Using the Cloud to Teach Computer Networks

Conference Paper · December 2015

Khaled Salah
Khalifa University of Science Technology & Research

Using the Cloud to Teach Computer Networks

Mhd Wael Bazzaza Khaled Salah
Electrical and Computer Engineering Department
Khalifa University of Science, Technology and Research, UAE
{mwael.bazzaza, khaled.salah}@kustar.ac.ae

***Abstract*—STEM education can enormously benefit from cloud technology. The cloud can offer instructors and students (whether local or remote) on-demand, dedicated, isolated, unlimited, and easily configurable compute and storage resources. The cloud can significantly reduce cost and expenditure on lab construction and maintenance. Due to these features, the cloud has been widely adopted by many universities and schools throughout the world. In this paper, we show how the cloud can be utilized to replace traditional physical computer networks laboratories. In particular, we demonstrate how cloud-based laboratory exercises related to computer networks can greatly help students in acquiring almost all crucial computer networks skills. The cloud we used for this course was the Amazon Web Services (AWS) public cloud. However, the use cases and approaches are equally applicable to other cloud platforms.**

Keywords—Cloud Computing; Computer Networks; eLearning, Education Technology .

I. INTRODUCTION

Effective pedagogy and delivery of a course on the subject of computer networks require not only theoretical learning outcomes, but more importantly practical and useful hands-on experience. This way, mastery of the topic can be achieved by enhancing theory with practical experience. Today, most computer network courses are supplemented with laboratory exercises to enable students acquire various networking skills related to network management and configuration as well as traffic monitoring and analysis.

Offering practical computer networks training for local and remote students poses some major challenges. Specifically, in a traditional classroom setting, a computer networks lab can be established with a number of machines networked with routers and switches and equipped with relevant network software packages. With the presence of local and remote students taking the same course across multiple university campuses, we need to replicate such a setting. Coordinating, managing and maintaining the same setting across campuses for students taking the same networking course are usually costly and not viable.

Managing a networks lab is not an easy task as lab technicians are usually needed to aid the instructor in installation of various software packages and tools, configuration of switches and routers, preparing workstations for students, and scheduling lab sessions. Moreover, students in an introductory course on computer networks may lack needed skills in configuring and installing various software tools and hardware equipment like switches and routers, which means the instructor has to spend extra time to troubleshoot misconfiguration and installation problems. In a way, with classical lab settings, hands-on projects can easily get diverted from meaningful, focused and enjoyable exercises to superfluous setup, installation, recovery, management and scheduling exercises for lab technicians, instructors and students alike.

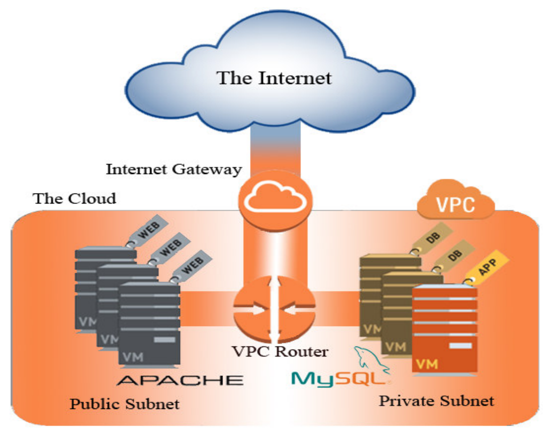

Fig. 1. A basic VPC with two subnets

The cloud computing model alleviates most (if not all) of the problems introduced by classical lab settings. The cloud provides on-demand, elastic, dedicated, isolated, scalable, (virtually) unlimited, easily configurable, and equally accessible virtual machines for all students whether they are local or remote. In this paper, we show how the cloud platform and services can address some of the aforementioned challenges caused by classical lab settings. In this paper, we have used Amazon Web Service (AWS) Cloud as an example; however, the use cases and approaches laid out in this paper are also applicable to other cloud platforms such as Rackspace and Google Compute Engine, among others.

