Threat Minimization by Design and Deployment of Secured Networking Model

Shamimul Islam[1], Haidar Ali[1], Ahsan Habib[1], Nur Nobi[1], Mahbub Alam[2], Dulal Hossain[1]
(Corresponding author: Shamimul Islam)

Institute of Computer Science, Bangladesh Atomic Energy Commission, Bangladesh[1]
E-12/A, Paramanu Bhaban, Shahid Shahabuddin Shorok, Agargaon, Dhaka 1207, Bangladesh
(Email: shamimul321@yahoo.com)
Institute of Electronics, Bangladesh Atomic Energy Commission, Bangladesh[2]
(Received Mar. 18, 2018; revised and accepted Apr. 22, 2018)

Abstract

Security is an important issue for organizational network design and development. With an increasing technology in cloud computing sector, enterprise Sector and specific organizational network Infrastructure development, network security always has remained as a great challenge. Our considerable Organization like different scientific/institutional institution faces core security issues challenges in network architecture design and development. A Secured infrastructure of a network always considers or concerns about different security attacks. Network security will prevent a organization network infrastructure from different types of attacks and threats. This paper intends to give an idea to design and deployment of a simple but better network security model and cost effective approach using routers and firewall. This research aim is also that how a network will be protected against vulnerabilities, configuration and security policy weaknesses. Our proposed network infrastructure is adaptable with secure structure.

Keywords: Firewall; Threats and Attacks; VLAN; VPN

1 Introduction

Increasing and overgrowing of networking volumes and internet, the network and information related threats has been risen significantly. These threats are exercised attacks causing damage of a network infrastructure and committing different types of criminal network or cyber activities. Now a days Internet and networking plays a important role in personal, enterprise, organization and different government application. So using network based application and services, Network Security is a major concern [1]. When we concerns about network security terms it includes authorization, identification, authentication and surveillance to the protection of computer hardware or network physical equipment and all other virtual and sophisticated things related with network infrastructure. Threats may arise from mis-configuration of hardware or software equipment, poor network design and deployment, technology weaknesses, or carelessness of end-user [3]. There is no specific laid-down procedure for secure network design and deployment. So Network security must be considered for designing and fit the needs of an organization especially for scientific/institutional organization.

An important secured network deployment and design consideration for today's networks is creating the potential to enhancement for future expansion in a scalable, reliable, and secure way [4]. This

paper focuses on the simple but hierarchical network design in which the proposed system will be scalable; better performance and security will be ensured and easy to maintain [7]. It also focuses on review of different types of attacks on routers, switch and its prevention and mitigation procedure. As Routers and firewall are crucial parts of network operations and network security, careful management of router and firewall operations and by avoiding of redundant installation of software and hardware equipments can reduce network downtime, prevent attacks, and proceed in helping in the analysis of security breaches [8].

2 Literature Review: Network Security, Attacks, Weakness and Threats

As the networks of today are more open and with the increased number of LAN, WLAN and personal computers, Wi-Fi and the Internet are beyond a huge numbers of security risks. Network security a important component in information security because it is responsible for securing all information passed through networked computers [2].

For the protection for hardware, software, and information within a network with a acceptable level administrative and management policy, access controls, hardware and software specific functions, features and operational procedures are required. Network security ensures three fundamental aspects: integrity, confidentiality, availability of information from top to bottom.

Real-world security includes prevention, detection, and response. As no prevention mechanism is perfect. Detection and response are more effective than prevention. We need to address protection different OSI layer protection for a secured networking.

Multilayer firewall is need for different level network security in network OSI layer protection [10]. When we considering or imagine a total secured network architecture then we need to consider the overall security in every layer of a network architecture. The protection in every layer provides a secured system where the end user are satisfied and secured within the network. So before designing a network we must be introduced with every layered function for ensuring a robust security firewall against total architecture (See Table 1).

