

# V-Lab: A Mobile Virtual Lab for Network Security Studies

Yugesh Suresh Bhosale  
School of computing Science  
and Engineering  
VIT University  
Chennai, Tamilnadu 600 127,  
INDIA

Jenila Livingston L. M.,  
Ph.D  
Associate Professor  
School of computing Science  
and Engineering  
VIT University  
Chennai, Tamilnadu 600 127,  
INDIA

## ABSTRACT

Virtual Laboratories has been accomplished as an economic support in educational institutions. Using emerging technology such as cloud computing and rapid development in the mobile operating system and mobile applications Virtual laboratories are becoming popular in the educational as well as in business organizations. Time and place are major constraints on the learning system. By taking facilities provided by M-learning technology learners and researchers are able to perform their learning task very efficiently and well organized way. In this paper a brand new implementation architecture is provided for developers those who are interested to develop a virtual laboratories. Mobile phones are used as a front end for GUI. XEN Cloud Platform (XCP) and OpenStack both are open source are used to create virtual laboratories. By using java API's application developers are able to create virtual laboratories for android phones. This paper is mainly focused on network security experiments which require highly available, reliable, flexible, re-configurable and isolated laboratories for performing network security experiments as an academic course or research purpose. Creating large number of cluster of Xen Servers we are able to run multiple VMs which can be used as router, switch, host, DHCP server, FTP Server, firewall etc. and using OpenStack virtualization technique we can create a network, configure a network as per our requirement by using android phone as a user interface.

## General Terms

Cloud Computing, M-learning, Virtual Machines (VM), XEN Cloud Platform (XCP), OpenStack, V-Lab.

## Keywords

Cloud Computing, E-Learning, M-Learning, Virtual Labs.

## 1. INTRODUCTION

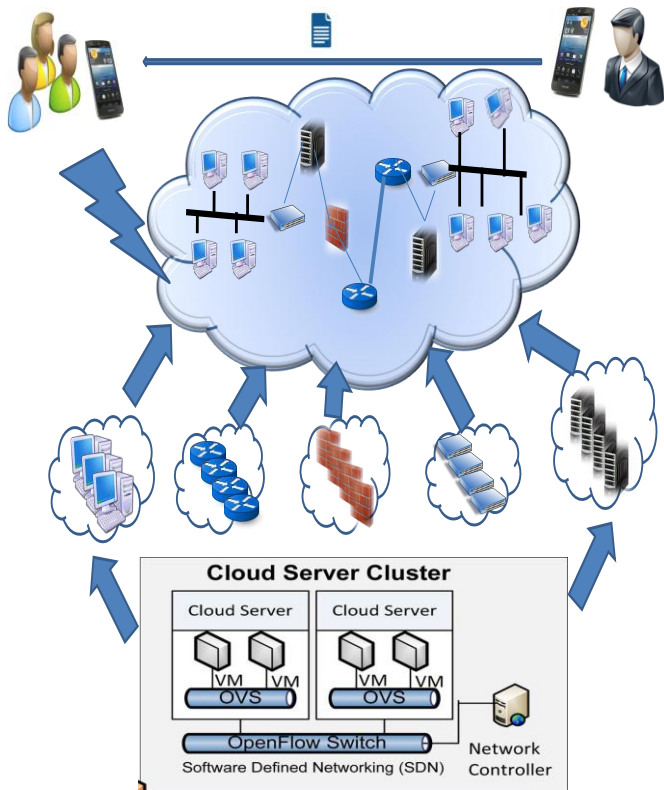
Time and place are major constraints in learning and education field. But nowadays it becomes easy because of newly emerged technologies and rapid development in electronic and telecommunication and computer science field. Mobile Learning called M-Learning is subset of E-Learning and both are part of distance education. Research shows that shipment in mobile phones and smart phones in previous last four years is rapidly increased as compared to PC's, laptops and desktop computers and tabs. Everyone is carrying mobile phones for doing their day to day activities. So why not in learning and education field. People are started using mobile devices for learning purpose. Virtual classrooms are available on mobile devices so no need to go at predefined location and

predefined time. But attending only theory classes is not helpful. For better understandings hands-on experiments are required but unfortunately we cannot perform hands-on experiments using mobile devices we need to go laboratories for performing such experiments. In this paper we tried to overcome this problem by proposing new brand methodology and implementation methods for creating virtual laboratories on mobile devices for network security education see Fig.1.

