DEVELOPING A SECURITY PROTOCOL FOR A WIRELESS COMPUTER VIRTUAL LABORATORY (WCVLAB)

EDWARD N. UDO
Department of Computer Science, University of Uyo, Uyo
Akwa Ibom State, Nigeria.
edwardudo@yahoo.com

IMO J. EYO
Department of Computer Science, University of Uyo, Uyo
Akwa Ibom State, Nigeria.

INI J. UMOEKA
Department of Computer Science, University of Uyo, Uyo
Akwa Ibom State, Nigeria

Abstract

For a Virtual Computer Laboratory (VCLAB) to operate effectively within a Wireless intranet setup, a lot of protocols are employed to function. This write-up is aimed at developing a protocol to secure a Wireless Computer Virtual Laboratory (WCVLAB) of any institution. The protocol developed secures a Wireless Computer Virtual Laboratory through an authentication server by supplying authentication parameters at registration, which will be stored to be used at login for comparison. Fingerprint is used to ensure that a user is who he or she claims to be. Duration for access is allotted for a user, after which initial parameters will be supplied for re-authentication. While a user is still logged-on, security questions will be posed intermittently to avoid spoofing. The methodology used for this research is Structured System Analysis and Design. Java Programming Language is used for coding the program and MySQL is the database tool. The result of the implemented system is a secured protocol that guarantees secured access. This is different from the security of other Computer Virtual Laboratory which uses only users name, pin or registration number.

Keywords: Security, Protocol, Wireless Computer Virtual Laboratory.

1. Introduction

The world is now in a new computer based age, one that can be called an “Age of Networked Intelligence” [Tapscott, 1996]. This is achievable through digital computer networks which interconnect multiple computers and other devices that are based on computer data [Wohorem, 2000]. These computers are connected using wireless technologies. The term wireless networking refers to a technology that enables two or more computers to communicate using standard network protocols, but without network cabling [Lammle, 2004].

With the development of new computer technologies and the World Wide Web (WWW), it is now possible to simulate engineering and science laboratory projects on a computer. With wireless intranet and internet access, it is now possible for students to be involved in laboratory exercises without being physically present in a traditional laboratory setting, rather through a virtual laboratory presence.

Traditional laboratories pose challenges from many aspects such as funding, space, support staff, etc. Consequently, it becomes necessary to design virtualized laboratories to eliminate the problems associated with traditional laboratory and in turn offer benefits such as effective utilization of computer laboratory resources, easy and quick configuration of multiple environments, and provision of access to external resources without permitting attacks to those resources.

To establish a virtual laboratory presence an Intranet is set up. An intranet is built from the same concepts and technologies used for the internet, such as client server computing and the Transmission Control

Protocol/Internet Protocol (TCP/IP) suite. Intranets are designed to permit access by users who have access privileges to the internal Local Area Network (LAN) of an organization. Within an intranet, Web Servers are installed in the network. Browser technology is used as the common front end to access information stored on those servers [Ward, 2003].

The word virtual has been applied to computing and IT with various meanings. It is the used of software systems that act as if they were hardware systems (virtual machine, virtual memory, virtual disk, etc) of computer generated simulations of reality [Border, 2007]. Virtual Laboratory is therefore a laboratory in which experiments and other laboratory exercises are stored in digital format and accessible by computers. Virtual laboratories use the power of computerized models, simulations and a variety of other instructional technologies to replace face-to-face lab activities [Gercek, 2006].

Creating a virtual laboratory (VLAB) does not ensure complete protection, since computer networks are typically shared resources used by many applications for many different purposes [Perterson, 2007]. Unauthorized access to company wireless and wired networks can come from a number of different methods and intents, some of which include, accidental association, malicious association, non-traditional networks, identity theft, man-in-the-middle attack, denial of service and network injection [Bardwell, 2005] and [Sickler, 2004]. Network computers can have their configuration changed, unauthorized students may log onto the server, other laptops with wireless Network Interface Cards (NIC) can access the wireless intranet, and students may use a laptop that is unprotected against viruses which may infect other computers causing problems in the Virtual Laboratory etc. Security issue is one of the detriments of virtual laboratory and therefore securing a wireless virtual laboratory remains a vital issue.

