**BIOINFO Security Informatics**
ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, 2012, pp.-33-36.
Available online at http://www.bioinfo.in/contents.php?id=344

# IMPLEMENTATION OF SECURITY PROTOCOL FOR WIRELESS COMPUTER NETWORK

**WATANE H.N.[1*] AND GAWANDE A.D.[2]**

[1]Department of Computer Science & Engineering, Sipna's COET, Amravati, MS, India.
[2]Department of I.T., Sipna's COET, Amravati, MS, India.
*Corresponding Author: Email- hwatane@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

**Abstract-** Implementing security protocol for wireless computer network we require effective Wireless intranet setup, many protocols are working to function. This thing is focused at developing a security protocol to secure a Wireless Computer network of any institution. The protocol developed to secures a Wireless Computer class-room through an authentication server by supplying authentication constraint at registration process, which is used at login for comparison then it will be stored. Fingerprint is used to make sure that a user is who claims to be. Time duration for access is allotted for a user, after which primary constraint will be supplied for re-authentication. While a user is still logged-on, some security questions will be posed intermittently to avoid counterfeiting. The methodology used for this research is Structured System Analysis and Design (SSAD). For coding the program Java Programming Language is used and MySQL is the database tool. The final result of the implemented system is a secured protocol that guarantees secured access. This is different from the security of other wireless virtual class-room which uses only users name, pin or registration number.
**Keywords-** Security, Protocol, Wireless intranet, virtual class-room

**Citation:** Watane H.N. and Gawande A.D. (2012) Implementation of security protocol for wireless computer network. BIOINFO Security Informatics, ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 1, 2012, pp.-33-36.

**Copyright:** Copyright©2012 Watane H.N. and Gawande A.D. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

## Introduction

The recent era is of computer based network intelligence. This is feasible through digital computer networks which intercommunicate multiple computers and other devices that are based on computer data [1] For connecting these computers wireless technologies are used. Wireless networking based on the technology which enables two or more computers to communicate using standard network protocols, and there is no need of network cabling.

The development of new computer technologies and the World Wide Web, it is now possible to suggest engineering and class-room projects on a computer. With wireless intranet and internet access, it is now possible for students to be involved in class-room exercises without being physically present in a traditional class-room setting. Usually class-room pose challenges from many aspects such as funding, space, support staff, etc. subsequently, it becomes necessary to design virtualized class-room to eliminate the problems associated with traditional class-room and in turn offer benefits such as effective utilization of computer class -room resources, easy and quick configuration of multiple environments.

To establish a virtual class-room an Intranet set up is required. Client server computing and the TCP/IP are conceptual technologies, which are used to build such internet based system. Intranets are designed to permit users access who has authentication to the internal Local Area Network of an institute. Within an intranet, Web Servers are installed in the network. Typically we used the common front end to access information stored on those servers is Browser technology.

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) [2]. Virtual Class-room are class-rooms in which exercises and tutorial are stored in digital format and accessible

by computers. Power of computerized models are used by virtual class-room, simulations and a variety of other instructional technologies to replace face-to-face class-room activities [3]. Due to shared resources of computer network Creation of a virtual class-room does not ensure complete protection [4]. Unauthorized access to 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 [5, 6].

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 Class-room etc. Security issue is one of the detriments of virtual class-room and therefore securing a wireless virtual class-room remains a important issue. Security requirements for transmitting information over a network to overcome Security threats are: privacy and confidentiality, integrity, authentication and non-repudiation [Leon-Garcia, 2000]. In this paper, the use of biometric authentication in securing a virtual class-room is introduced.

In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.

Biometrics is defined as automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics [7]. The basic processes of a biometric system are:

Enrolment, Feature Extraction, Template Creation and Biometric Matching [8].

The process includes embedded protocol development together with one or more security questions and allotted time frame for enhanced protection. Security is a main function that needs to be fixed primarily to the role of the user accessing networked computer systems. The individual computers used as access devices need to be protected instead of maintaining the security of critical systems. Here we can design and implemented security architecture for most computers which are connected to a single wireless Local Area Network or Wide Area Network.

