Automation of Lab with Attendance Monitoring, Screen Capturing and Performance Analysis

P. Rajesh Kanna¹, S. Keerthi²

¹Assistant Professor, Department of Computer Science and Engineering, M.Kumarasamy College of Engineering, Karur
rajeshkannap.cse@mkce.ac.in, keerthisridhar77@gmail.com

Abstract—Network security is the authorization of access to data in a network, which is controlled by the network administrator and protecting the computer systems in the network from unwanted intrusions. Users are assigned with their credentials that allow them access to information and applications within their authority. A number of lab management software is available these days. In these software’s the desktop of the client/student machines is captured and the attendance is recorded using client login. The login and logout time of the client/student is not recorded. The softwares that are used for lab management is expensive. The system is developed with the aim to overcome the drawbacks of the existing applications. The Staff can access the server system by using their credentials. The staff can create the student’s account by providing credentials which is done by uploading an excel sheet in the server instead of manual work. The credentials in the database are used for student login. When the student logs in; their login details will be stored in the database which can be used for attendance generation. The client system will be shutdown automatically if it is idle for certain amount of time. The performance of the client system can be analyzed by using the log file generated in the server.

Keywords—Server, Client, Screen Capturing, Attendance Monitoring, System Performance

I. INTRODUCTION

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats. Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned with an ID and password or other authenticating information that allows them access to information and programs within their authority. At present the computer lab becomes a more integral part of education and it became the hub of activity. The Staff who needs instructional and technical assistance can find it in the computer lab. As professionals maintain a computer lab, many things may fall under jurisdiction from system allocation to monitoring the student’s activities. Here are some great management ideas to help keep a computer lab run smoothly throughout the year. The Staff can monitor the client/student system. The staff can generate the student’s lab
attendance such as login and logout details. At the same time the server can analyze the system performance.

II. LITERATURE SURVEY

The Computer Lab Monitoring System is developed to automate the Students Practical Session by Client Server Protocol [1]. Once the server is started the client send request to the server by using the server IP. Students submit their program to the server and the staff can easily view the work done by the students from the server and analyze the result.

Remote Lab Monitoring is implemented to monitor activities of the student over a LAN. [2]. Whenever student logs-in to the system then their attendance is automatically recorded in the database and student’s desktop can be viewed from the server by the staff. Files can be shared by the staff to the students through the server.

The lists of clients connected with the server are displayed in the server using RMI mechanism [3]. Instead of displaying the student’s desktop live on the server it will just list out only the currently running processes.

A secure Personal Computer Network Monitoring System is proposed to monitor the working between the handheld devices and the personal computer over Wi-Fi [4]. Sharing data in remotely monitoring PC or handheld devices over Wi-Fi, 3G and Bluetooth is insecure. To secure the data wireless protocol such as WPA/WPA2 is used.

Lab Automation using Remote Desktop is an application developed for the improvement of the lab sessions [5]. The staff can share the files to the students through the server. The students desktop can be viewed in the server. The student attendance is recorded during the practical lab slots.

Smart Lab is a LAN based application developed for improving the effectiveness of lab sessions [6]. The desktop of the client systems are displayed in the server. File sharing can be done by the staff through the server. Sending quick messages, freezing the PCs, blanking out the screens etc are available. If the student’s system is idle for certain amount of time then the server will automatically shut down the system.

III. EXISTING SYSTEM

The existing system uses a client server implementation model where one system acts as a server and all other acts as a client. The server and client systems are accessed by the staff and the students respectively by using their credentials respectively. The student’s login details are recorded in the database which is further used for attendance generation. The students system can be viewed in the server. Files can be shared to the students from the server.

IV. DRAWBACKS

The staff cannot know which system is used by a particular student as the IP address of the student’s system is not recorded. The login and logout time of the students are not recorded. The student account is created manually by the staff. The screen capture of client systems is done without displaying the user name of the student who uses the system. The Client system performance is not analyzed.

V. PROPOSED SYSTEM

To avoid the drawbacks in the existing system, the proposed system is designed as a computerized one with security features ensured where one PC in the lab acts as a server and others act as a client. Fig.1. represents the architecture of the proposed system.

