Planned Future Internet Infrastructure: A Plot Model for Higher Education Institution

Adnan Ahmed[1] Syed Asif Ali[2] Basit Hassan[3]

Abstract

Nowadays Higher Education Institutions (HEI) are very dependent on their networks because of communication development, and for achieving this objective a proper infrastructure is required. Security is the main and progressive condition to maintain and update information of any Higher Education Institution. This research work proposes Future Internet Infrastructure (FII) and related security issues. This research is conducted on a public-sector university of Karachi, Pakistan. The main purpose of taking the example of Education Institution is that in an education environment usually, multi-discipline users and this is an observed practice that the users in HEI increase gradually. Therefore, the flow of data is increased in term of their users. A proper internet infrastructure is required to maintain all data with a security concern. The university which is the part of our case study is an multi-campus institution. Its network works on technical concepts such as, planning and designing of network infrastructure which control whole network infrastructure, Cloud, Social Media safety policy, risk analysis for network security, network security policy on advanced networking concepts. The existing system in university has some challenges in overall IT structure. The overall infrastructure needs advanced concept and physical facilities (authorization of the transaction, user authentication, encryption of data, planning of backup policies, disaster recovery plan and physical security strategies with application security policy, emails and website security, etc.).

KEYWORDs: Higher Education Institutions (HEI), Network Security Policy (NSP), Future Internet Infrastructure (FII), Internet Infrastructure Security (IIS) and Planned Future Internet Infrastructure (PFII).

1 Introduction

Many IT infrastructure-related securities belong with new and advanced threats and very risky for the whole organization. It can damage the entire network of an organization and can fail the overall working of the network system. The network has been changed from simple LAN, MAN, WAN to wireless LAN, Wireless MAN, Wireless WAN. The latest Computer Crime and Security Survey of the Computer Security Institute (CSI) [1] report that 49% of the respondents faced IT security incidents due to the actions of legitimate users.

Wireless networks have been in widespread used since few years [2]. Smartphones and handheld technologies are being used instead of desktops. Demand for wireless services are increasing

[1] Sindh Madressatul Islam University, Karachi, Sindh Pakistan adnan.ansari@yahoo.com
[2] Sindh Madressatul Islam University, Karachi, Sindh Pakistan asifkhi@hotmail.com
[3] Sindh Madressatul Islam University, Karachi, Sindh Pakistan basithq@yahoo.com

rapidly as evident by the tremendous growth in recent years in smart mobile phones [3], for instance, smartphones have changed the way of doing the job. Users prefer to connect via smartphones using 3G, 4G technologies or wireless networks. The usage of social networking has also raised and cloud computing has changed networking. In the last decade, many online social networks, such as Facebook, Twitter, and LinkedIn, have emerged and connected web users all over the world [4]. Schools and universities are taking benefit of the recent development in Information and Communication Technology (ICT) embracing Online Learning Resources (OLR) as an integral part of teaching and learning activities [5].

As this research focuses on Higher Education Institution, the number of students increase each semester wise, which are bulk users of the higher educational institute. They interact with other students and staff through digital social media network. As per the record, 25 million users are registered from Pakistan and out 25 million 19% are belonged to Karachi [6]. Due to the implementation of 3G in all over the world, the usage of *YouTube* has also increased but the security privilege is the lesser on social networks [7].

2 Research Background

Developments in information technology infrastructure during the past decades have exact to logical changes in the modern society. For instance, organizations are adopting several new technologies, deploying their own devices at work, use of social networking, and use of wireless based networking environment [8]. It opened many complications; however, cybercrimes turn into organized and broadly equipped, resulted in battle amongst hackers and security administrators. Hackers are trying to break the network security, attacking IT infrastructure through browsers and add-on software [9]. It's opening to sort IT infrastructure secure and protected through Cabinet Servers, deployment of policies, rules, and firewalls. IT infrastructure must be innovative. Controlling of user's activities, virtualization of servers, DNS server protection and recovery of data [10].

This case study provides a raised area through planned future internet infrastructure for Higher Education Institutions (HEI) and its security which provides a secure and protected atmosphere in HEI to gain access information about the past, present, and future from social media via cyber world.

