Techniques of Enhancing usage Management of a Local Area Network of a Higher Educational Institution

Nikhil Sharma

Abstract*: : Managing the usage of Local Area Network is an important task as it helps in maintaining the productivity of the LAN There exists tools for this purpose and most of them are web interface based, they can control and monitor the usage only when connected to internet. Moreover proper usage logging and usage control based on the already set schedule is also absent. Practically, this management do not suffice the need of higher educational institutions because the areas like accountability, usage logging and control is not addressed in this approach. Both are important factor of enhancing management of LAN. This research paper proposes a tool-LABGUARD to incorporate these features. Further the tool has been implemented using .Net Technology. As a result, the usage of systems was accountable, only the authorized user could access the assigned sites with granted privileges at the retrospective time. Thus the system became more accountable and secured. It also enhanced the control of administrator on entire lab setup. It also facilitates the administrator to retrieve log details.

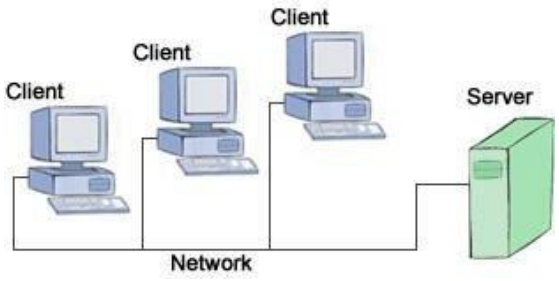
Keywords— Open source, firmware Software Reliability; Reliability Testing; module;

I. INTRODUCTION

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. The IP addresses of systems in an LAN belong to the same class. This makes systems communicate to each using Internet Protocol. Higher educational institutes have established LAN in their computer labs. Tools which are currently used for managing a computer lab use internet for sending and receiving the requests between the clients and servers systems. One such tool is Insight by a Canadian Software Company. It has multiplatform applications which require functioning internet. This type of model is not suitable when a LAN is not connected to outer internet. There should be a model which should also work even when LAN is not connected to the outer internet. Other tools also exists but as identified most of them are web based. This research paper proposes a tool-LABGUARD to incorporate these features. Further the tool has been implemented using .Net Technology. As a result, the usage of systems were accountable, only the authorized user could access the assigned sites with granted privileges at the retrospective time. Thus the system became more accountable and secured. It also enhanced the control of administrator on entire lab setup. It also facilitates the administrator to retrieve log details. This research paper has been divided in sections. Section II elaborate proposed work.

II. PROPOSED SYSTEM

The model on which we used these techniques is based upon the general model of a computer lab with a functioning LAN. There is one server and all other systems in the LAN are client systems. The server is administered by the LAB Administrator. The other client's systems are used by the Students/Professionals. The model assumes a workflow with an environment of an array computers connected with each other through a network such that data can flow between them. There is one administrator and others are users in the environment. The administrator is assumed to have responsibility of taking decision of privileges and allocations of resources.



Sample LAN

III. TECHNOLOGY STACK USED IN TEST IMPLEMENTATION OF MODEL

A Following were the attributes of Software and Hardware Stack used :

- Windows Server 2008 on Server and Windows 7 on Client Machines
- Microsoft .Net Framework 4.5 on all machines
- A Functioning LAN to make the machines connected to each with same Internet Protocol Address Class.

A. Feature of 'LABGUARD'

The We propose the following set of usage management requirements of LAN for our model of a computer lab in an Educational Institution:

- Authentication based system access on the LAN.
- Recording the usage logs of a student as per timestamp with control of when the student can use the system .
- Taking control of usage of external peripheral like USB Storage Devices and controlling these usages from a central server.

Revised Manuscript Received on July 22, 2019.
Nikhil Sharma, Clicklabs, Haryana, India

• In case of LAN Failure, the systems should be able bypass the authentication using a set of credentials stored at client's side which should be updated regularly from the server .

• Creating a Time Table Rule for giving access to the students who can access systems as per there time table and allowing proxy only if they have special permission.

• Providing control of the student's system to the central server so that the user of central server who would be the Administrator will be able to broadcast or unicast personal messages and control important system processes of the student's system .

• Server should be able to blacklist authentication request from certain Student Registration Numbers .

• The internet browsing should be monitored and each student's system should respond with the current web page opened when the server send the request to unravel the currently browsed web page . This ensures student's accountability mostly in the scenarios of a Assessment Test.