Security threats to a network give rise to one or more of the following security requirements for information that is transmitted over a network: privacy and confidentiality, integrity, authentication and nonrepudiation [Leon-Garcia, 2000].

In this write up, the use of biometric authentication in securing a virtual laboratory is introduced. Biometrics is defined as automated methods of identifying a person or verifying the identity of a person based on physiological or behavioural characteristics [Podio, 2002]. The basic processes of a biometric system are: Enrollment, Feature Extraction, Template Creation and Biometric Matching [Bubeck, 2003]. These processes are all embedded in the protocol development together with intermittent security questions and allotted time frame for enhanced protection.

Security is a function that needs to be tied primarily to the role of the person accessing networked systems. Apart from maintaining the security of critical systems, the individual computers used as access devices need to be protected. In a situation where most computers are connected to a single wireless Local Area Network or Wide Area Network, security architectures should be designed and implemented. Deployment of security architecture is now more important than ever as it allows for complex and secure interaction of multiple computer systems, communication protocols and other infrastructures over public and even private networks. To ensure comprehensive security, an organization must address all host systems, applications and networking devices with a policy that maximizes users' convenience and productivity, while at the same time blocking security violations [Asor, 2003].

This work is aimed at (i) developing a security protocol to authenticate WCVLAB users thereby reducing or eliminating incidents of unauthorized persons logging-on into the VLAB through spoofing or theft of access parameters (ii) deploying biometric authentication and security questions for enhanced security (iii) Analyzing and demonstrating the performance of the protocol developed.

1.1. *Methodology*

The use of effective and appropriate methods in facilitating projects enhances its effectiveness and efficiency. The method applied in this project is the Structured System Analysis and Design method where an existing system is studied to proffer better options to solving existing problems. In this research a security protocol to secure a Wireless Computer Virtual Laboratory is developed (using structured approach), tested and implemented within a computer system but at two different ends: the server and the client side. The result is of assurance that when used within a wireless intranet setup, it will work effectively.

2. User Identification/Authentication in Computer Vlab

Proper user identification/authentication is a crucial part of the access control that makes the major building block of any system's security. User identification/authentication of Computer Virtual Laboratory is in line with the traditional method which is based on:

(i) Something that the user knows (typically a PIN, password etc.)

(ii) Something that the user has (example a key, a token, a magnetic or smart card, a badge, a passport etc.)

These traditional methods of user authentication unfortunately do no authenticate the user as such traditional methods are based on properties that can be **forgotten, disclosed, lost or stolen**. Passwords often are easily accessible to colleagues and even users tend to pass their tokens to or share their passwords with their colleagues to make their work easier.

3. The Proposed Protocol

Security issues in VLAB stems from the user trying to hack into the wireless intranet, exchanging his/her password/registration number and/or other authentication details with other users. Introducing fingerprint technology into VLAB can help check some of these security issues. This therefore calls for the development of a protocol (software) to secure a Wireless Computer Virtual Laboratory that will deploy fingerprint as part of users' authentication. The protocol will among other things perform the following:

i. Allow users to supply parameters for registration into the VLAB
ii. Accept biometric samples and match against stored samples
iii. Allocate time slots for users of the VLAB
iv. Pose security questions for enhanced security
v. Allow users access into the Wireless Computer Virtual Laboratory.

3.1 *Authentication in the Proposed System*

The protocol developed to secure a Virtual Computer Laboratory would authenticate users using **biometrics and intermittent pop-up screen** posing questions to the users from a pool of the security questions supplied at registration, to avoid spoofing. That is the proposed protocol is designed such that for the virtual laboratory user to be authenticated, identification parameters will be supplied along with security questions and the user's finger print.

When the user has logged-on to the Computer Virtual laboratory, a time slot is given to each access. At the expiration of the allotted time, the user is automatically logged-out, with a prompt requesting from the user whether he/she needs more time. If **yes**, the user will be prompted to login again, with transfer of operations to where he/she was before the time expired. If **no,** the session will terminates finally.