Table 1: Multilayer activities

OSI Layer	Areas
Application Layer	- OS and Application level threats - Application-level gateway
Presentation	encryption
Session	Socks Proxy server
Transport	- Packet filtering -TCP/UDP Flooding.
Network	-NAT/PAT -IP Alternation and DHCP attacks
Data link & Physical	MAC Address alternation, physical port, Traffic Flow changing *etc.*

Firewall security provides centralization, Identify weak points in security system so it can be strengthened, identify intruders so they can be apprehended, provide for authentication, and contribute to a VPN. In Transport layer packet filtering firewalls scan network data packets looking for compliance

with, or violation of, rules of firewall's database. Restrictions most commonly implemented in packet filtering firewalls are based on IP source and destination address, Direction (bound and unbound) and TCP or UDP source and destination port [6] network-level proxy; convert IP addresses of internal hosts to IP address assigned by firewall. NAT uses pool of valid external IP addresses, assigning one of these actual addresses to each internal computer requesting an outside connection. Application gateway Frequently installed on a dedicated computer and known as application-level firewall, proxy server, or application firewall. It also can control applications inside a network that access the outside world by setting up proxy services. This security techniques covers: 1) IP address mapping; 2) URL filtering; 3) Content filtering.

Security Weakness and Threats Issues in Network:

In network security every network and device consists of its weak points which are inherently described as its weakness. The weakness can be categorized into 3 ways:

1) Technological Weaknesses: Protocol related weaknesses like TCP/IP protocol, network equipment and Operating System weaknesses.
2) Configuration Weaknesses: it concerns with correctly configuration of computing and network devices. Some configuration weakness is: unsecured user accounts which deals with transmission of insecure user account information over network. System accounts with easily guessed passwords. Misconfigured internet devices such as turn on JavaScript on web browser, Misconfigured network equipment can cause a large security hole.
3) Security Policy Weaknesses: It can create unforeseen security threats. It may consists of points like lack of written security policy, logic access control not applied, software and hardware installation and changes which do not follow the proper policy and lack of disaster recovery plan existence [9].

Network Security:

It faces potential threats generally. The threats may include: 1) Passive attack; 2) Active attack; 3) Distributed attack; 4) Insider attack; 5) Close in attack; 6) Phishing attack; 7) Hijack attack; 8) Spoofing attack; 9) Buffer overflow; 10) Exploit attack; 11) Password attack; 12) Session hijacking attacks; 13) TCP SYN attack; 14) Smurf attacks; 15) Routing attacks; and 16) Masquerade attacks, *etc.* Explanations of some attacks are given here:

1) Denial of Services(DoS): DoS often attacks the specific target by traffic flooding. An attacker tries to prevent actual users from accessing information or services. Flood attacks occur by receiving too much traffic and it cause the server to buffer, causing them to slow down and stop. In this attack, the specified server does not know from which actual port the request are sending. Attacker overloads the server with requests. Buffer overflow attacks, ICMP flood, SYN flood are popular DoS attack. Again DDoS(Distributed Denial of Services) attack occurs when multiple systems target a synchronized DoS attack to a single target. Figure 1 shows a general server connected with specific address with different IP address.

   Figure 2 shows after DoS attack server for IP flooding.
2) ARP Spoofing Attacks (See Figure 3): This kind of attack occurs over a Local Area Network (LAN). Generally ARP Protocol translates IP addresses into MAC addresses. This attack occurs when malicious ARP packets are sent to a default gateway on a LAN to change the pairings in its IP to MAC address table. ARP Poisoning attacks are easy to carry out as the attacker has the control of a machine within the target LAN or is directly connected to it [5].

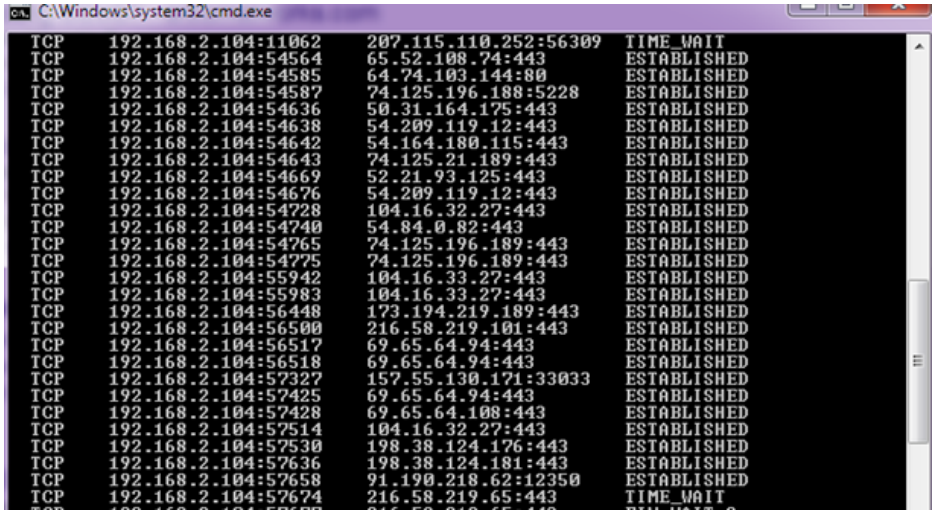

Figure 1: A general server connected with specific address with different IP address