3 Existing Internet Infrastructure

The existing network infrastructure of HEI is insecure due to traffic congestion and excessive nodes. As existing infrastructure not fulfilling the demands of users and protocols which are used to protect the entire network. Additionally, the use of smartphones, laptops, wireless access points, torrents with social media connections is also responsible for creating an insecure environment.

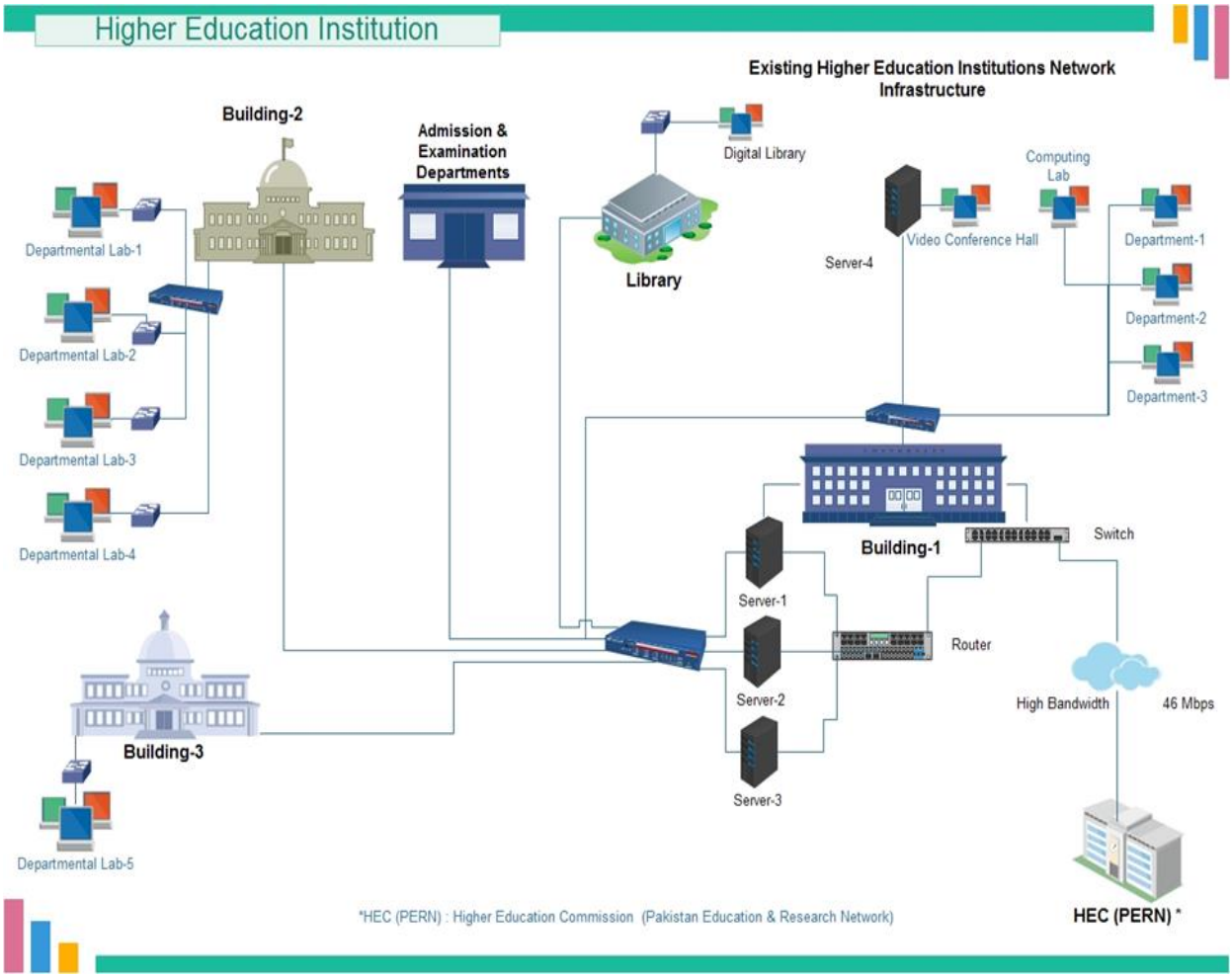


Figure 1 shows the existing network Infrastructure. In the institution, presently there are around 750 to 800 users. The employees have permission to access multiple emails, downloading, uploading, webmail, web sites and file sharing.