AWS Cloud provides the user the ability to build a virtual private cloud (VPC) of many virtual machines that are networked together. This VPC can be used by students and instructors as a basis to conduct numerous hands-on lab exercises related to computer networking concepts. The VPC owner can set and configure various control and management functionality and features over the virtual networking environment. These include IP address range selection, the number of subnets, as well as routing tables and network gateways. It is also possible to configure security access and control on the instance level by using security groups, or on the subnet level by using network access control lists. Fig. 1 shows a simple diagram of a VPC. It consists of public and private subnets. The public subnet can contain instances like web servers that are open to the public where these nodes are accessible from the Internet. On the other hand, the private subnet contains instances that are not exposed to the public. Examples of such instances are MySQL database servers and application servers.

The remainder of this paper is organized as follows. Section II provides a brief overview of AWS Virtual Private Cloud environment and its different configurations. Section III summarizes the main advantages of using the VPC as a platform to conduct computer networks lab exercises. Section IV describes various hands-on computer network lab exercises that can be carried out by students on the cloud. Section V presents some challenges and limitations for using the cloud as a laboratory platform to teach computer networks. Section VI discusses related work found in the literature, highlighting key differences from our work. Finally, Section VII concludes the study.

II. THE AWS VIRTUAL PRIVATE CLOUD

One of the leading cloud providers today is Amazon AWS. With Amazon VPC, it is possible to employ a private virtual network that is logically isolated in the Cloud. Having a VPC is similar to building a private network with multiple virtual machines which can be networked in different subnets and attached to network devices such as routers, servers as those of DHCP and DNS, as well as firewalls. Virtual machines can have private or public IP address or both. Amazon's VPC dashboard allows users to build, manage and configure a VPC in terms of subnets, routing tables, IP addresses, connections, security groups and network ACLs.

In AWS terminology, the virtual machines (VMs) in the VPC are called EC2 (Elastic Compute Cloud) [1]. VM instances can be Windows or Linux based, and they come in different sizes and compute power. With VPC, it is possible to use various network configurations. Within the VPC, a user can create a publically accessible subnet which may contain public servers such as web servers, e-mail servers, or FTP servers. Also the user can create one or multiple private subnets of VMs with restricted access using security group configurations. These subnets may host app, database, compute, and storage servers. Fig. 2 shows an illustration of an example of VPC 1 with two subnets: (a) a public subnet with CIDR address block of 10.0.0.0/24, and (2) a private subnet with CIDR address block of 10.0.1.0/24. VPC 1 has a CIDR address block of 10.0.0.0/16. The VMs within the public subnet is configured with two IP addresses: public and private. The public IP address is called EIP (Elastic IP) in AWS terminology. With the proper network ACL and security groups, the VMs with EIPs can be made accessible from the Internet.

As shown in Fig. 2, it is possible for the user to extend a VPC to other VPCs. The extension can be to another VPC in the same cloud geographical area via a VPC peer-to-peer connection setup. In addition, a corporate or enterprise network can be extended to the VPC via secure IPSEC connection with configurations at on-premise gateway and cloud-based virtual private gateway, whereby it becomes possible to securely connect to the instances of the cloud directly through the private IP addresses. As shown in the figure, access from the Internet to VPC can be done via the public subnet with EIPs or by using a single host with a single public IP address by setting a NAT server, as will be discussed in Section IV.

III. ADVANTAGES OF USING VPCS

In this section we highlight the main advantages of using the cloud, particularly the concept of VPC, in conducting lab exercises related to computer networks. The biggest advantage of using the VPC to teach computer networking to students is that it is scalable, reliable and cost-efficient. It is possible to expand or shrink the amount of computing resources that are required for each student. Each student can have his own VPC without interfering with other students' setup or configuration. This means that students will no longer have to compete for classical lab resources. In addition, the high cost needed to operate and maintain classical labs is eliminated. Time flexibility is achieved, as students are no longer required to sit in a classical lab for a few hours to solve an exercise. Instead, they can log on into their AWS accounts on any time at their convenience.