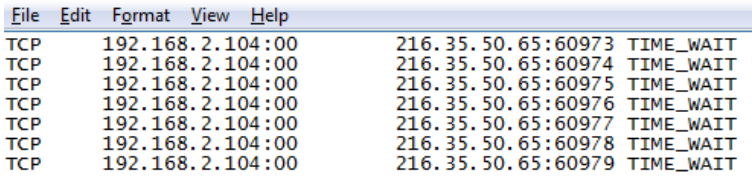

Figure 2: After attack of DoS for IP flooding

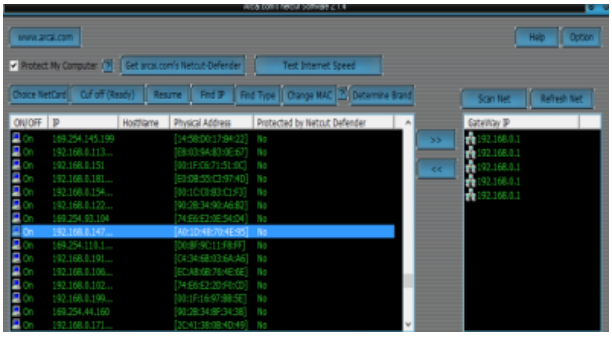

Figure 3: ARP spoofing

3) Session Hijacking Attacks: In this kind of attacks, attacker insert falsified IP packets after session establishment, sequence number alternation and prediction.

4) Man-in-the-Middle Attacks (MITM): This kind of attacks rely on ARP spoofing for intercepting and modify traffic.

3 Building a Secure Network by Decreasing Familiar Attacks

To design a Secure Network we need to define the security function against a network intrusion by decreasing the familiar attacks. When we consider secure but cost effective way for designing and deployment a network infrastructure we must have to analyses the feasibility both. To design a cost effective secured organizational network system here we proposed the steps generally: 1) Implementation of both Hardware and software firewall. 2) Establishment of Virtual Private Network (VPN) for one or more network connection. 3) Implementation of MAC-Bindings with IP addresses registration on server side for network broadcasting. 4) For Wi-Fi Router establishment within same server use the Authentication server for end user identification and tracking. 5) Synchronizing, Observing and tracing of internal gateway router and core router and core switch. 6) VLANs (Virtual LAN) creation.

1) Implementation of Both Hardware and Software Firewall: Firewall concept is adapted to centralize access control. It works as the gatekeeper between the untrusted Internet and the more trusted internal networks. A firewall may be software and hardware firewall. Firewalls provide several types of protection:

   a. It blocks unwanted traffic.

   b. It can direct incoming traffic to more trustworthy internal systems.

   c. It hides vulnerable systems which aren't easily be secured from the Internet.

   d. It can log traffic to and from the private network.

   e. It can hide information like system names, network device types, network topology and internal user ID's from the Internet.

   A hardware firewall is in Figure 4.

2) Establishment of Virtual Private Network (VPN) for One Or More Network Connection (See Figure 5): A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. By establishing a virtual point-to-point connection through the use of virtual tunnelling protocols, dedicated connections, or traffic encryption a VPN is created. For encrypting and secure user different VPN protocol are used such as IPsec, TLS (Transport layer Security), SSL (Secure Socket Layer), Open VPN or Point-to-Point Tunnelling Protocol, *etc.* Common uses of the organization VPN include access to file sharing/shared drives.

3) Implementation of MAC-Bindings with IP Addresses Registration on Server Side for Network Broadcasting (See Figure 6): Binding IP addresses to MAC addresses could avoid IP address changing with reconnection. Once specified device's MAC address and IP address are bound, the IP address will be reserved for the device and the device is easy to trace if any occurrence is happened. It is easy for the Administrator to manage critical devices and a great method to manage the LAN clients.