3.2 *System Design*

The protocol developed is designed on the Java platform as a standard Java desktop (network) application that runs on any operating system with the appropriate Java Virtual Machine (JVM) specific to that operating system. The application is made up of two ends: The client application and the server application. The client application (VirtualLab Client) can be hosted on the user's computer which is part of a wireless intranet while the server application (VirtualLab Server) can be hosted on any computer on the same network (intranet). The client application as well as the server application interacts with the database.

The client interface presents the input environment for Virtual Laboratory users to register to use the VLAB by supplying required details to the database and the environment for login to validate users' credentials for access into the VLAB. The server interface provides the environment to administer the session time and monitors processes such as number of connected clients, number of request, number of submitted assignment etc

3.3 *System Flow Diagram*

The overview of the entire system is represented diagrammatically in figure 1 below:

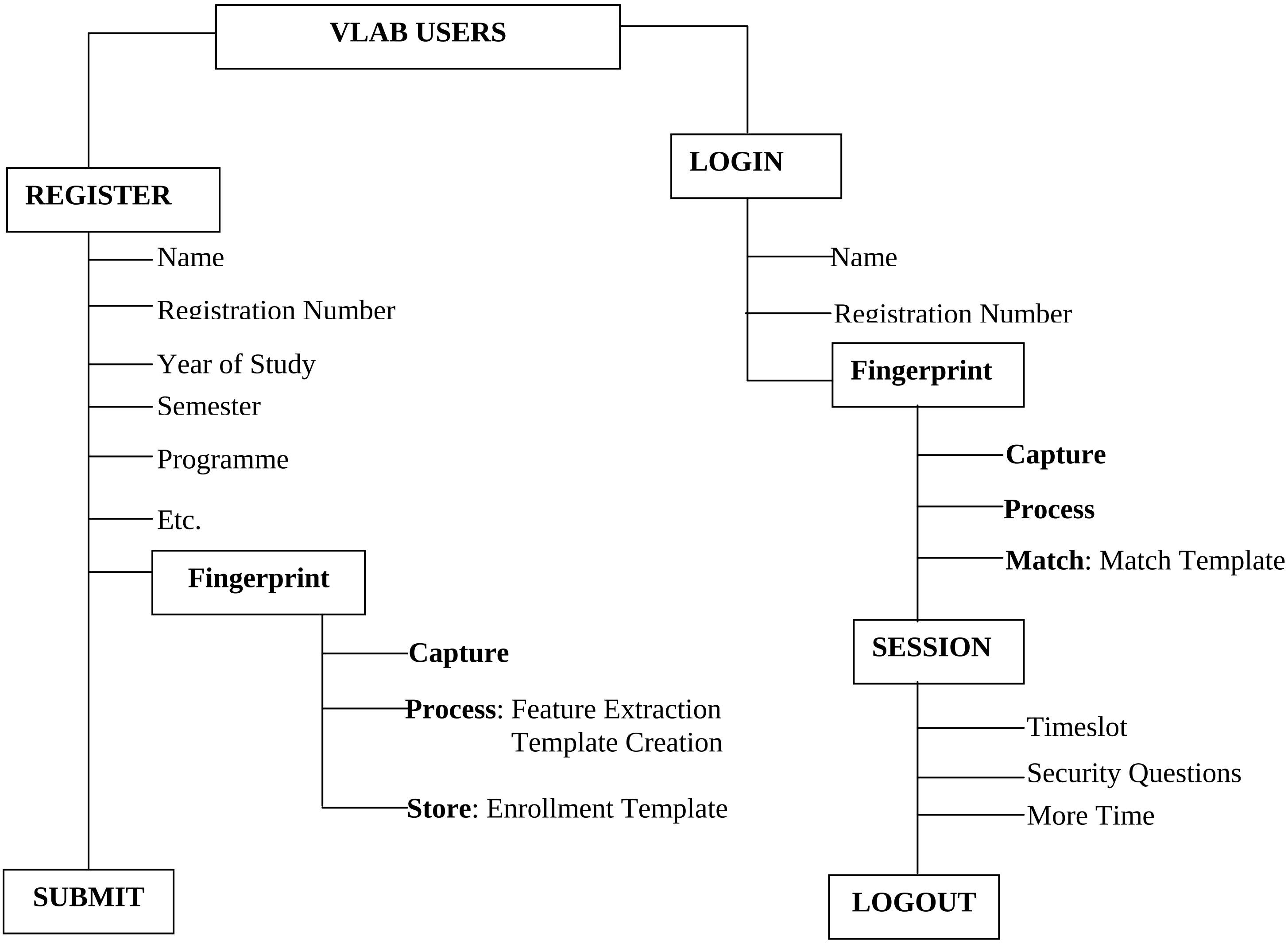


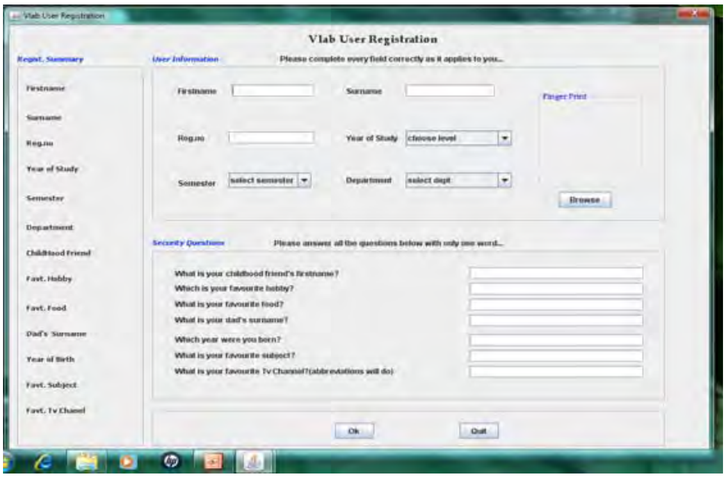
Figure 1 – Diagrammatical Overview of the System

4. Implementation