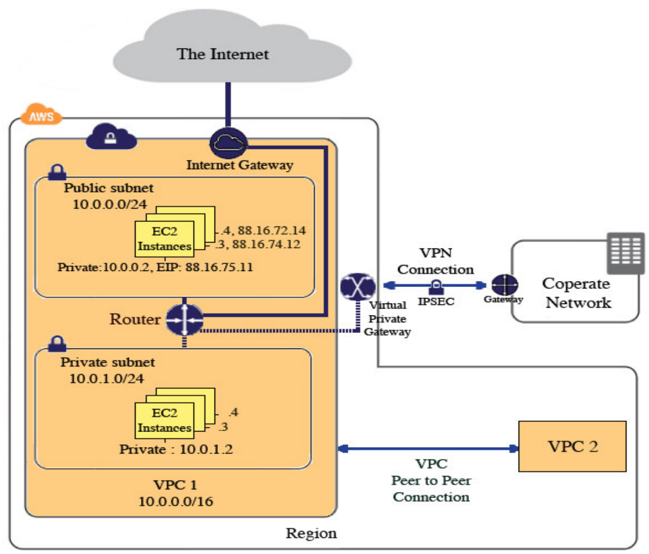

Fig. 2. A VPC model with different connections

With this configuration, students (whether they are local or remote) can equally access the VPC at any time and from anywhere. Also the instructor has the ability to log in and access the work done by the students whether students are remote or local. The instructor can easily troubleshoot instances and VPC configurations. Under this configuration, the instructor does not have to rely on a lab technician to supervise the students as the situation in a classical lab setting. The problems of troubleshooting software and tampered switches, routers and other hardware are all eliminated, as students can easily terminate a non-functioning VM or network devices and rapidly in minutes create another one on the cloud.

IV. CLOUD BASED HANDS-ON EXERCISES

In this section, we list examples of cloud-based hands-on lab exercises related to computer networking that the students can carry out using the concept of cloud VPC. The exercises aim to complement theoretical knowledge taught in the lectures and provide students with necessary computer networking skills to configure, manage, and setup various networking functionalities and devices. The following is a brief description of practical examples with basic and advanced network configurations.