Rapid growth has been started towards online tutorials, E-learning, Learning Management Systems (LMS) and Microsoft's Dream Spark's portal which is provided by Higher Education Commission of Pakistan for students.

Following are the reasons which pose sort of risks causing unsecure network infrastructure in existing system.

a. Use of obsolete technology.
b. Weak network policies.
c. Unauthenticated access of user e.g. (passed out students) in the network.
d. Wrong network configuration by the network administrator and grant permission to users without standard policies.
e. Use of unauthorized and unlicensed software, which allows hidden viruses and hackers.
f. The weak configuration of TCP/IP.

Highlighted reasons are permission easy access to hackers, who can destroy the privacy.

4 Planned Future Internet Infrastructure

The planned future internet infrastructure shows in figure 2, which divides the entire network into different security zones with security devices to protect network infrastructure from internal and external attacks and threats. For this purpose, planned Demilitarized Zone (DMZ) in the entire network of the higher education institution and it will separate the network into three different zones such as,

The planned future internet infrastructure shows in figure 2, which divides the entire network into different security zones with security devices to protect network infrastructure from internal and external attacks and threats. For this purpose, planned Demilitarized Zone (DMZ) in the entire network of the higher education institution and it will separate the network into three different zones such as:

a. External DMZ
b. Internal DMZ
c. DMZ Server Zone

Proposed future internet infrastructure depends on multiple networks and servers. First, install the configured firewalls for securing and protect all zones. This will block the threat from application-based attacks and outsider's attacks from the internet.

Planned future internet infrastructure will decrease the flow of traffic from internal network zone to DMZ. The users cannot communicate directly with others system in the internal and external DMZ because of firewalls securities. Two Firewalls are proposed in the (FII) for security zones to control, and threat management.

a. External DMZ

   Proposed external DMZ in the future internet infrastructure is to restrict public access to the education institution's network and to restrict HEI's employee's access to the internet.

   The external public users authorized to get access HEI's mail server and web server only but not authorized to access other services. Therefore, the firewall provides the secure platform to allow access the HTTP and HTTPS services and to email services. The firewall allows seeing only the addresses of the web server and emailing server on the internet.

   The external firewall implemented in future internet infrastructure for work based on proxies. It will create the scenario that, when any email communication being started, the email (SMTP) receives the mail and scans it for viruses and threats. If email is clear and not found any specious then forward it to the Mail server in the DMZ. Same as a web access connection builds, firewall scan the access request for specious elements (such as evidence of the threats and attacks). If it is clear and protected, then forward to the Web server into the DMZ. Both Web and Mail server in the DMZ should have different proxies.