• Computer Lab usage Report Generation along with facts generations out of all the logs of the usages and all events .

B. PROPSOED MODEL

Modules

1. Client Modules

1.1 Login and Authentication

This module is responsible for authenticating the client login that occurs in Figure 1. Client Logins through unique ID.

Authentication is done in following 5 steps 1 . Server Validates the ID.

2 . Checks if ID is not one of the Blacklisted one.

3. Checks if the ID is allowed to use the system during that particular time.

4. If Step 3 Fails, check if ID is allowed to have time table conflicts . If yes then proceed. 5 . Set the default session time usage for ID and allow the access.

Figure 1:Login screen at Client's End

2. Server Modules

2.1 Time Table System and Time Table Conflict

The Time Table module focuses to describe and save the schedule of all the clients who intends to use the system and the time slot in which they will use it regularly. It is analogous to the Time Table of Lab Usage.

Time Table Conflicts occurs when user ID tries to access the system when he is not allowed as per Time Table .By Default, Time Table Conflicts user to login. Time Table Conflicts can be bypassed for some user IDs which can be set by the Server Administrator. Below are the screenshots of Time Table and Time Table Conflict Module.

2.2 Client Session and System Management

Server uses .Net Services to interact with client system. .Net Services allows server to control client's specific system services.

Client is given a pre-defined usage session time which can be changed during the session by server. Once expired, the same ID is not allowed to login for the next 10 seconds.

2.3 Logging System

Each and every event is logged onto the CSV files . Corresponding to each. Each row in the CSV file corresponds to each event that occurred in that day.The logging is done with the format EVENT_NAME-EVENT_META_DATA in each row.

2.4 Facts Generation System

The Facts are generated by parsing the csv files .The events are extracted by string extraction and the array functions then allow them to aggregate into the results. Below is screenshot of the control window of generating the facts and logs.

2.5 Browser Activity Spoofing

This module helps in monitoring the usage of internet on the client machines. The server sends the signal to all connected systems to get the current title of their web browser's active tab. This is done using specific .Net Services triggers.

2.6 Server Cache Management

Related to each request and successful login a Thread [1] is created and respective to each Thread a Hash. Is maintained which stores the data from SQL queries. This improves the server response time for subsequent requests to the server.

2.7 Security and Privileges

The security is a very important aspect of a Computer Lab in an Institution. The security encompasses keeping the resources in the computer lab intact and safe from any type of bugging .The security of a Computer Lab very much depends on how privileges are managed in the Lab as proper privileges imposes accountability on its users.

One of the major threat is using external data sources for devices. Our model enforces privilege of allowing the usage of such external devices only to the Lab Administrator thereby limiting this threat.

information storage and transfer between the system

Enforcing Accountability also adds up to the intent of increasing the security of LAB and our model does this by monitoring the use of system per user level.