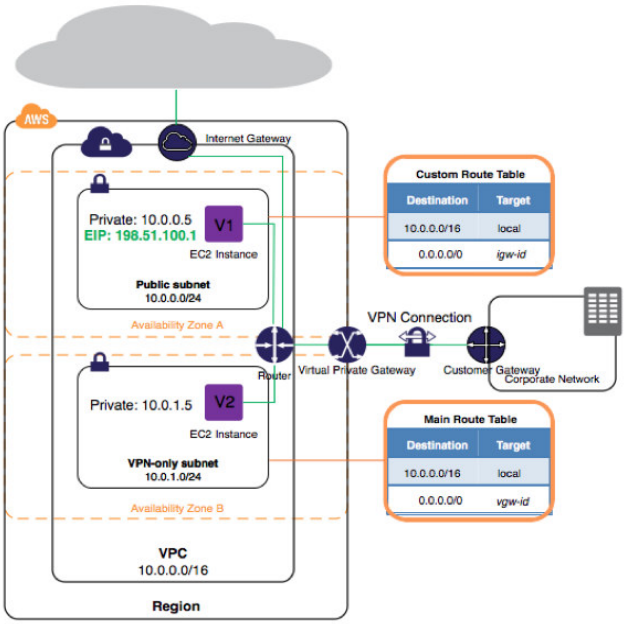

Fig. 3. Routing in VPC

Basic Computer Networking Exercises: Students can begin by creating a simple VPC using AWS which can be used to run various basic and fundamental networking exercises. They can start by creating the first and easiest configuration, which is the VPC with a single public subnet with one or two VMs running Linux or Windows. Students can learn how to connect to these instances remotely via SSH, RDP, or Putty, and locally within the same subnet using telnet or rlogin utilities. Students can learn and examine the different IP address configuration like private and EIP given to each instance. Students can examine for each instance the ARP cache, DNS cache, netmask, gateway addresses, security policies, etc. Students can examine these by running popular networking tools and utilities such as ping, ipconfig, ifconfig, nslookup, dig, host, arp, traceroute, whois, etc. More importantly, students can also carry out important protocol analysis exercises involving tools like tcpdump and wireshark in which students examine the various packet headers of protocols as those of TCP, UDP, ICMP, and Ethernet. Students also can use tools such as nmap and netstat to perform network discovery and reconnaissance exercises.

Establishing P2P Connections: Another practical exercise for students to carry out is to establish VPC P2P connections between two or more VPCs. At minimum, the student would create two VPCs in the same region and connect them together. A VPC peering connection is a networking connection that enables the students to route traffic between them using their private IP addresses. Instances in either VPC can communicate with each other as if they were on the same network. In this exercise students would learn about configuring carefully the proper IP address blocks and subnet masks, as well as CIDR blocks to be able to seamlessly connect all instances in both VPCs.

Configuring Routing Tables: Each Amazon VPC has an implicit router with a main routing table that can be configured [2]. This means there is no need to manually configure numerous physical routers and test them across several machines, as is the case of a classical lab setting. Instead, each subnet in a VPC can have a custom routing table created, which controls the routing of the subnet. Each route in a table specifies a destination CIDR and a target host. Fig. 3 shows a VPC with two subnets: a public subnet with CIDR address block 10.0.0.0/24 and another private VPN subnet with 10.0.1.0/24 block. As shown in the figure, each subnet can be configured with a separate routing table. For the public subnet, local traffic can be routed locally, and remote traffic can be routed to *igw-id* which is the Internet Gateway. For the private subnet, local traffic can be routed locally, and remote traffic can be routed via *vgw-id* which is the Virtual Private Gateway. Similarly, the private VPN subnet must be able to connect to the instances in the VPC and also to the corporate network through the VPN tunnel. This is done with two routing table entries. The first entry will be the similar to the public subnet entry to allow local routing. The second entry will allow all other traffic (0.0.0.0/0) to go through a virtual private gateway that connects the VPN subnet to the corporate network through the VPN tunnel.

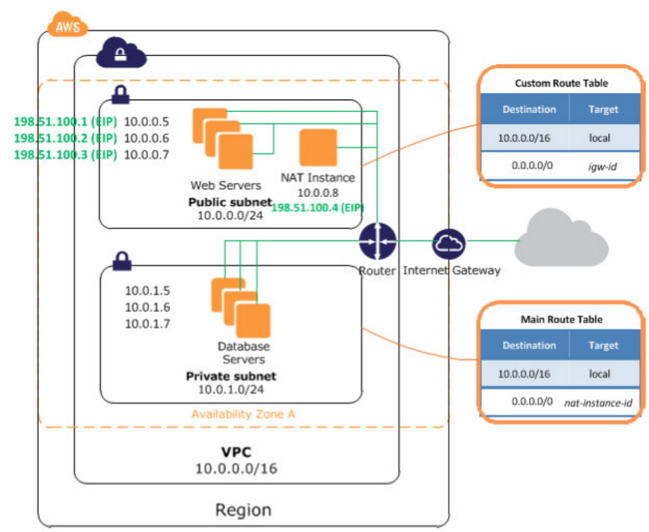

Fig. 4. A VPC with NAT configuration

NAT Configuration: A practical hands-on lab exercise to solidify the important concept of NATing (or Network Address Translation) is to allow students configure a NAT virtual sever in a VPC, as shown in Fig. 4. In this exercise, students can set up a NAT instance [3], which is readily available on AWS cloud platform for users to launch and configure. As depicted in the figure, a NAT instance with IP address 10.0.0.8 is situated in the public subnet, and the routing table of the private subnet is configured such that all remote traffic is destined to this NAT instance. As shown in the figure in the routing table for the private subnet, the default traffic other than the VPC local traffic is destined to "*nat-instance-id*". This will allow all instances within the private subnet to access the Internet. The configuration shown in Fig. 4 enables instances in the private subnet to initiate outbound traffic to the Internet, but prevent the instances from receiving inbound traffic originating from the Internet.