Virtual laboratories for studying network security are making importance for students, faculties and researchers. Traditional physical laboratories require purchasing high cost equipments such as routers, switches, firewalls, host computers, etc. Reconfiguration and maintenance of these physical laboratories are very difficult and time consuming. For networks security education we require highly flexible, scalable and reconfigurable and isolated laboratories. Therefore our traditional physical laboratories are not suitable for doing such experiments. We cannot use internet for doing Network security experiments because any experimental attack like man in middle or denial of service attack may damage the hardware or software's so these experiments are vulnerable for outside world in perspective of information, data, or software and hardware. So better to use virtual networks for doing such experiments. In case any damage happens then simply reconstruct new laboratory and continue our work.

In this paper we proposed a new technique for implementing mobile virtual laboratories for performing network security experiments. Using XEN cloud computing platform and OpenStack we are creating a virtual laboratory because XEN and OpenStack are open source virtual computing platforms. XEN Cloud Platform (XCP) and OpenStack are major components of this virtual laboratory. For accessing, reconstructing and reconfiguring this virtual lab remotely we provide an attractive GUI on android based application.

Rest of the paper is organized as follows Section I gives introduction of the topic and overall idea. Section II presents background of E-Learning and M-Learning with evolution, Section III provides related work and advantages and drawbacks, V-lab proposed architecture is explained in section IV ,Section V gives Conclusion and finally Section VI gives future scope.