4) For Wi-Fi Router Establishment within Same Server Use the Authentication Server for End User Identification and Tracking: If we want to keep end user track for Wi-Fi connection where Wi-Fi

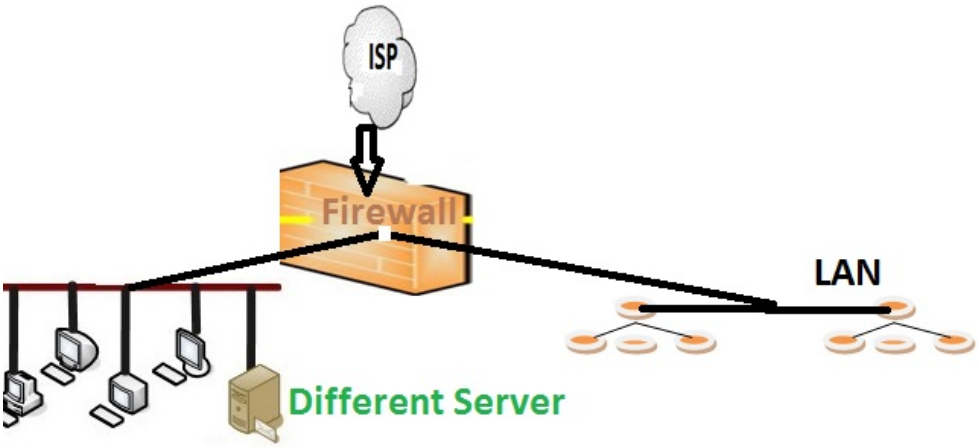

Figure 4: A simple firewall implementation

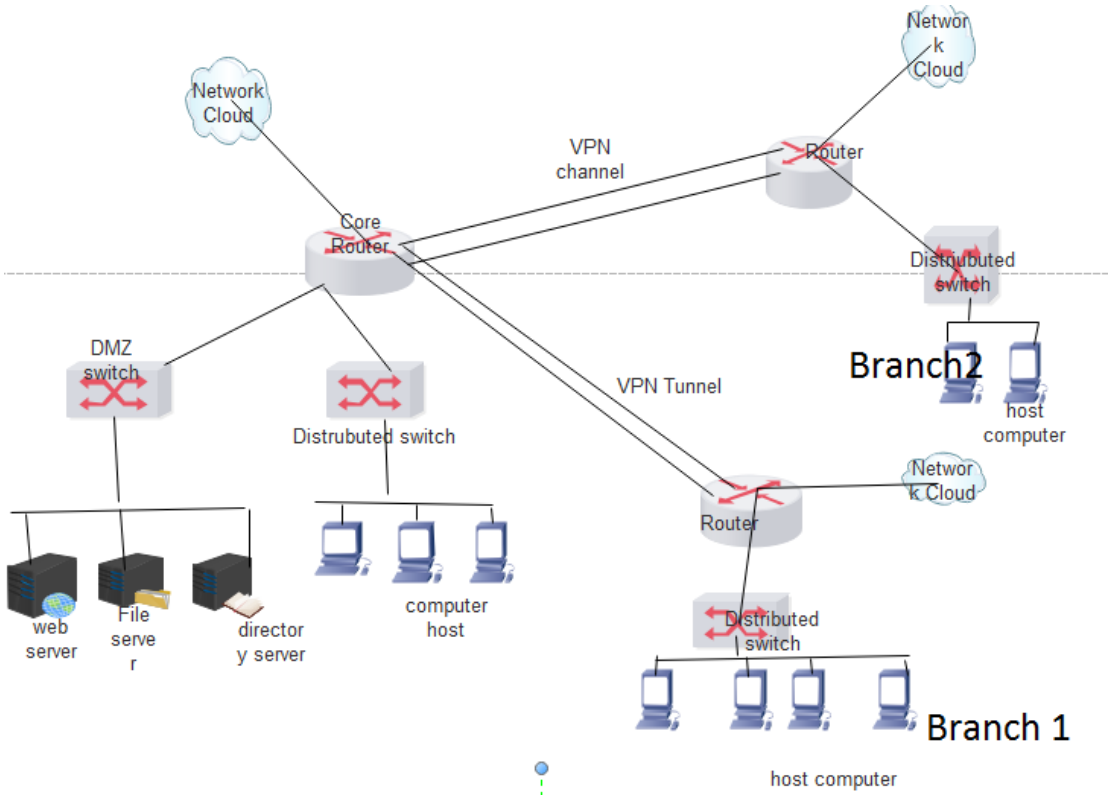

Figure 5: VPN connection for organizational branch

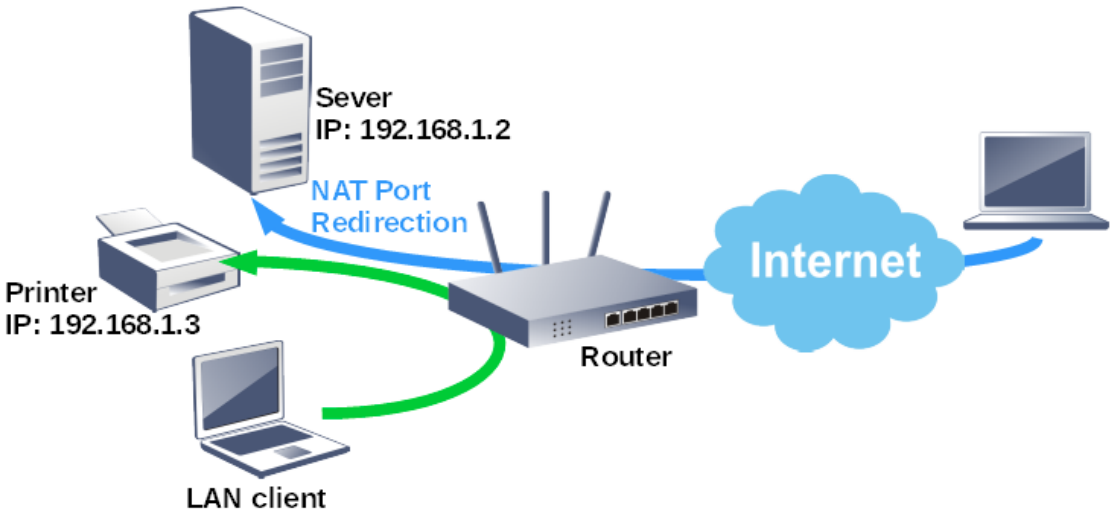

Figure 6: MAC Bindings with IP for secure networking

router and WLAN are configured in same proxy server then we must use an authentication server for user identification and tracking. Radius Server and AAA server are used for authentication, authorization, accountability and user logs filtering. Scalability, security and flexibility are ensured by using those server mechanisms. When the terms wireless network comes into front the Strong authentication, Strong data encryption, Protects broadcast and multicast traffic, User authentication, Secures access to the WLAN instead of just to the packets and Additional network devices required are most considerable things in wireless establishment.

5) Synchronizing, Observing and Tracing of Internal Gateway Router and Core Router and Core Switch. As we know that every internal private network of organization is created from a Real IP that is connected to the real world network like internet. In this sense a core router and switch is designed for creating network. For a secure network design and deployment we need to synchronize, observe and trace of internal gateway router and core router for every user. The other objective we need to consider that monitoring this it is easy to avoid external and internal threat. Flexibility and scalability can be assured through it.

6) VLANs (Virtual LAN) Creation. It works in data link layer. VLAN partitions and isolate a computer network. In practical terms, multiple VLANs are pretty much the same as having multiple separate physical networks within a single organization - without managing multiple switches and cable plants. Because VLANs segment a network, creating multiple broadcast domains, they effectively allow traffic from the broadcast domains to remain isolated. We have suggested some VLANs for better security of campus network and reducing broadcast [11]. Table 2 shows an example of the proposed VLAN creation.

By examine all above the designed structure of the suggested model are as in Figure 7.