Configuring Security Groups and Network ACLs: Security groups and network ACLs can be used as virtual firewalls to control inbound and outbound traffic [4,5]. As shown in Fig. 5, security groups operate at the instance level whereas network ACLs operate at the subnet level. Different rules can be added to control inbound and outbound traffic at each level. The rules are similar to those rules of traditional firewalls where traffic can be allowed or denied based on source or destination IP addresses, protocol, port, etc. It is worth noting that security groups are stateful in which return traffic is automatically allowed; however, network ACLs are stateless in which return traffic must be explicitly allowed by rules. Therefore, useful and practical exercises to empower student with necessary skills to manage and configure rules to control traffic to a subnet or an instance can be given. As a simple exercise, students can be asked to setup multiple subnets with different traffic control rules among instances as well among subnets and the outside world. For example, students can be asked to setup and test different network services such as Telnet, Web, and FTP in one subnet and then set up the necessary rules for both security groups and network ACLs to allow HTTP, FTP, and Telnet traffic to all instances within the VPC; however, for the outside world, the rules have to be setup such that only HTTPS, SFTP, and SSH traffic are allowed.

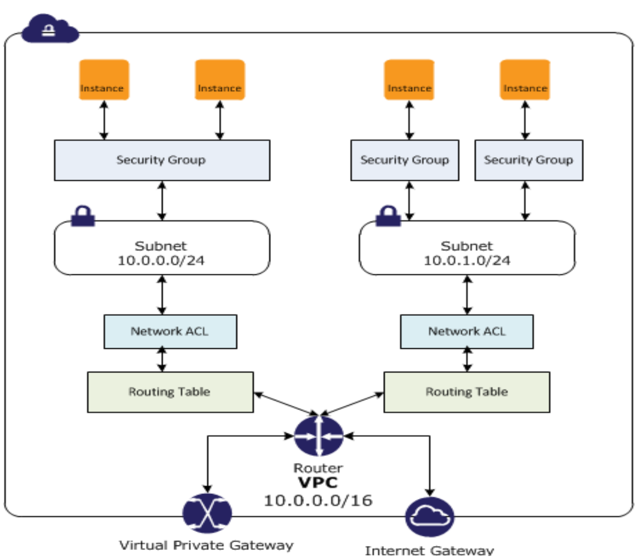

Fig. 5. Security groups and network ACLs in VPC

Configuring Host-level Firewalls: Students can also be asked to experiment with configuring personal Linux and Windows firewalls from inside the VM itself. Students can develop skills to experiment with a Windows firewall utility via "$netsh advfirewall" and with Linux IPTables to add, delete and test the activation of simple firewall rules. Simple rules can be set for passing and denying FTP and HTTP traffic. Moreover, students can be asked to examine the impact of changing the order of rules in the firewall rulebase so as to demonstrate that the first match counts. For this experiment, each student would use two machines: one EC2 instance with firewall setup and FTP and HTTP services, and another client machine (which could be a local PC, a laptop or an EC2 instance in the same or different subnet within the VPC) to send HTTP and FTP requests.

DNS and DHCP Configuration: More advanced exercises can be given to students related to setting up DNS and DHCP [6,7]. Students can be asked to set up a DNS server for multiple VPCs which can be used to map and resolve IP addresses of hostnames and domain names. In addition, DHCP server configurations are also needed to associate a private or public IP address to an instance when launched. DHCP server configuration involves adding the IP addresses for DNS, NTP, NetBIOS servers.