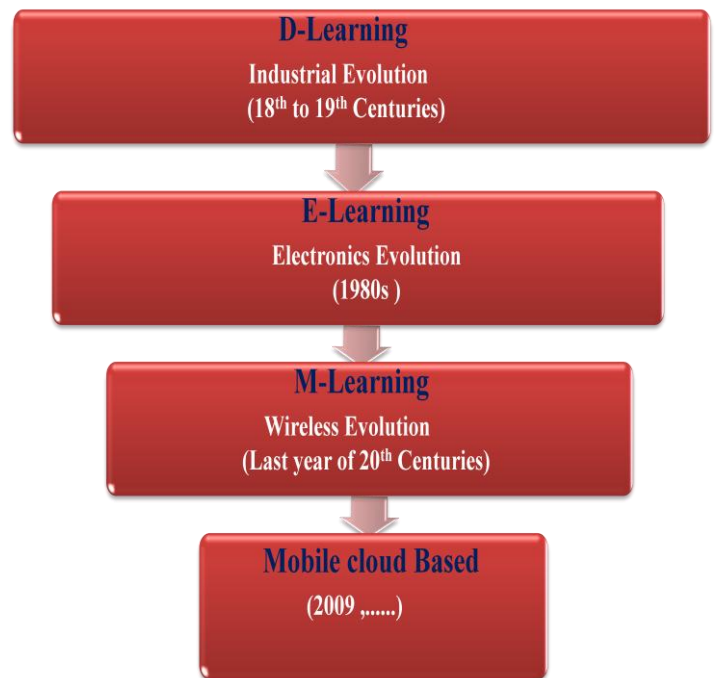


**Fig. 1. Basic idea and user Interaction**

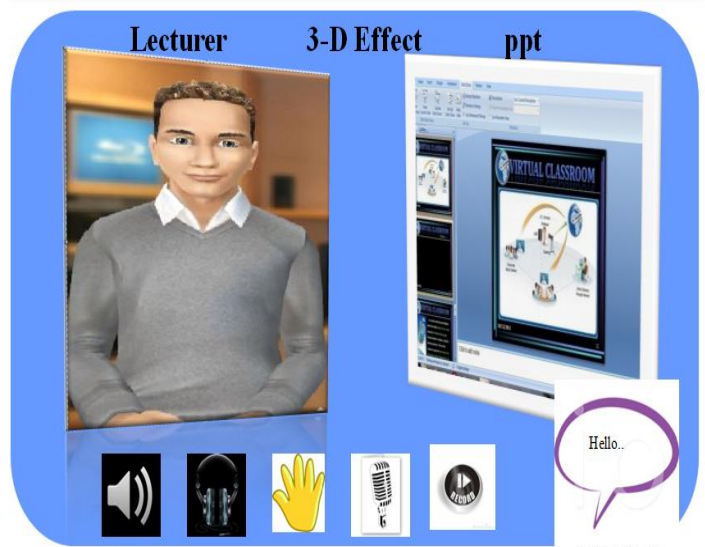
## 2. E-LEARNING AND M-LEARNING: BACKGROUND

The history of the evolution of the M-learning is shown in Fig. 2. In early eighteenth and nineteenth century D-Learning called distance learning started from traditional classroom learning is the industrial revolution. Some universities started distance learning courses for students who are from different geographical areas. In latest nineteen eighties E-learning started. People are started use of electronic devices in their learning environment so this evolution called electronic evolution. Online learning, video conferencing, virtual classrooms are available for learning different courses. Virtual classroom is shown in Fig.2.

In early last year of twentieth century shipment in mobile devices increasing rapidly a research shows as compared to shipment in desktop computers, laptops and tablets. As a result people are started use of Smartphones and mobile phones in learning. But unfortunately mobile devices have constraints on processing power, storage and battery lifetime. Heavy E- learning applications cannot run on mobile devices so nowadays cloud computing technology is used in mobile phones called Mobile Cloud Computing. Running powerful E-learning applications on cloud and getting response to mobile devices we can run heavy applications on mobile phones. As application is running on cloud server large computations are executing on the servers so battery of mobile phone is saving automatically. Even if internal memory of mobile phones is not sufficient to run application still user can feel application is running on his personal device. Offloading concept is used in this technique [1]. User's data is not stored on his/her personal mobile phones instead data is stored on cloud storage.



**Fig. 2. Evolution of M-learning**



## 2. RELATED WORK

In this section we will see few existing laboratories for performing hands-on experiments in network security studies. This section provides summarized existing work and their advantages and drawbacks.

### A. Physical Laboratories

1. This is our traditional laboratories in which organization or institutions spend high amount on purchasing costly devices like routers, switches, hubs, firewalls and nodes, etc.
2. By using this labs students and researchers can perform their hands-on experiments on these

laboratories and will actual response from real hardware to the situation so more effective.

3. Cost is more. Reconfiguration and reconstruction is difficult. Maintenance cost is high.
4. Lab assistant is required for every setup.
5. Not flexible and scalable.

#### **B. Network Simulators(Simulation Software's)**

1. By using network simulators and simulation software's students and researchers can create their network as per requirements of the experiment; but these networks are not realistic networks.
2. Simulators are purely based on the software and independent to actual hardware devices.
3. Cost of simulators is less as compared to other laboratories.
4. However simulators do not provide actual interface and physical devices.

#### **C. Virtualized Application Laboratories**

1. These types of laboratories are built on concept of desktop virtualization.
2. In these types of laboratories hands-on experiments are restricted by already defined algorithms in software.
3. Problem solving and simulation is done using predefined algorithms.
4. Application data and status cannot keep on remote servers so students need to finish assignments in same session.

#### **D. Remote Desktop Laboratories**

- These types of laboratories are also called as shared-host laboratories.
- These types of laboratories are created on pool of computers and they can be used by students using remote desktop access protocol.
- Many students can access these computers concurrently for performing their experiments at the same time.
- Load balancing and security issues among students.
- Because of several students are accessing same computer for performing experiment which restricts the computer to be used for different purposes.

#### **E. Single Virtual Machine Laboratories**

1. Student can create multiple virtual machines on their own PC's or laptops and perform their network security experiments.
2. During any attack a particular virtual machine if crashed then student can create another new virtual machine or student can request for new virtual machine to server or remote machine.
3. Students can request any VM and release any VM at any time.
4. This type of approach is not suitable for complicated Multi VM networking system because central management portal is not supporting.