Users' authentication parameters, including fingerprints are gotten from intending users and stored in a database. Anytime a user is to access the Virtual laboratory, the user input will be re-collected and matched against the database. Access is granted to a user who has passed the authentication.

4.1 *Input Data*

The input data to the system is captured when a student registers to use the Computer Virtual Laboratory. Some of the input data is as shown in the screen below:



Vlab User Registration

Vlab User Registration

Regist. Summary

Firstname

Surname

Reg.no

Year of Study

Semester

Department

Childhood Friend

Favt. Hobby

Favt. Food

Dad's Surname

Year of Birth

Favt. Subject

Favt. Tv Chanel

User Information — Please complete every field correctly as it applies to you...

Firstname

Surname

Reg.no

Year of Study: choose level

Semester: select semester

Department: select dept

Security Questions — Please answer all the questions below with only one word...

What is your childhood friend's firstname?

Which is your favourite hobby?

What is your favourite food?

What is your dad's surname?

Which year were you born?

What is your favourite subject?

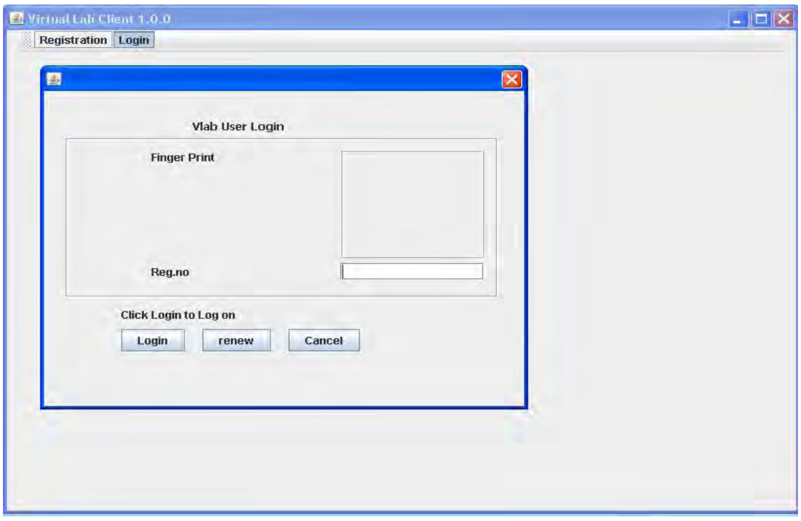
What is your favourite Tv Channel?(abbreviations will do)

Figure 2 - Registration Page

The data required to be supplied form the different fields in the database. The security questions form part of the input data into the system, which after a while into a session will be scrambled and posted to a user who has been granted access to be sure the user is still the one who was earlier authenticated.