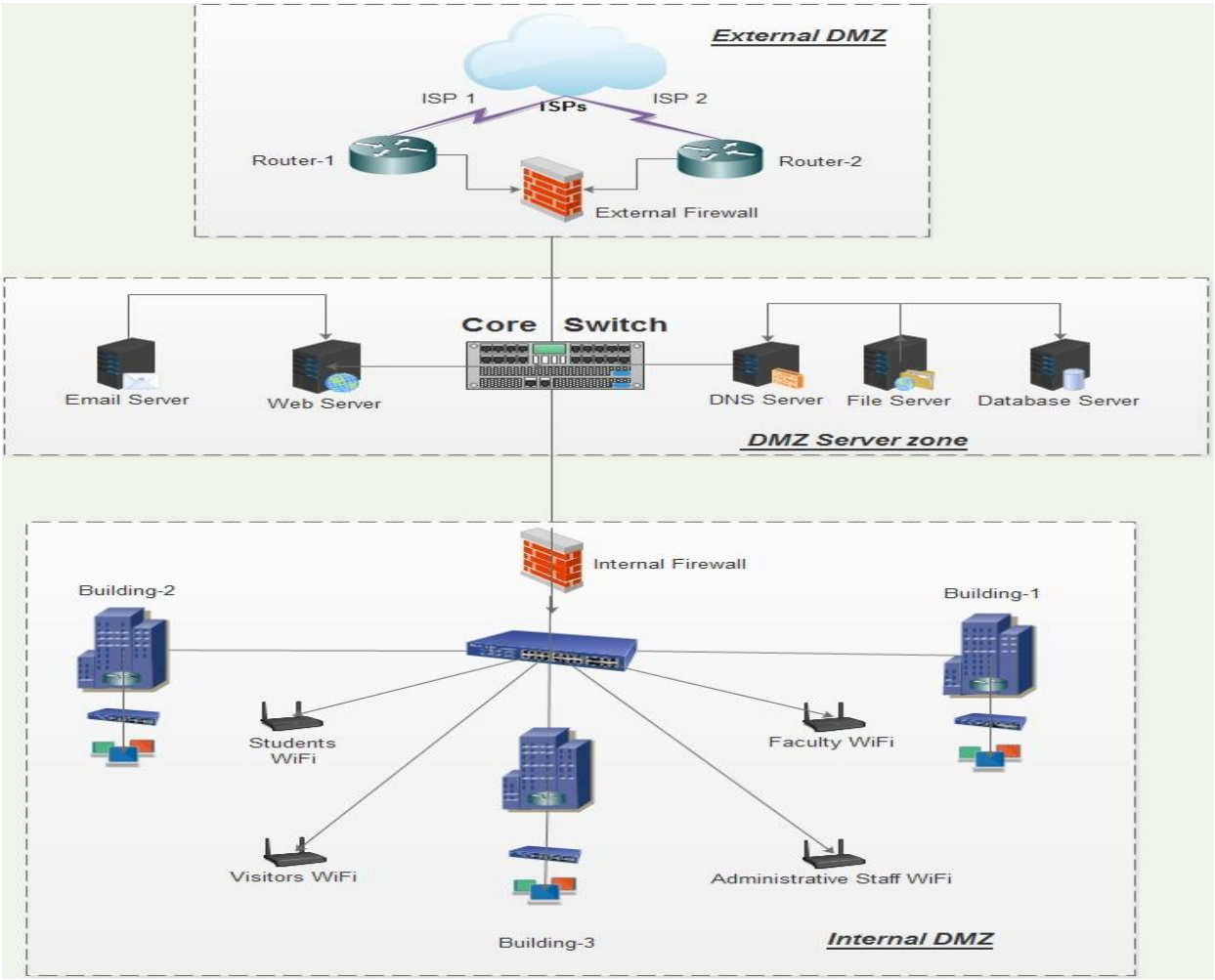


Figure 2 Proposed Future Internet Infrastructure of Higher Education Institution

b. Internal DMZ

The recommendation of the internal DMZ in (FII) is the protection and the security of sensitive data and information from outsiders. The internal firewall will only allow the authorized users to access and block all other connection through the direct internet.

The education institution uses file sharing system to share the data among its network. In file sharing system sends and received the data files in the network and these packets carrying sensitive data to leak out to the public internet. For blocking leakage of sensitive data and information to the internet, proposed internal firewall for all over protection and the security policy with DMZ server zone.

Internal firewall will control all the traffic of entire zone network and following;

- It will permit SMTP by using proxies and emails are sent to the mail server in the DMZ.

- It will permit secured communication services to the DNS server in the DMZ server zone.
- It will permit system administrators to get access servers in the DMZ server zone for the management of all servers.
- It will disallow all the connections except authorized users to the DMZ server zone.
- It will block building wise collision and data leakage.
- It will block all the restricted websites in the EI's computing labs.

c. DMZ server zone

i. E-mail Server in DMZ server Zone
ii. Web Server in DMZ server Zone
iii. DNS Server in DMZ server Zone
iv. File Server in DMZ server Zone
v. Database server in DMZ server Zone

i. E-Mail Server

In the proposed (FII) DMZ server zone, mail server will operate email addresses and content checking on all emails. The main purpose of mail server DMZ server zone is to protect and secure internal information from external users in the internet. As any email, will be receive from the internet, mail server will check and scan then will forward the information to the destination and same procedure will perform for outgoing emails to the internet.