Table 2: An example of the proposed VLAN creation

VLAN ID	VLAN Name
1	A
5	D
10	L
15	C
20	F
40	I

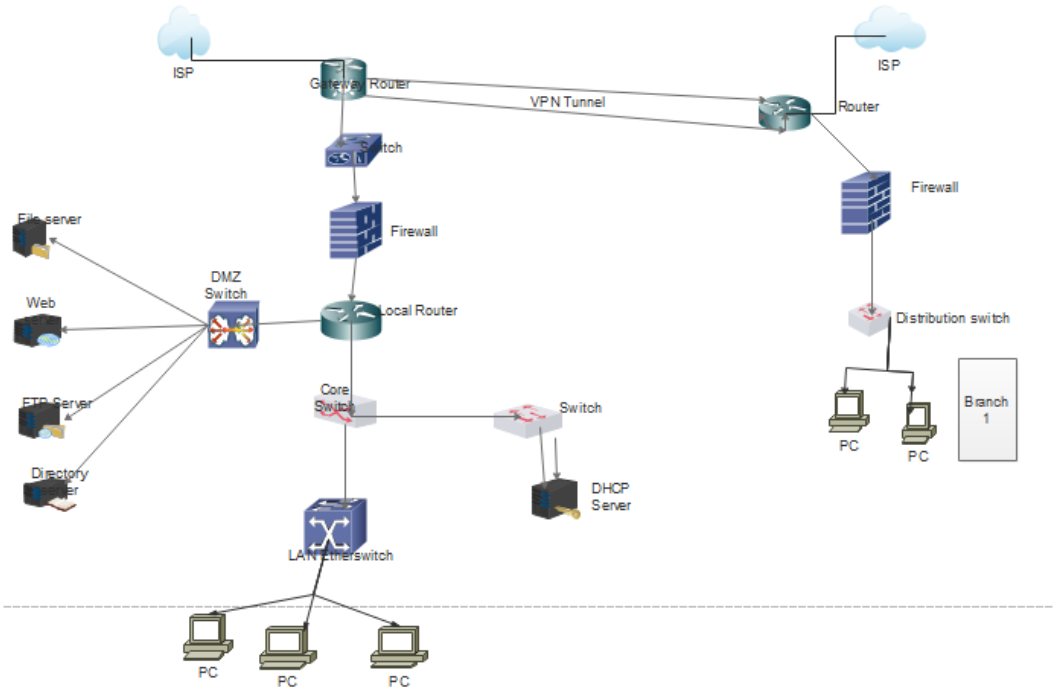

Figure 7: Structure of suggested secure network model

4 Conclusion

When we design the architecture and deployment of a network system, its security becomes an important issue and considerable matter for any organization. So by following the above network design and considering the above discussed security terms, one organization can design and deploy a scalable, better performer and secured network which is easy to maintain. In this discussion and work, we have proposed a cost effective secure network design based on the work environment and required security, scalability and other aspects. The terms we have introduced and considered in designing network architecture are helpful in mitigating the known attacks and reoccurrence attacks.

This paper presented the tips and recommendations to achieve a best security and to protect the network from threats, vulnerabilities and attacks by applying security configurations such on strong routing filtering using router and firewall which can assure a better network security.

References

[1] S. Alabady, "Design and implementation of a network security model using static VLAN and AAA server," in *3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA'08)*, 2008.

[2] S. Alabady, "Design and implementation of a network security model for cooperative network," *International Arab Journal of e-Technology*, vol. 1, no. 2, June 2009.

[3] M. N. B. Ali, M. L. Rahman, S. A. Hossain, "Network architecture and security issues in campus networks," in *Fourth International Conference on Computing, Communications and Networking technologies (ICCCNT'14)*, 2014.

[4] G. Gur, S. Bahtiyar1, F. Alagoz, "Chapter 30: Security analysis of computer networks: Key concepts and methodologies," in *Modeling and Simulation of Computer Networks and Systems Methodologies and Applications*, pp. 861–898, 2015.

[5] S. Keshav, *An Engineering Approach to Computer Networking*, Addison Wesley, 2010.

[6] J. F. Kurose and W. R. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Pearson, 2000.

[7] S. Al Maskari, D. K. Saini, S. Y. Raut and L. AHadimani, "Security and vulnerability issues in university networks," in *Proceedings of the World Congress on Engineering (WCE'11)*, London, U.K., 2011.

[8] B. Mulyawan, "Campus network design and implementation using top down approach," in *Proceedings of the 1st International Conference on Information Systems for Business Competitiveness (ICISBC'11)*, 2011.

[9] L. L. Peterson and B. S. Davie, *Computer Networks: A System Approach*, Elsevier, 1996.