4.2 *Login*

At registration, the captured data is stored in the database against each registered user. A user logs-on by supplying his/her registration number and fingerprints, which will be matched against the stored samples. The finger print will be captured through a fingerprint scanner. The login screen is as shown in the figure below:



Virtual Lab Client 1.0.0

Vlab User Login

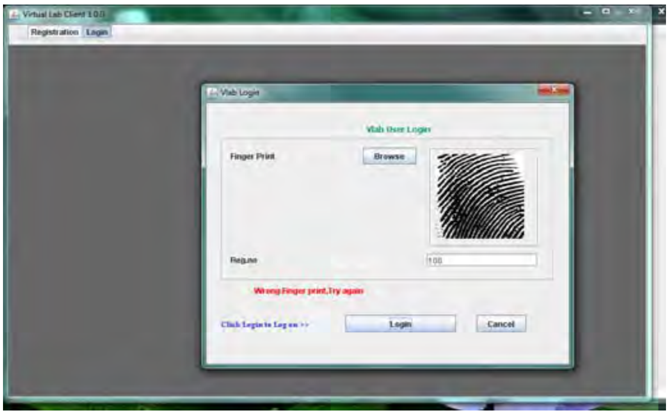
Finger Print

Reg.no

Click Login to Log on

Figure 3 - Login Screen

The renew button is used if the thumbprint was not properly captured and wish to be recaptured. Login operation can equally be cancelled by clicking the cancel button. If the fingerprint does not match the one stored in the database, the user will see a prompt “wrong fingerprint. Try again”.



Reg.no: 100

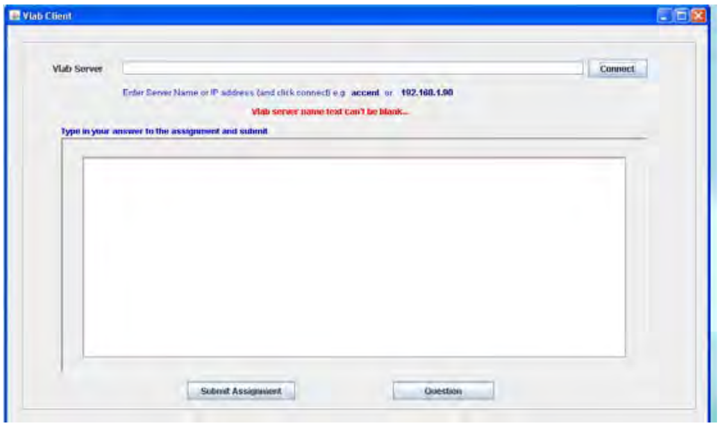
Wrong Finger print,Try again

Click Login to Log on >>

Figure 4 -Incorrect Login Screen

4.3 *Accessing the Server*

When a user has successfully logged on into the VLAB, he/she must supply the name or IP address of the server to be accessed in order to get the questions or submit an assignment. If the server parameter supplied is not valid, the user will receive a prompt to that effect.

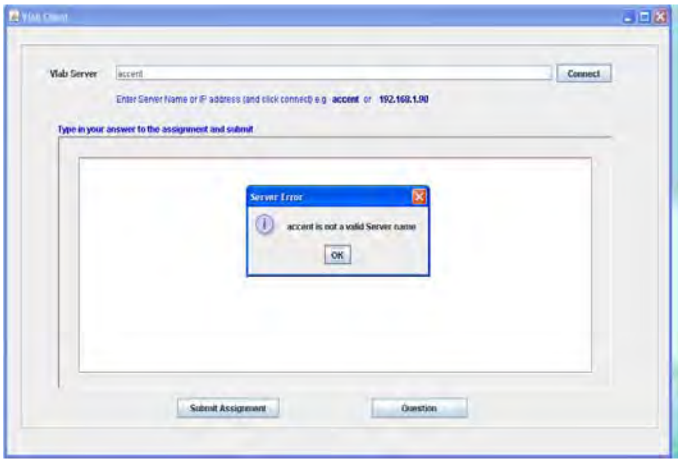


Enter Server Name or IP address (and click connect) e.g accent or 192.168.1.90

Vlab server name text can't be blank...