#### **F. Multi-VM Laboratories**

1. This type of laboratories takes advantages of cloud computing.
2. Multiple virtual machines are running in powerful servers.
3. Cloud provide multi virtual machine environment which allows student to make complicated and complex network.

4. These laboratories are not sufficient for performing network security experiments because of reconfiguration and isolation capabilities.
5. All VM's are running in same cloud server (XEN Server or KVM) so students are restricted to create only one network.
6. Most of the network security experiments are based on the multiple networks. So students are not able to perform all experiments using these types of laboratories.

### **3. PROPOSED ARCHITECTURE**

#### **3.1 Overview:**

This proposed laboratory architecture is developed for overcoming the drawbacks of Multi-VM based laboratories. As mentioned in section III Multi-VM laboratories are limited to single network only. Therefore students cannot perform multiple network based experiments using these laboratories. This restriction is overcome in this proposed architecture by using cloud servers cluster. Multi-VM and Multi network can be created using cloud servers cluster [2]. Several cloud servers are running concurrently and several VM's are running on each server. These servers are connected by using OpenStack. Students can download a V-lab android application for creating, re-configuring network setup. An Android application provides a drag-n-drop feature to create network as per requirement of experiment. After creating network setup student submit this network design to server and as per requested network cloud creates the required network. Further students can perform these network security experiments as shown in Fig. 4.

#### **3.2 An Android Application as a Front End:**

OpenStack and XEN Server are open source projects so they provided API's for developers those who want to make application based on cloud. Android is based on java language so using java API's we can create our virtual laboratory. Students can login using their username and password. After logged in successfully students can drag-n-drop several virtual machines hosts on the canvas and configure them as a router, switch, hub or DHCP server, HTTP server, FTP server as per requirements of experiment. After configuration is complete this can be submitted over internet to our backend.

#### **3.3 Creating Virtual Network with XEN Server:**

- a. Single Server Private Network:
  - This is an internal network.
  - Single server private network used for communicating several virtual machines on the specific Xen Server host.
  - Used internal virtual switch.
  - All Virtual Machines on same XEN Server.
- b. Cross Server Private Network:
  - It requires the distributed vSwitch and it allows internal Virtual Machines communication across Xen Server hosts.
  - Multiple XEN Servers.
- c. External Network:
  - A vSwitch bounded to a one physical adapter.

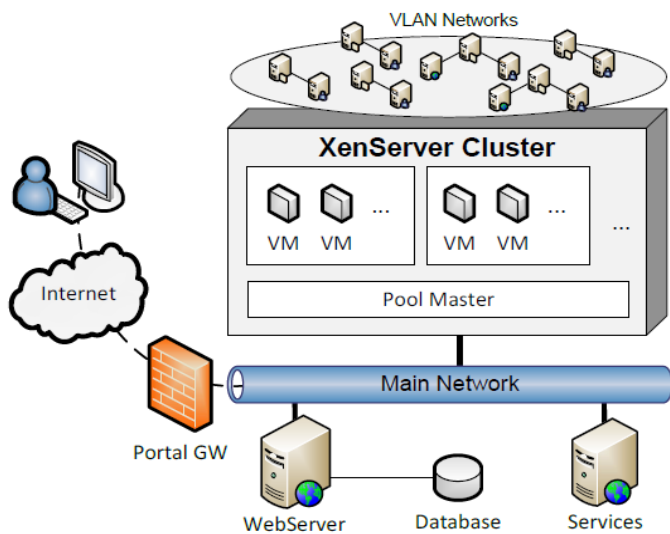
- External network used for communication with devices on the physical network.
- d. Bounded Network:
- A vSwitch bound to two physical adapter used to provide redundancy and load balancing [3], [7].
  - Bounded network used for communication with devices on the physical actual network.

1) 3.4 OpenStack

### 3.4 OpenStack:

- OpenStack is an operating system which is open source.
- OpenStack network management can allow static IP addresses or using DHCP server.
- Students are able to create their own specific networks, and OpenStack is takes responsibility to control traffic and connection to servers and resources to one or more multiple networks.
- Admin can take advantages of SDN (software defined networking) technology like OpenFlow to allow for high levels of multi-tenancy and massive scale.

