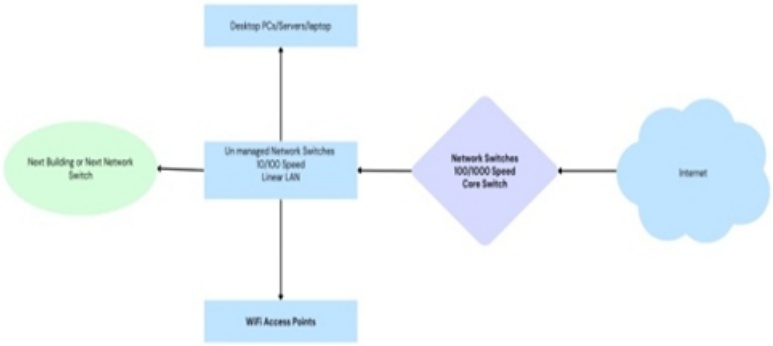

Figure 2: Traditional Campus Network Design

PROPOSED COST-EFFECTIVE CAMPUS NETWORK DESIGN

- The development of virtual local area networks (VLANs) for security reasons.
- To protect data both within and outside the campus, set up a firewall.
- Branch campus's use of virtual private networks

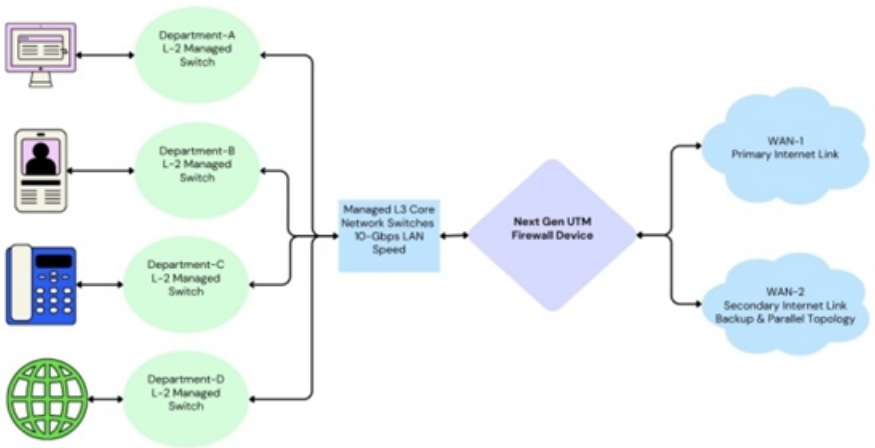

Figure 3. Cost-Effective Secure Network Design

Implementing a cost-effective and secure campus network presents various challenges, with security being the central concern. Therefore, in order to tackle these issues, we have thoroughly discussed a multitude of possible solutions and the architecture of our network. We have to deploy star topology network infrastructure for fast and seamless network connectivity and minimum failures of local network

The network must be enabled with two (ISPs) Internet Service Providers for uninterrupted internet facility for educational campus with UTM firewall device security

C. Deployment of VLANs (Virtual LANs) for Enhanced Security The widespread adoption of virtual LANs across networks of all scales underscores their effectiveness. The complexity of maintaining several cable infrastructures and switches is eliminated when a single organisation employs multiple VLANs, which function similarly to separate physical networks. By segmenting the network, VLANs create multiple broadcast domains, facilitating the isolation of traffic within these domains. This not only enhances network bandwidth and availability but also significantly bolsters security measures.

We have suggested some VLANs for better security of the campus network and reducing Broadcast.

Table 2. VLan Structure

Proposed VLAN for HEIs Campus Network		
Sr.No.	**VLAN IDs**	**VLAN Names**
1	10	Admin/Server Room
2	11	Computer Lab
3	12	Local Servers
4	13	Computers Lab
5	14	Faculty PCs
6	15	Students Device

In order to protect the campus network from outside threats, it is essential to install a firewall. To protect a private network from unauthorised access, firewalls monitor and filter all data packets entering and leaving the network. The campus network is protected by a hardware firewall, which selectively controls outward traffic and blocks unauthorised incoming traffic. Outbound traffic is prohibited on some ports due to security vulnerabilities. These ports include NetBIOS, SMTP, and others. But most of the campus's academic programmes can still run normally with this precaution in place.

D. Virtual Private Network (VPN)

The Internet is only one example of a public network that may be accessed using a Virtual Private Network

(VPN). It creates the illusion that a computer or other network-enabled device is directly connected to a private network, allowing it to send and receive data via public or shared networks. Users are able to take use of the public network's features, security, and administration rules thanks to this setup. Dedicated connections, virtual tunneling protocols, or traffic encryption are the most common methods for establishing a virtual private network (VPN). Among the most well-known VPN implementations are Open VPN and IPsec.

Connect safely and securely to the campus network even when you're not physically there with the help of the Campus VPN's all-inclusive tunneling VPN service. Using the Campus VPN is common for accessing shared files and file sharing, and for several apps that need a Campus IP address. It is worth mentioning that the Campus VPN has a session restriction of 8 hours.

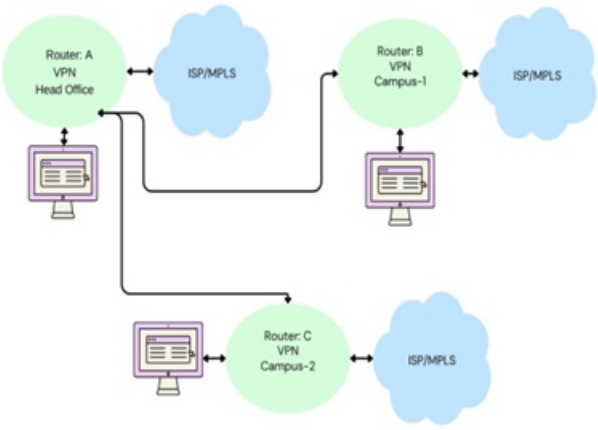

Figure 4.VPN Connectivity Diagram for Campus

Enable Kill Switch: Some VPNs offer a kill switch feature that disconnects your internet if the VPN connection drops, preventing your data from being exposed.