Deployment of security architecture is now much more essential because it allows for complex and secure interaction of multiple computer systems, communication protocols and other infrastructures over public and even private networks. To ensure broad security, an institution must address all host systems and networking devices with a strategy that maximizes users ease and productivity, on the other hand blocking security violations [9]. This work is going to

i. Developing a such security protocol to authenticate Wireless Computer Virtual CLASS-ROOM users thereby eliminating incidents of unauthorized persons logging-on into the Virtual CLASS-ROOM through spoofing or theft of access parameters
ii. In order to enhanced security, biometric authentication and security questions are deployed.
iii. The performance of the protocol developed is further analyzed and demonstrate

**A. Methodology**

The use of effective and appropriate methods for developing projects, enhances its effectiveness and efficiency .To solve existing problems we uses Structured System Analysis and Design method. In this research paper a security protocol to secure a Wireless Computer Virtual Class-room is developed, tested and implemented within a computer system at two different ends: the server and the client side. It result a wireless intranet setup , will work effectively.

**User Identification/Authentication in Computer Virtual class-room**

The major building block of any system's security is a proper user identification/authentication which is a crucial part of the access control system. User identification/authentication of Computer Virtual Class-room is corresponding to 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 passport etc.) As traditional methods are based on properties that can be forgotten, lost or stolen. These traditional methods of user authentication unfortunately do not work. Passwords often are easily accessible to colleagues or share their passwords with their colleagues to make their work easier.

**The Proposed Protocol**

Security issues in the Virtual CLASS-ROOM come from user trying to hack into the wireless intranet, exchanging password or registration number with other users. Introducing biometric authentication technique as fingerprint technology, which can help into Virtual CLASS-ROOM to check out some security issues? Because this things we develop security protocol (software) to secure a Wireless Computer Virtual Class-room which use users authentication by fingerprint technology. Things that can be performed by protocol are:

i. Initially we allow users to give parameters to registered into the Virtual CLASS-ROOM
ii. Accept biometric samples (fingerprint) and match it with stored samples.
iii. Assign time slots for users of the Virtual CLASS-ROOM
iv. In order to enhanced security, security questions are posed
v. Allow users access into the Wireless Computer Virtual Class-room.

**A. Authentication in the Proposed System**

By using biometric and pop-up screen we developed protocol to secure virtual computer class-room and it authenticates users and then asks some questions which are answered by user during registration Secure to avoid spoofing. That is the proposed protocol is designed such that for the virtual class-room user to be authenticated, identification parameters will be supplied along with security questions and the user's finger print. When 1st time the user logged-on to the Virtual class-room, 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 more time will be needed. If Y, the user will be prompted to login again. If N, the session will terminates finally.

**B. System Design**

The Security protocol designed and developed which is based on

the Java platform as a standard Java desktop, that application can runs on any operating system like window with the appropriate Java Virtual Machine precise to that operating system. The application is having two ends: The client application and server application.

The Virtual Class-room Client can be hosted on the user's computer which is part of a wireless intranet while the Virtual Class-room Server can be hosted on any computer on the same intranet. The client and server application interacts with the database. The input atmosphere is provided by client interface for Virtual Class-room users to register and use it by supplying required details to the database and the environment for login to validate users identification for access into the Virtual CLASS-ROOM. The server interface provides the atmosphere to administer the monitors processes and session time such as number of connected clients, number of submitted tutorials, number of request, etc

### C. System Flow Diagram

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

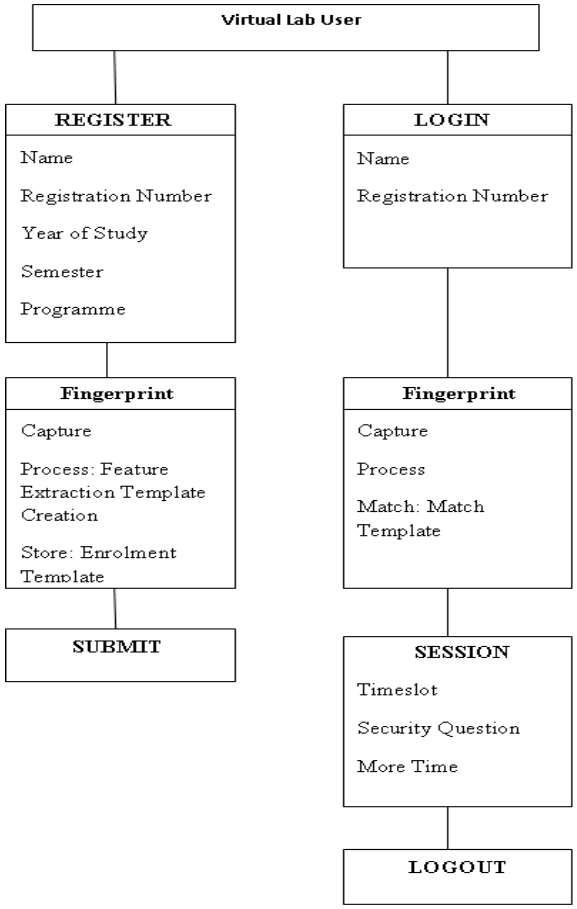


**Fig. 1-** System flow diagram

### Implementation

Users' authentication parameters, including fingerprints are taken from users and stored it in a database. Anytime a user is to access the Virtual class-room, the user input will be re-collected and matched against the database. Access is granted to a user who has passed the authentication. If fails access is denied.