Type in your answer to the assignment and submit

Figure 5a – Screen showing the parameters a user must supply to connect to server for questions and assignment.



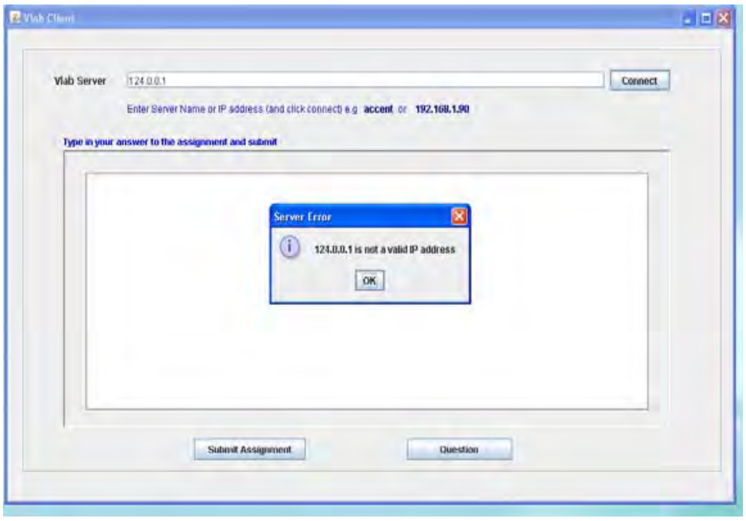
Vlab Server: accent

Enter Server Name or IP address (and click connect) e.g accent or 192.168.1.90

Type in your answer to the assignment and submit

accent is not a valid Server name

Figure 5b – Prompt for incorrect server name



Vlab Client

Vlab Server 124.0.0.1 Connect

Enter Server Name or IP address (and click connect) e.g **accent** or **192.168.1.90**

Type in your answer to the assignment and submit

Server Error

124.0.0.1 is not a valid IP address

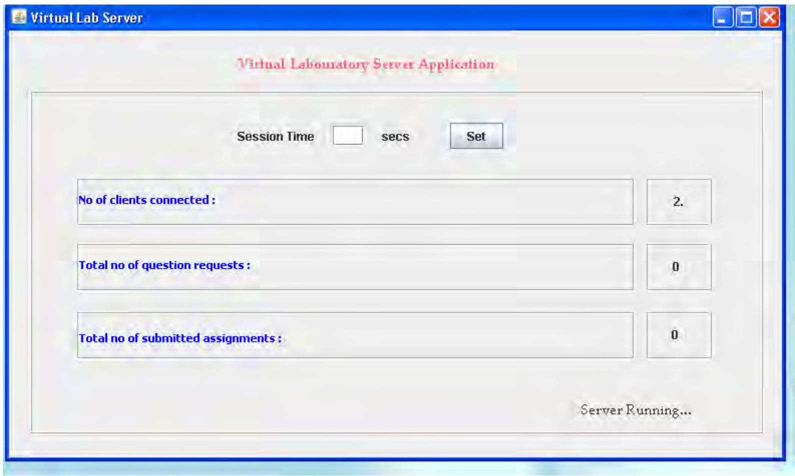
OK

Submit Assignment Question

Figure 5c – Prompt for incorrect IP Address

4.4 *Session Time*

A VLAB Administrator, at the VLAB server application end, must set the amount of time (in seconds) that will elapse before security questions are posted to the user. The default time is 20 seconds. If a VLAB Administrator clicks on Reset Button, the session time will be set to the default. The VLAB Administrator can also monitor the number of clients connected, total number of questions requested and total number of assignments submitted.