OpenStack cloud technology has an expanded framework allowing additional network services such as load balancing, intrusion detection systems (IDS), firewall and VPN (Virtual Private Network) to be deployed and managed [4].



**Fig. 4. Proposed Architecture**

### 3.5 V-lab Back End

One of the important components of the proposed architecture is V-lab back end system. Two major subcomponents of the back end system are Xen Cloud Platform (XCP) and OpenStack. Xen Cloud Platform and OpenStack are open source cloud virtualization platforms. Several virtual machines are running in Xen Servers. Each Virtual Machine may be Windows XP, Vista, Windows 8 or Linux machine like Fedora, Ubuntu etc. Running Virtual Machine may be DHCP Server, FTP Server, Database Server, and HTTP Server or may be Firewall, Router, etc. There are several Xen Servers connected with each other by using the OpenStack. So using OpenStack we can create a cluster of Xen Servers therefore multiple networks and multiple virtual machines are ready for students to reconfigure the required network for network security experiments.

## 4. CONCLUSION

This research paper proposed new brand architecture for mobile virtual laboratory design. By using Xen Cloud Platform and OpenStack virtualization techniques we can create Multi-VM's Multi network mobile virtual laboratory. Android application as a front end therefore very attractive GUI with mobility makes these types of laboratories flexible. By using our own mobile phones or Smartphones students and researchers can perform the network security experiments at anywhere and anytime. This is very appropriate example of "Networks as a Service" so institutions and business organizations can make use of this architecture to create virtual laboratories for commercial purpose.

As compared to physical laboratories our mobile virtual laboratory is re-configurable, flexible, scalable, isolated, secure and cost efficient. Network security researchers and students can make use of these laboratories using mobile phones so no restrictions on location and time.

## 5. FUTURE WORK

In the future, interested users can work further on this proposed work to make this architecture highly available and can add redundancy features to provide more reliable platform. Researchers can use this same architecture to build a new mobile virtual laboratory for distributed system studies. Hands-on experiments are plays an important role in distributed system course. So modifying proposed architecture researchers can try to create mobile virtual laboratory for distributed system course.

Replacing Xen Server with KVM hypervisor researchers can build same mobile virtual laboratory and can compare these two implementations. Comparative studies of Xen Server based labs and KVM based labs will give important analytical results which may be beneficial for commercial products.

## 6. REFERENCES

- [1] Yugesh S.Bhosale and Dr.Jenila Livingstone L.M. "Mobile Cloud Computing for m-Learning applications" in International Journal of Engineering Research and Technology Vol. 3 Issue 2 in Feb. 2014.
- [2] L. Xu, D. Huang, and W. T. Tsai, "V-Lab: A Cloud-based Virtual Laboratory Platform for Hands-on Networking Courses," in *Proc. 17<sup>th</sup> Annu. ACM ITiCSE*, 2012.
- [3] <http://www.xenproject.org/developers/teams/xapi.html> Online Web reference.
- [4] <http://docs.openstack.org/api/openstacknetwork/2.0/content/POST/os-networks/v2.0/createNetwork/v2.0/networks/networks.html> online web reference.
- [5] H. E. Schaer, S. F. Averitt, M. I. Hoit, A. Peeler, E. D. Sills, and M. A. Vouk, "NCSU's Virtual Computing Lab: A Cloud Computing Solution," *Computer*, vol. 42, pp. 9497, 2009.
- [6] M. Wannous and H. Nakano, "NVLab, a networking virtualWeb-based laboratory that implements virtualization and virtual network computing technologies," *IEEE Trans. Learning Technol.*, vol. 3, no. 2, pp. 129–138, Jun. 2010.
- [7] Xen Virtualization Open Source Project." [Online]. Available: <http://xen.org>.
- [8] Virtual LAN Technology." [Online]. Available: [http://en.wikipedia.org/wiki/Virtual\\_LAN](http://en.wikipedia.org/wiki/Virtual_LAN).