### A. Input Data

The input data to the system is captured when a student registers to use the Computer Virtual Class-room. 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 twisted and post to a user who get grant to access virtual class-room this is for the user who still the one which was earlier authenticated.

### B. Login

At login process, the captured data is stored in the database against each registered user. A user logs-on by supplying user registration number and fingerprints, which will be matched against the stored fingerprint pattern. The finger print will be captured through a fingerprint scanner, hardware device. The renew button is used if the print was not properly captured and wish to be recaptured. Cancel button is provided to cancelling login operation . If the fingerprint does not match the one stored in the database, the user will see a message "Miss Match Fingerprint. Try once again".

### C. Accessing the Server

When a user has successfully logged on into the Virtual CLASS-ROOM, it must supply the name or IP address of the server to be accessed in order to get the questions or submit an tutorials. If the server constraint supplied is not valid, the user will receive a prompt.

### D. Session Time

A Virtual CLASS-ROOM Administrator, at the Virtual CLASS-ROOM server application end, must set the amount of time (in sec) that will elapse before security questions are posted to the user. The default time is 30 seconds. If a Virtual CLASS-ROOM Administrator clicks on Reset Button, the session time will be set to the default. The Virtual CLASS-ROOM Administrator can also monitor the number of clients connected, total number of questions requested and total number of tutorials submitted.

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 Virtual CLASS-ROOM. 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. 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.

### Conclusions

The major purpose for this paper has been achieved through the use of fingerprints authentication and intermittent pop-up screen for user verification. Developing a security protocol for wireless computer virtual class-room has been presented. This method is used in addition to the traditional constraints employed to authenticate users in a virtual class-room. These traditional constraints include user name, user registration number etc. The method adopted is different from other methods of securing a virtual class-room which are based only on something that the user knows. The developed protocol is therefore superior as it uses biometrics

technology for users' authentication and is economical, simple, easy to use and users' friendly.

**References**

[1] Wohorem Evans E. (2000) *Information Technology in the Nigeria Banking Industry*. Spectrum Books Ltd, Spectrum House, Ring Road, Ibadan, Nigeria.
[2] Border Charles (2007) *38th Technical Symposium on Computer Science Education*, Covington, Kenturky, USA, 576-580.
[3] Gercek G. and Naveed S. (2006) *Journal of Information Technology Education*, 5, 13-26.
[4] Peterson Larry L. And Davies Bruce S. (2007) *Computer Networks, a Systems Approach*.
[5] Bardwell J. and Akin D. (2005) *CWNA Official Study Guide* (3rd Edition). McGraw-Hill, 45.
[6] Sickler N., Kukula E. and Elliot S. (2004) *World Conference on Engineering and Technological Education*, Santos, Brazil.
[7] Podio Fernado L. and Dunn Jeffrey S. (2002) *Biometric Authentication Technology*.
[8] Bubeck U. and Sanchez D. (2003) *Term Project*, Dan Diego State University.
[9] Asor Vincent E. (2003) *Proceeding of the Nigeria Computer Society (NCS)*, 14, 388 -395.
[10] Udo E.N., Eyo I.J., Umoeka I.J. (2012) *Developing a Security Protocol For a Wireless Computer Virtual Laboratory*.
[11] Lammle Todd (2004) *CISCO Certified Network Associate Study Guide* (4th Edition). Sybex Inc., 1151 Marina Village Parkway, Alameda.
[12] Leon-Garcia A. and Widjaja I. (2000) *Communication Networks, Fundamental Concepts and Key Architectures*. McGraw Hill Higher Education, Boston Burr Ridge, New York.
[13] Tapscott D. (1996) *The Digital Economy. Promise and Peril in the age of Digital Intelligence*. McGraw Hill, New York.
[14] Ward T. (2003) *http://www.presidentdigital.com/articles/intranetarticles/intranet* planning-an-intranet-model-for-success.