Use Split Tunneling: If your VPN app supports split tunneling, you can choose which apps or websites use the VPN connection and which do not.

Regularly Update the VPN App: Keep your VPN app up to date to benefit from the latest security features and improvements.

Understand the VPN's Privacy Policy: Ensure that the VPN provider does not log your activities and has a strong privacy policy.

CONCLUSION

Security measures and network design are critical to the smooth running of any Higher Educational Institutes. By adhering to a hierarchical network design, scalability, performance, and security can be significantly enhanced while also simplifying network maintenance. In our endeavor, we have put forth a streamlined, cost-effective design for a secure campus network, tailored to suit the specific work environment and accommodate the necessary scalability security, and other essential factors.

References

1. Lalita Kumari, Swapan Debbarma, Radhey Shyam, Security Problems in Campus Network and its Solutions, International Journal of Advanced Engineering & Application, Jan 2011issue

2. Mohammed Nadir Bin Ali, Mohamed Emran Hossain, Md. Masud Parvez, Design and Implementation of a Secure Campus Network International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 5, Issue 7, July 2015

3. Yuxin Cheng, Optical Interconnects for Next Generation DataCenters, Architecture Design & Resource Allocation TRITA-EECS-AVL-2019: ISBN 978-91-7873-108-4Stockholm, Sweden

4. Sheikh Raashid Javid & Sheikh Mohsin Pervez Planning a Smart Network Design in Home Networking: A Survey, International Journal of Advanced Research in Computer Science & Software Engineering 3(5), May - 2013, pp. 1308-1312

5. Bi Bi Ayesha & Dr. Shreedhar Murthy, Implementation of Network Design for Universities without IOT, International Research Journal of Engineering & Technology (IRJET) ISSN:2395-0056Volume: 09, Issue: 07, Julay-2022

6. Mr. Umeh Innocent Ikechukwu, Modeling the Design of Computer Networks for Effective Management, International Conference on Advances in Computing Control & Networking ACCN At: Bangkok, Thailand Volume: 2nd

7. Bagus Mulyawan, Campus Network Design & Implementation Using Top Down Approach a Case Study, International Conference on Information Systems for Business Competitiveness (ICISBC) 2011

8. Mohit Dixit & Lovish Raheja, ICT in HigherEducation,A review of issues, challenges & solutions with special reference to India, IITM Journal of Management & IT2020,Vol:11, Issue: 1, ISSN: 0976-8629 ISSN: 2349-9826.

9. Prof. Swati Pawar, Prof. Vivek D. Ugale Ankita Nirmal, Pallavi Badgujar, Swapnali BoradeNetwork Design for College Campus: 2020 IJRAR March 2020, Volume 7, Issue 1, ISSN 2348-1269

10. Garima Jain, Nasreen Noorani, Nisha Kiran, Sourabh Sharma, Designing &simulation of topology network using Packet Tracer, International Journal of Engineering & Technology (IRJET),2 (2) 20215

11. S. Raja Gopal, P. Sallem Akram, S Sriram, T.Pravin Kaushik, V.Mohan Krishna, Design & Analysis of Heterogeneous Hybrid topology for VLAN Configuration, International Journal of Emerging Trend in Engineering Research Vol7, No.11, PP 487-491, 2019

12. G.L.P Ashok, P. Sallem Akram, M Sai Neelima, I Nagasaikumar, A,Vamshi, Implementation of Smart Home by Packet Tracer, IEEE

13. Md. Waliullah, 'Wireless LAN Security Threats & Vulnerabilities' International Journal of Advanced Computer Science and Application, Vol. 5, 2014

14. Lalita Kumari, Swapan Debbarma, Radhey Shyam, Security Problems in Campus Network and Its Solutions, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre

15. Sanad Al Maskari, Dinesh Kumar Saini, Swati Y Raut & Lingraj A Hadimani, Security and Vulnerability Issues in University Networks Proceedings of the World Congress on Engineering 2011 Vol I WCE 2011, July 6 - 8, 2011

16. Network Security, Sulaimon Adeniji Adebayo, Bachelor's Thesis (UAS) Degree Program in Information Technology Specialization: Internet Technology

17. Kozma, R.J. (Ed). (2003), Technology innovation and educational change: a global perspective. A report of the Second Information Technology in Education Study (SITES)

18. M. Wasif Nisar, Ehsan Ullah Munir and Shafqat Ali shad, (2011), Usage and Impact of ICT in Education Sector; A Study of Pakistan, Australian Journal of Basic and Applied Sciences, 5(12): 578-583, 2011 ISSN 1991-8178

19. Meenakshim M, Importance of ICT in Education, OSR Journal of Research & Method in Education (IOSR-JRME) e-ISSN: 2320–7388,p-ISSN: 2320–737X Volume 1, Issue 4(May. –Jun. 2013), PP 03-08

20. Samuel Mofoluwa Ajibade, Technological Acceptance Model for Social Media Networking in e-Learning in Higher Educational Institutes, International Journal of Information and Education Technology, vol.13, no.2, pp.239-246, 2023 (Scopus)