[10] M. T. Soleimani, M. Kahvand, " Defending packet dropping attacks based on dynamic trust model in wireless ad hoc networks," in *IEEE 17th Mediterranean Electrotechnical Conference (MELECON'14)*, Beirut, Lebanon, pp. 362-366, 2014.

[11] Z. Xiaozhe, W. Zaifang, L. Qiong, F. Guiming, *The Design and Implementation of the Integration between Switches and Routers*, Computer Engineering and Application, 2014.

Md.Shamimul Islam was born in Satkhira, Bangladesh, on 28th October, 1988. He received the B.Sc. and M.Sc Degree in Computer Science and Engineering from the Jahangiranagar University, Bangladesh in 2011, and in 2012 respectively. He worked at Samsung R&D Institute Ltd., Bangladesh from 1 Oct, 2012 to 31 Dec, 2014 as a Software Engineer. From 27th July, 2016 he is being as a Scientific Officer of Institute of Computer Science Division in Bangladesh Atomic Energy Commission (BAEC). He is a member of Bangladesh Computer Society. His research interest includes Network and Cyber Security,

Communication Engineering, IoT, Software Engineering and Human Computer Interaction.

Md. Haidar Ali was born in Kishorgonj, Bangladesh, on 25th January, 1985. He received the B.Sc. Degree in Computer Science and Engineering from the Daffodil International University, Bangladesh in 2010, and in 2012, he received the M.Sc. degree in Computer Science and Engineering from Daffodil International University. He worked at Padma Multipurpose Bridge Project, Bridge Division under Ministry of Road Transport & Bridges, Bangladesh from 14 October 2014 to 05 November, 2016 as a Assistant Programmer. From 15 November 2016 to still now, He is being a scientific officer of Computer Science Division in Bangladesh Atomic Energy Commission. He is a Life Time Member of Bangladesh Computer Society and Also Life Time Member of IEB. His research interest includes Network and Cyber security, communication Engineering.

Md. Ahsan Habib was born in Comilla, Bangladesh. On 05th December, 1984, he received the B.Sc degree in Electrical, Electronics and Telecommunication Engineering from Dhaka International University, Bangladesh in 2010 and in 2014, received the M.Sc degree in Computer Science from Jahangirnagar University, Bangladesh. He worked at Bangladesh Chemical Corporation, Bangladesh from 01 February, 2016 to 14 November as an Assistant Engineer. From 15 November, 2016 he is being a Scientific Officer of Institute of Computer Science in Bangladesh Atomic Energy Commission. He is a member of Bangladesh Computer Society.

Mohammad Nur Nobi was born in Bangladesh in 1987. He received the B.Sc. (Engg.) and M.Sc. (Engg.) degrees from Mawlana Bhashani Science and Technology University, Tangail, Bangladesh, in 2011 and 2015, respectively. He joined Samsung R&D Institute Bangladesh, in 2011. Since 2016, he has been with the Bangladesh Atomic Energy Commission, where he is a Scientific Officer. His main areas of research interest are algorithm, machine learning, artificial intelligence and cyber security. Mr. Nobi is a member of the Bangladesh Computer Society (BCS).

Md. Mahbub Alam was born in a rural area called Dhamrai of Dhaka in 1991. He has completed his B.Sc & M.Sc from the Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh. He worked as a lecturer in Gono University at the Dept. of CSE from January 2015 to February 2016. He worked as an Assintant Engineer in WALTON Group at the Computer R&D section from February 2016 to November 2017. Currently he is working as a Scientific Officer at the Institute of Electronics in Bangladesh Atomic Energy Commission. His research interests include big data analysis, artificial intelligence, pattern recognition and expert system, computer vision, system that can provide distinct service through internet protocol and any system that can be beneficiary for common people. He is also interested in entrepreneurship.

Dr. Hossain has been working at Bangladesh Atomic Energy Commission (BAEC) for more than 18 years. He actively involves in the R&D, and training activities in BAEC. He received his PhD in Innovation Technology & Management, MS in Electrical & IT Engineering from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea, and BS in Electrical & Electronic Engineering from Chittagong University of Engineering & Technology (CUET), Bangladesh. Hossain's research interest includes; (i) Nuclear innovations/knowledge management (ii) Nuclear cyber security, (iii) Computer security in nuclear facilities. His articles have appeared in several international journals and conferences proceedings as well.