Virtual Lab Server

Virtual Laboratory Server Application

Session Time secs Set

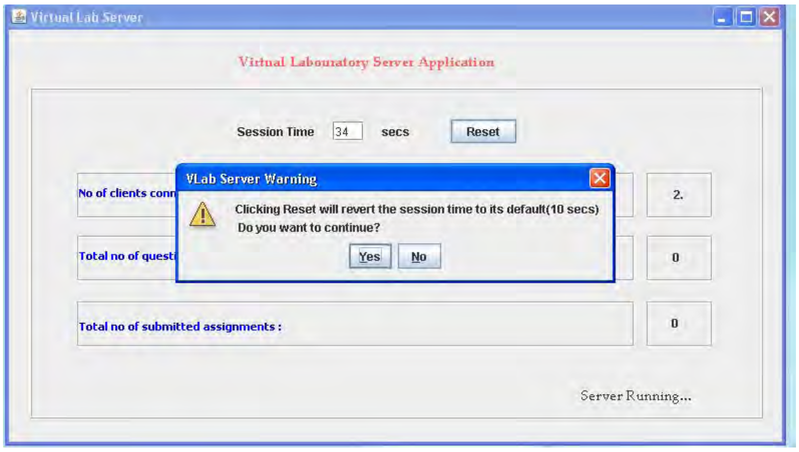
No of clients connected : 2.

Total no of question requests : 0

Total no of submitted assignments : 0

Server Running...

Figure 6a – VLAB Server Application end for VLAB Admin.



Virtual Lab Server

Virtual Laboratory Server Application

Session Time 34 secs Reset

No of clients conn 2.

Total no of questi 0

Total no of submitted assignments : 0

VLab Server Warning

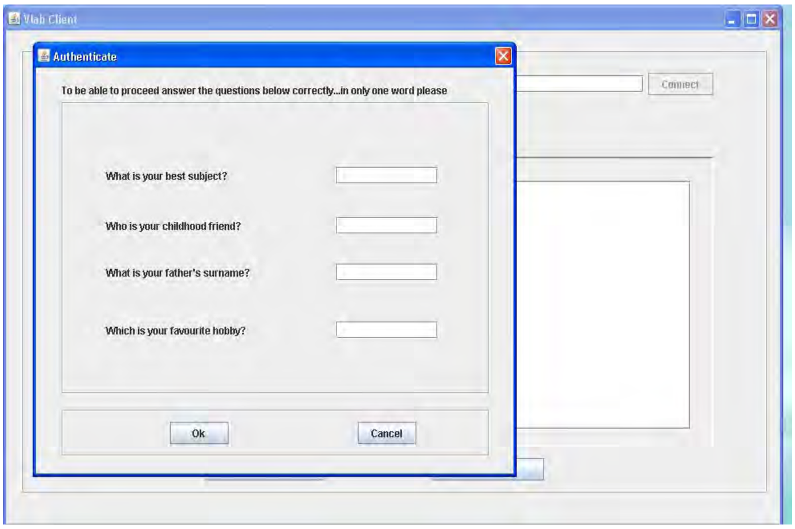
Clicking Reset will revert the session time to its default(10 secs)
Do you want to continue?

Yes No

Server Running...

Figure 6b – Prompt showing when Reset Button is clicked

During the session time allotted to a user, security Questions, selected from those answered at registration, will be posed from the database to the user, to be sure the user who logs-on is still the one accessing the VLAB. On re-supplying the correct answers earlier given at registration, the user will still be allowed to log-on else the user will be logged-out.



To be able to proceed answer the questions below correctly...in only one word please

What is your best subject?