![Fig. 1 Proposed Architecture](image_url)

The Staff can access the server system by using their credentials. The staff can store the student’s details in the database by uploading an excel sheet in the server. The credentials in the database are used for student login. When the student logs in; their details such as id, name, department, year, login time, logout time, IP address and laboratory name are automatically fetched by the server and it will be stored in the database which can be used for attendance generation. The
student desktop along with the username can be viewed by the staff from the server. The client system will be shutdown automatically if it is idle for certain amount of time. The performance of the client system can be analyzed by using the log file generated in the server when the student login.

VI. MODULE DESCRIPTION

The modules of the proposed architecture are described below, which includes attendance monitoring, Screen Capture, System Performance etc.

A. Admin

The Server is used to process the incoming client requests. The Staff should log in to the server system by using their credentials. The connection between the server and client (student’s system) should be established for further processing. Fig. 2. describes the functionalities of the server.

![Fig. 2 Server Home Page](image)

The Staff can upload the student details in an excel sheet into the SQL server which can be further used for attendance generation of the students. The fields in the excel sheet should match with the fields already defined in the database. Fig.3 shows the excel sheet upload of student details.

![Fig. 3 Excel sheet upload](image)

After successful establishment of the connection between the server and the client, whenever the student logs in to the system the server gets a notification and stores the login details of the particular student in the database. The IP address in the database helps the staff to identify the system and laboratory used by the student. The logout time of the student gets updated in the database when they log out. Both the login time and the logout time are fetched from the system by using the function System.DateTime.Now().ToString().

B. Client

The name and id of the students in the database act as their credentials to grant access to the client machine. The client application which will display the student login screen is added to the start up in the windows of the client machine. The client system cannot be accessed without the correct credentials. It will throw an error as “incorrect login” when the credentials doesn’t match. The student will get a socket exception “unable to connect to the receiver” when the connection is not established correctly between the server and the client.

![Fig. 4 Client Login Screen](image)

No other student can log in the system unless the student who logged in already logs out of the system. The client system automatically gets shutdown by the server if the system is idle for certain amount of time.
Fig. 4. shows the client login screen which pops out when the client system is turned on. The students can access the system by using their credentials. They have to choose the laboratory name in which they are going to work. These details are checked against the data stored in the database and access is granted if they match.

C. Attendance

The client application which will display the student login screen is added to the start up in the windows of the client machine. And so the student login screen is popped out in the client machine asking for the credentials at once the student turned on the system.

The login authentication of each student is stored in the database. After the login process, the student can view the desktop of an operating system. In this verification process the date and time details are updated in the server database along with the student name, register number, laboratory name and ip address of the system.

The server always listens to client when the student logs out; it gets updated in the database. The attendance of each student is recorded easily. This reduces manual entry of students in the lab register using the laboratory.

D. Screen Capture

On successful login of the student in the client machine, the desktop of that student’s client machine can be viewed by the staff in the server machine.

E. System performance

System performance analyses the performance of the system which includes the response time for a given work, utilization of resources and the data transmission time. This process is done by comparing the log files created in the server.

The performance of the client systems is fetched by using the performance information and tools functionality in the control panel. The system performance table displays the processor, memory (RAM), primary hard disk, graphics, gaming graphics and the name of the client system. Fig. 7 shows the performance details of the client system.

This feature helps in analyzing the performance of the client systems from the server. The lab assistant does not want to go and check each and every system in the lab.
VII. RESULT AND FUTURE WORK

We have implemented the attendance recording of students and screen capturing of student systems. Attendance is recorded with the help of client login which will record the name, roll no, department, course name, ip of the system and the date and time of login and logout. The screen capture of student systems is done by using the logged in user name of a particular system. The systems that are idle for certain amount of time are shutdown automatically by the server with a pop up message. Files are shared to the students by the staff through the server. The performance of the system is analyzed by the log file generated in the server when the student login.

In future, we have planned to implement Proxy login; it can be avoided by providing time limitations for attendance entry. An Alert message can be generated on the server when the student tries to open the application that is listed out in the blacklist.

REFERENCES