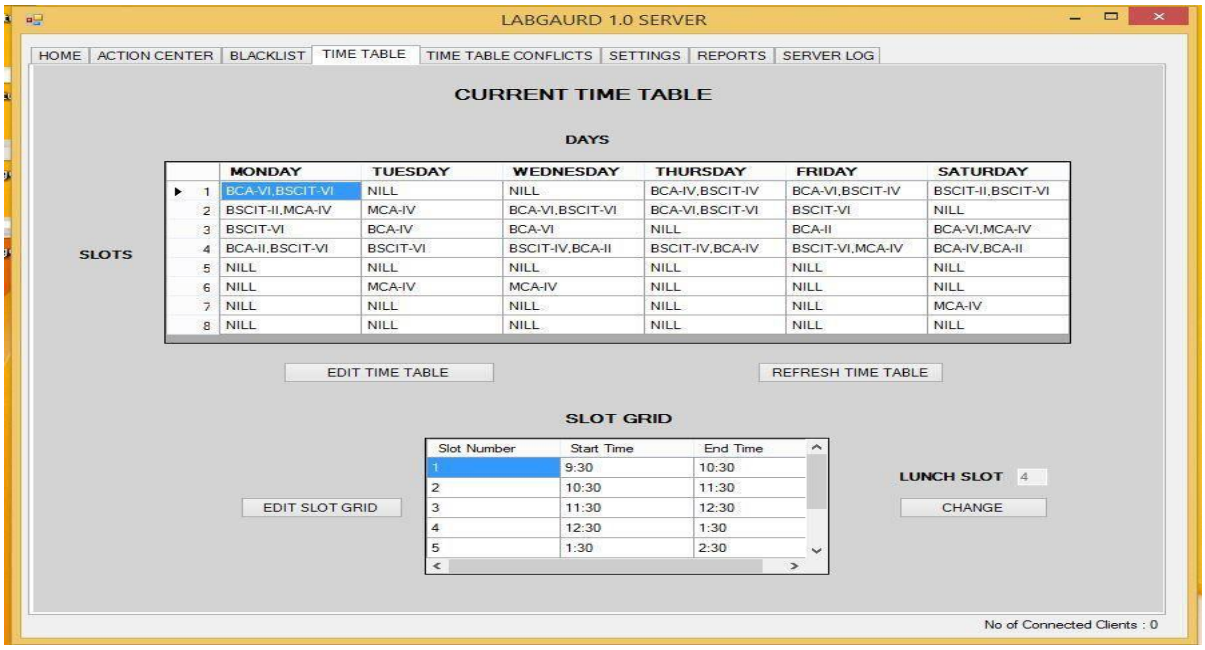


Figure 2 : Time Table Module at Server End

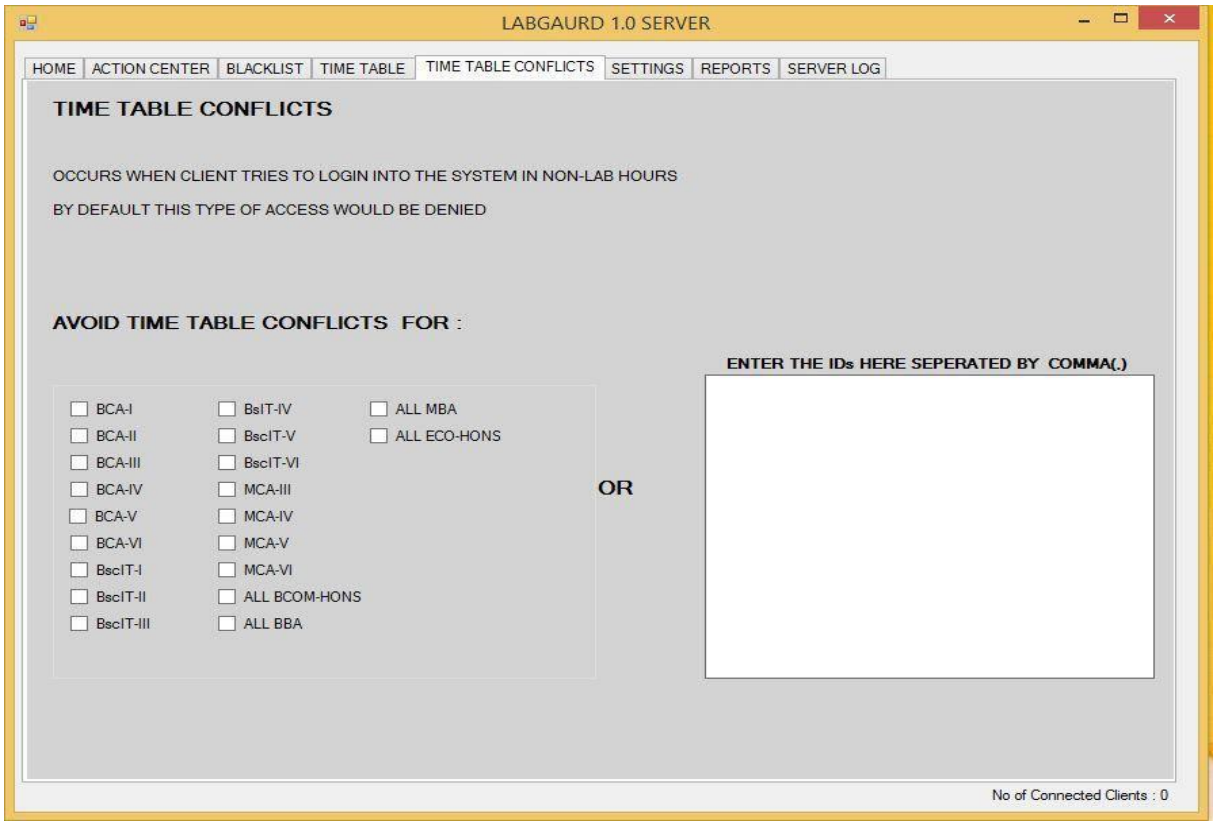


Figure 3 : Time Table Conflicts Module at Server End

.