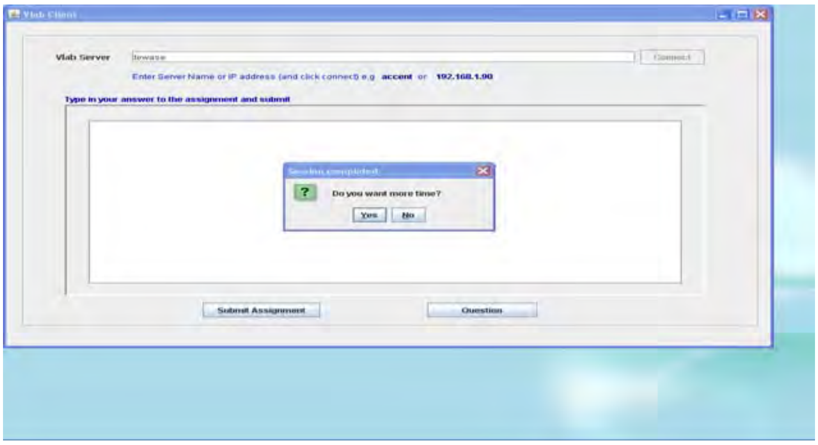
Who is your childhood friend?

What is your father's surname?

Which is your favourite hobby?

Figure 7a – Screen showing Security Questions selected from Database

At the expiration of the session time, the system will logs out the user with a prompt finding out whether the user needs more time. If more time is needed, the system will re-logs-in the user, but return him/her to the operation point at which the time expired.



Vlab Server lewase

Enter Server Name or IP address (and click connect) e.g **accent** or **192.168.1.90**

Type in your answer to the assignment and submit

Do you want more time?

Figure 7b – prompt asking a user whether more time is needed

5 Conclusion

In this paper, developing a security protocol for wireless computer virtual laboratory has been presented. The primary motive for this paper has been achieved through the use of fingerprints authentication and intermittent pop-up screen for user verification. This method is used in addition to the traditional parameters employed to authenticate users in a virtual laboratory. These traditional parameters include name, registration number etc. The method adopted is different from other methods of securing a virtual laboratory which are based only on something that the user knows or has (traditional method). The developed protocol is therefore superior as it uses biometrics for users' authentication and is economical, simple, easy to use and users' friendly

REFERENCES

[1] Asor, Vincent E. (2003**):** On Design and Deployment of Information Security Architecture. Proceeding of the Nigeria Computer Society (NCS), Volume 14, June 2003, 388 -395

[2] Bardwell, J. and Akin, D. (2005): CWNA Official Study Guide (3rd Edition). McGraw-Hill, page 45

[3] Border, Charles**,** The Development and Deployment of a Multi-user Access Virtualization System for Networking Security and System Administration Classes. Proceedings of the 38th Technical Symposium on Computer Science Education, Covington, Kenturky, USA, 2007, 576 – 580

[4] Bubeck, U. and Sanchez, D. (2003): Term Project, Dan Diego State University

[5] Gercek, G. and Naveed, S. (2006): Designing a Versatile Dedicated Computing Lab to Support Computer Nerwork Courses: Insights from a case study. Journal of Information Technology Education, Volume 5, 2006, 13 – 26

[6] Lammle, Todd (2004): CISCO Certified Network Associate Study Guide (4th Edition). Sybex Inc., 1151 Marina Village Parkway, Alameda.

[7] Leon-Garcia, A. and Widjaja, I. (2000): Communication Networks, Fundamental Concepts and Key Architectures. McGraw Hill Higher Education, Boston Burr Ridge, New York

[8] Peterson, Larry L. And Davies, Bruce S. (2007**):** Computer Networks, a Systems Approach. Morgan Kaufmann Publishers, 340 Pine Street, Sixth Floor, San Francisco, USA

[9] Podio, Fernado L. and Dunn, Jeffrey S. (2002): Biometric Authentication Technology: From the Movies to your Desktop, Convergent information Systems Division

[10] N. Sickler, E. Kukula and S. Elliot (2004): The Development of a Distance Education Class in Automatic Identification and Data Capture at Purdue University, in World Conference on Engineering and Technological Education, Santos, Brazil.

[11] Tapscott, D. (1996); The Digital Economy. Promise and Peril in the age of Digital Intelligence. McGraw Hill, New York.

[12] Ward, T. (2003**):** Planning an Intranet Model for success Intranet. http://www.presidentdigital.com/articles/intranetarticles/intranet planning-an-intranet-model-for-success. (last visited, June 2009)

[13] Wohorem, Evans E. (2000): Information Technology in the Nigeria Banking Industry. Spectrum Books Ltd, Spectrum House, Ring Road, Ibadan, Nigeria