Elastic Network Interfaces: Setting elastic network interfaces is another advanced exercise that can be given to students with the aim of providing students with extra networking management skills [8]. A student can select an instance to attach multiple network interfaces with attribute settings related to private and public IP addresses, MAC addresses, security groups and network ACLs, etc. Use cases for attaching multiple network interfaces to an instance can include setting up own virtual routers or gateways, routing to security appliances like IDS, workload balancing and high-availability solutions.

V. LIMITATIONS AND REMEDIES

In this section, we discuss some challenges and limitations for using the cloud as a laboratory platform to teach computer networks. We also suggest ways to address such limitations. First, cloud-based teaching requires a learning curve for both instructors and students. A second limitation is that AWS VPC dashboard, as of this writing, is lacking the feature of visualizing the network topology to show the various nodes within the subnets and VPCs. Students would need to keep in mind or on paper the network topology. This should not be a major concern as most of the lab exercises involves a small-scale network comprises handful of network nodes. Publically available tools like Zenmap can be used to build easily the network topology. For large-scale networks, commercial network mappers from RightScale, Cisco Netflow, or Kaseya can be used to offer advanced visualization and interactive network management and configurations.

A third limitation of using the cloud to teach computer networking is that some networking exercises cannot be carried out on the cloud. Packet sniffing cannot be done on wireless protocols such as WEP and WPA. However, this can be easily resolved as students can install WireShark on their laptops and sniff packets from any access point that can be set up using a wireless router or a smartphone. Moreover, some aspects of networking lab exercises involving physical networking hardware may not be feasible in a cloud environment. For example, making Ethernet cables of different types (e.g., straight-through/crossover/rollover) or configuring physical Ethernet switches and MAC address tables may not be possible. Also, configuring VLANs, physical routers, and full functionality DHCP service may not be feasible. As a workaround for these obvious shortcomings is to allow students to install a simulation program such as Cisco Packet Tracer [9] which provides almost real networking topologies using Cisco routers and switches that can configured using the command line interface utility.

VI. RELATED WORK

In this section, we discuss related projects found in the literature, highlighting key differences from our work. One popular project is Emulab PlanetLab portal [11,12]. This portal gives access to physical resources with capabilities to remotely allocate, configure, and manage physical machines. The platform can be used to support the research and development of new network services, protocols, and technologies. Another popular project is the GENI project [13,14]. GENI is an open, large-scale, realistic experimental facility to conduct research in global communication networks. GENI can also be used in for education purposes [14]. Both PlanetLab and GENI are not cloud-based, and are designed primarily for research, and not as teaching laboratories or educational platforms.

Virtual technology has also been used to build remotely accessible laboratories for providing hands-on and practical training. Some of the other popular projects include DeterLab [15,16], TeleLab [17], and VITAL. These labs provide students with remotely accessible virtual networked machines that can be configured and used to carry out hands-on exercises. These platforms offer limited features to carry out important networking configuration lab exercises such as NAT, IP address configuration, routing tables, ACL, and security groups.

NETinVM (NETwork in Virtual Machine) is a standalone virtualized environment [18]. NETinVM runs multiple virtual machines (VMs) on a single Linux host, utilizing thereby the concept of UML (User-Mode Linux). Running experiments with reasonable performance when having many virtual machines launched within NETinVM requires the student to own a high-speed laptop or a desktop with large RAM. Unlike the cloud, NETinVM does not offer remote control access to the instructor to troubleshoot, check, and grade student hands-on coursework.

Perhaps the closest to our work is presented in [19,20]. In [19,20], the author showed how the cloud can be used as platform for remote and local students to perform hands-on practical laboratory exercises related to cyber security. The author showed how popular network security exercises can be carried out in the cloud. The concept of utilizing the cloud to teach specifically hands-on lab exercises related to computer networks and VPC was not addressed in [19,20]. The exercises were mostly carried out within one single virtual machine with installation and configuration of many security tools.