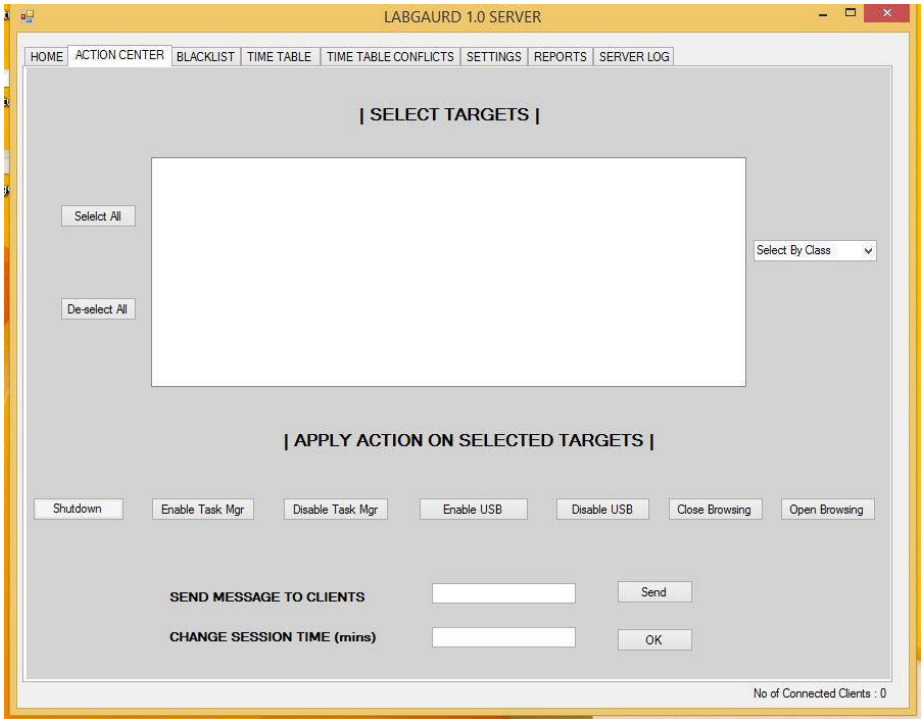


Figure 5 : This tab enables administrator control the client's system

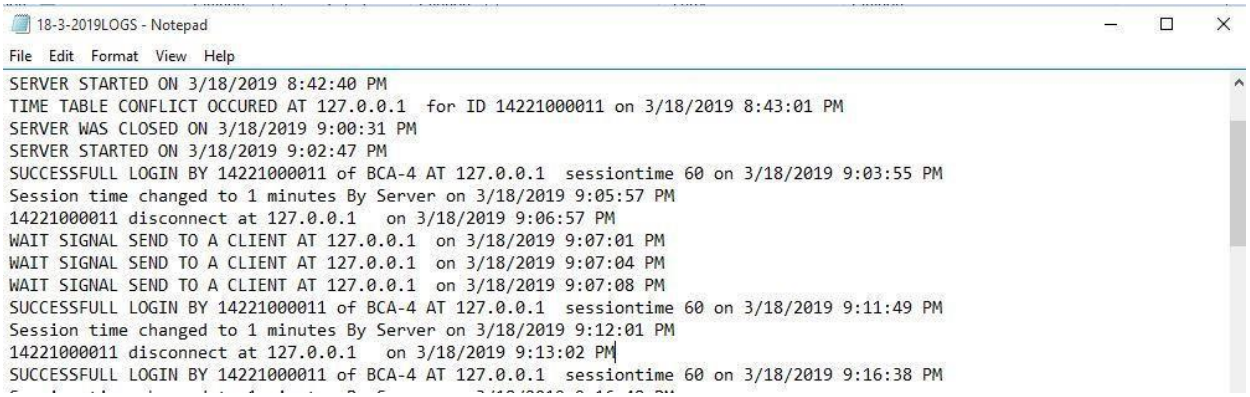


Figure 6 : Example of a Log file for the Date 18/3/2019

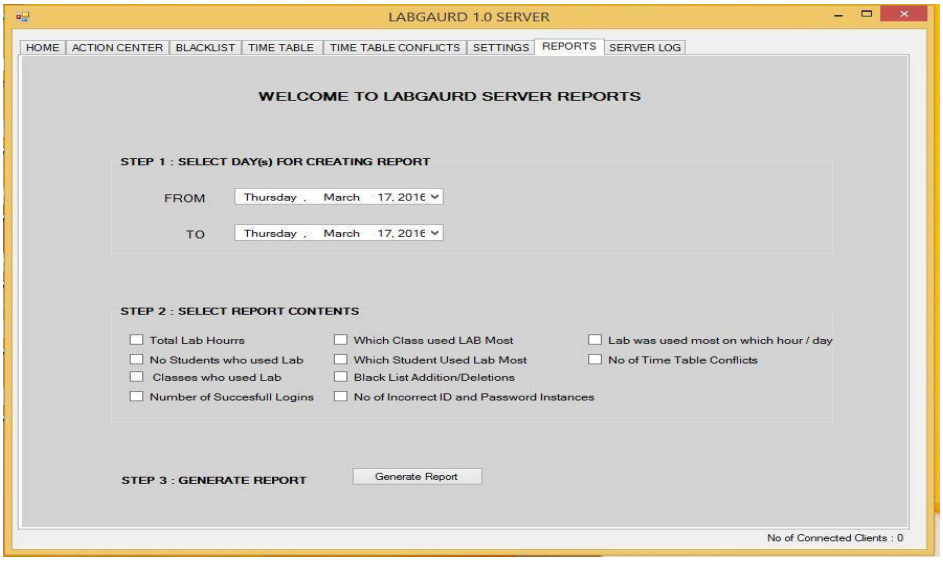


Figure 7 : Server Control Screen for generating log.

Figure 8: The above example shows the client being caught browsing a specific website]

IV. RESULTS

After the implementation of this model, a survey was conducted. Data from 288 respondents was collected to quantify the efficiency of the model on the following parameters:

- Accountability
- Security
- Usage Control

Each parameter had a scoring range of 1-10. Following attributes were attached to the sub-ranges of the score given by the respondents.

Very Good: 9-10

Good: 5-8

Satisfactory: 1-4

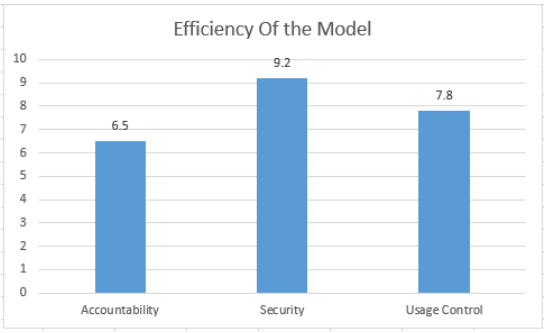
The weighted mean was then calculated for each parameter using the following formula:

Weighted mean = $\Sigma wx / \Sigma w$

Σ = the summation.

w = the weights. x = the value.

The Below graph was plotted based upon the data. The Y-axis represents the weighted mean which was calculated of each parameter:



V. CONCLUSION

The We first collected the limitations of the current LAN management techniques in the Higher Education institutions, We proposed a model and implemented the model using .Net technology. The implementation increased productivity and usability of the computer lab in the institution. We were able to increase the accountability, usability, usage control as depicted in Section III. The usage of systems were accountable, only the authorized user could access the assigned sites with granted privileges at the retrospective time. Thus the system became more accountable and secured. It also enhanced the control of administrator on entire lab setup. It also facilitates the administrator to retrieve log details. We can thus conclude that using these techniques will increase management techniques of the LAN in Higher Education Institution.

The model can be also implemented using other technologies based upon the requirements and availability of the resources in the Institution. For further enhancements the model can incorporate the class tests which can be given on any system which is connected to the LAN.

.

REFERENCES

1. Yang Chenghui,"A Design of Laboratory Information Management System" IEEE Xplore 2010
2. Chang Sheng, "Security of office management information system analysis" IEEE Xplore 2011.
3. Wu, Ziyan & Wu, Jinlang & Sun, Dan & Wu, Xiaoya. (2006). "Remote measurement platform based on DataSocket and .NET framework". 63581W-63581W. 10.1117/12.717947.
4. Davis, Keir & W. Turner, John & Yocom, Nathan. (2004). "Securing Network Communication" 10.1007/978-1-4302-0748-1_10.
5. Buis, P. (2002). Socket-level server programming & .NET. Doctor Dobbs Journal. 27. 25-32.