ii. Web Server

Web server will handle the requests and services from the internet. Web server will not communicate any sources within the internal DMZ and it will not contain any confidential data. If any specious activity will begin from internet by hackers, it will block the process and the internal network will be secured. The web server will consider itself as "www.hei.edu.pk" and will use the IP address of the external firewall security zone and it will hide the configuration of DMZ server zone.

iii. DNS Server

DNS server will hold directory name services and all the related information which are required for controlling and managing are as,

- DMZ mail server, web server
- External firewall
- Internal firewall
- Internal authorized administrative users

Policies for entire network will be manage and control with the domain names.

iv. File Server

In the proposed (FII) DMZ server zone, file server will perform its duties as file sharing in the internal network with assign rights to authorized users. It will provide a centralized storing place and sharing of files and folders. Internal staff and authorized administrators will be able to access the file server for sharing files.

It will also provide a centralized zone to handle file and folder storage and access only by internal users in the DMZ network. It will use word processing information and personal data too.

v. Database Server

In the proposed (FII) DMZ server zone, database server will handle the client/server background resources for shared software, online application, campus management system (CMS) (which is designed for higher education institution), web server backup and learning management system (LMS). It will be safe and secure against internal attackers but authorized user can access services.

5 Comparison Between Existing Infrastructure and Proposed Future Internet Infrastructure

Comparison of both infrastructures is shown in table 1.

6 Verification of Proposed Future Internet Infrastructure in Various Organizations

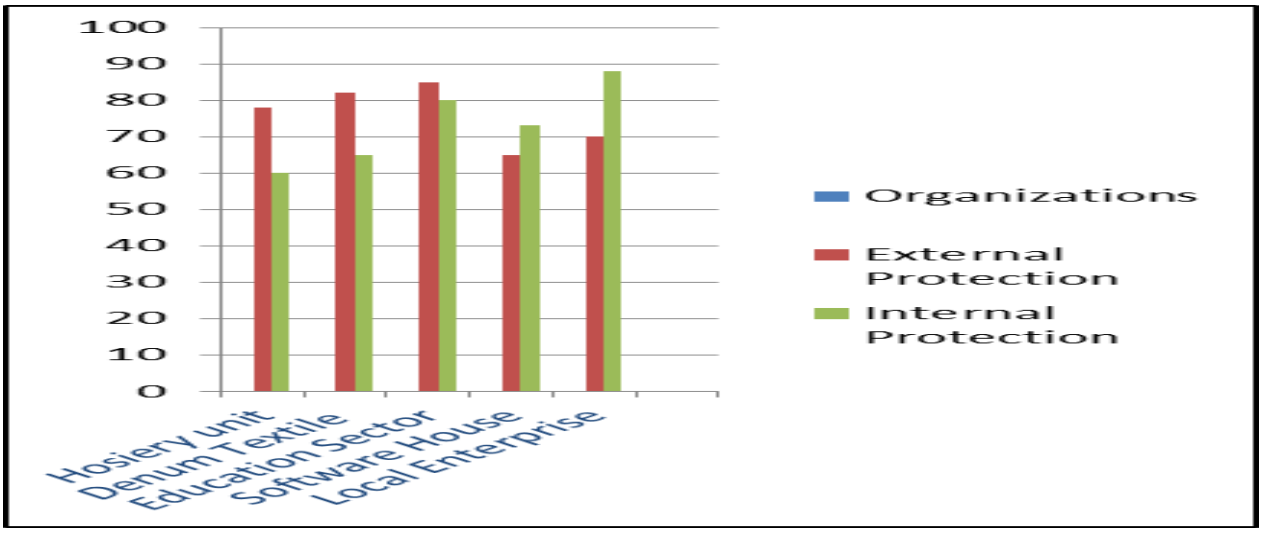
Same case study has been implemented in different organization result are as below;

Full secured from lack of information, protection against external attacks from internet. Improved design for network transactions and reliability of data sharing, with secured from viruses and Trojans, alternative ISP's for backup, if one's link down then switched to alternative link to network continuity. Highly protect to blockage for hackers and vulnerable services. 24 hours a day and 7 days a week full network monitoring of internal network users. Automatic backup procedure for store files server and server's data.