VII. CONCLUSION

In this paper, we have illustrated how the cloud can be used as a platform to conduct and carry out various lab exercises related to computer networks. In particular, we showed how Amazon VPC can be used to empower students with needed networking skills related to managing, monitoring, analyzing, and configuring subnets, network hosts, devices, traffic, and protocols. It has been noted that, except for a few exercises, which require physical hardware, the majority of networking lab exercises can be carried out conveniently and effectively in the cloud.

ACKNOWLEDGMENT

Special thanks for Amazon AWS for providing a research grant to support this study [10].

REFERENCES

[1] Amazon Web Services, Amazon Elastic Compute Cloud (EC2) User Guide," [Online]. Available: http://aws.amazon.com/documentation/ec2/

[2] Amazon Web Services. Amazon Virtual Private Cloud Route Tables [Online]. Available: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html

[3] Amazon Web Services, "Amazon Virtual Private Cloud NAT Instances," [Online]. Avaialble: http://docs.aws.amazon.com/AmazonVPC/latest/ UserGuide/VPC_NAT_Instance.html

[4] Amazon Web Services, "Security Groups for Your VPC," [Online]. Avaialble: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/ VPC_SecurityGroups.html

[5] Amazon Web Services. Network ACLs [Online]. Avaialble: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

[6] Amazon Web Services, "Using DNS with Your VPC," [Online] Avaialble: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html

[7] Amazon Web Services, "DHCP Options Sets," [Online]. Avaialble: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html

[8] Amzaon Web Services, "Using Elastic Network Interfaces in Your VPC," [Online] Avaialble: http://docs.aws.amazon.com/ AmazonVPC/latest/UserGuide/VPC_ElasticNetworkInterfaces.html

[9] Cisco Inc., "Cisco Networking Academy," [Online]. Available: https://www.netacad.com/web/about-us/cisco-packet-tracer

[10] Amazon Web Services, "Education Grants," [Online]. Available: http://aws.amazon.com/education

[11] S. Karlin, "An Overview of the PlanetLab Architecture," [Online]. Available:http://www.planet-lab.org/Talks/2004-01-7/JointTechs.pdf.

[12] K. Webb, M. Hibler, R. Ricci, A. Clements, and J. Lepreau, "Implementing the Emulab-PlanetLab Portal: Experience and Lessons Learned", In Proc. of Workshop on Real, Large Distributed Systems, 2004.

[13] Berman, M., Chase, J. S., Landweber, L., Nakao, A., Ott, M., Raychaudhuri, D., and Seskar, I. (2014). GENI: A federated testbed for innovative network experiments. Computer Networks, Elsevier, Vol. 61, No. 1, pp. 5-23.

[14] GENI Project, "Resources for using GENI in the classroom"[Online]. Available: http://groups.geni.net/geni/wiki/GENIEducation

[15] J. Mirkovic, and T. Benzel. "Teaching cybersecurity with DeterLab", In Proc. of IEEE Security & Privacy, January 2012, pp. 73–76.

[16] DeterLab. [Online] Available: http://deter-project.org and http://education.deter-lab.net

[17] C. Willems, T. Klingbeil, L. Radvilavicius, A. Cenys, and C. Meinel. 20 "A Distributed Virtual Laboratory Architecture for Cybersecurity Training", In Proc. of the 6th International Conference on Internet Technology and Secured Transactions, 2011, pp. 408– 415.

[18] D. Perez, and C. Perez. "NETinVM: A Tool for Teaching and Learning about Systems, Networks and Security," [Online]. Available: http://informatica.uv.es/~carlos/docencia/netinvm/ netinvm.html

[19] K. Salah, "Harnessing the Cloud for Teaching Cybersecurity," In Proc. of the 45th ACM Technical Symposium on Computer Science Education (SIGCSE), Atlanta, Georgia, USA, 2014.

[20] K. Salah, M. Hammoud, and S. Zeaddaly, "Teaching Cybersecurity using the Cloud," IEEE Transactions on Learning Technologies, Vol. 11, No. 4, November 2014, pp. 1-10.