Organizations are successfully running their network with test deployment of proposed future internet infrastructure. Some of them had needed to protect their internal network and some had to both external and internal network.

Table 1 Comparison between existing and proposed future internet infrastructure

Existing Internet Infrastructure	Proposed Future Internet Infrastructure
Less secured and open network to get into without blockage.	Completely secured with authentication and verification of users.
External user can easily get access into internal confidential data.	Divided and separated security zones in three partition and external user cannot pass and break internal security zone and server DMZ.
Files and data sharing leakage issue on internet.	Files and confidential data protection without leakage.
Possibility of outside attacks and accidentally leakage of information.	This reduces the possibility of outside attackers accidentally identifying information assets through standard port attacks.
Low security level of local area networking.	All components are maintained through a complete management and monitoring system implemented in a protected management LAN.
No prevention system of intrusion detection.	Intrusion detection and prevention systems.



Graph 1 Security improvement level of various organizations

7 Result

The main purpose of DMZ is to separate the entire network of an educational institution into three Zones to improve security. Implementation of policies and rules into entire network to protect inbound and outbound attacks and threats.

Managing future internet infrastructure, educational institution must implement some services and internal network could not be accessible and kept in a secure internal DMZ which isn't accessible from the external DMZ.

The new infrastructure design is implemented, which safely is being done by using a DMZ. Used DMZ to create different network zones, where only specific traffic can pass through firewalls and threats security scan and intrusion prevention mechanism. HEI must upgrade the network infrastructure in advance and with high security. Properly manageable and secured a DMZ network infrastructure from external as well as internal attacks.

8 Conclusion

The main objective of this paper was to provide an explicit analysis of security challenges of the of HEI's network infrastructure, in order to understand what is its place in the Future Internet. There is strongly need the update network infrastructure, the changes accurse at the basis of technology. This is necessary for moving with global needs. In this paper different security aspect in like internal network security, external network security, Demilitarization of networks are proposed. All these securities should be properly implemented in the HEI's network infrastructure. Planned future internet infrastructure will decrease risks of threats and attacks.

References

[1] Power, R. (2001), '2001 CSI/FBI Computer Crime and Security Survey', Volume VII — No.1, Computer.

[2] Jabeen, Q., Khan, F., Khan, S., & Jan, M. A. (2016). Performance improvement in multihop wireless mobile adhoc networks. The Journal Applied, Environmental, and Biological Sciences (JAEBS), 6, 82-92.

[3] Verma, D. (2016). *U.S. Patent No. 9,531,556*. Washington, DC: U.S. Patent and Trademark Office.

[4] Peng, S., Wang, G., & Xie, D. (2017). Social influence analysis in social networking big data: opportunities and challenges. *IEEE Network*, *31*(1), 11-17.

[5] Anshari, M., Alas, Y., & Guan, L. S. (2016). Developing online learning resources: Big data, social networks, and cloud computing to support pervasive knowledge. *Education and Information Technologies*, *21*(6), 1663-1677.

[6] "Pakistan Facebook Users Crosses The Landmark Of 25 Million Users". Umair Qureshi | Digital Marketing Specialist | Blogs about Digital Analytics, SEO & Social Media. N.p., 14 May. 2016.

[7] "Youtube Traffic From Pakistan Is Picking Up As The Ban Enters Its Fourth Year!" Propakistani.pk./2015/09/21.

[8] Niebert, N., Schieder, A., Abramowicz, H., Malmgren, G., Sachs, J., Horn, U., & Karl, H. (2004). Ambient networks: an architecture for communication networks beyond 3G. *IEEE Wireless Communications*, *11*(2), 14-22.

[9] Leavitt, N. (2011). Internet security under attack: The undermining of digital certificates. *Computer*, *44*(12), 17-20.

[10] Buecker, A., Browne, K., Foss, L., Jacobs, J., Jeremic, V., Lorenz, C., & Van Herzele, J. (2011). *IBM security solutions architecture for network, server and endpoint*. IBM Redbooks.