

Development of a Web-Based Network Access Monitoring and Control System for Systems Plus College Foundation's Computer Laboratory

Charlie Gutierrez
Arquillo, Zyide Osmond
Bagang, Paulo
Ayson, Jaycee
Carlos, Nathaniel

¹ CCIS, Systems Plus College Foundation, Angeles City, Philippines

² BSIT – Network Administration, Philippines

*Corresponding Author Email: Gutierrezcharlie57@gmail.com

ABSTRACT

Computer laboratories are important facilities in educational institutions because they provide students with access to computers, network resources, and software needed for academic activities. However, monitoring and controlling computer laboratory usage can become difficult when laboratory personnel rely on manual supervision and non-centralized network controls. These approaches may limit the ability of administrators to identify individual users, monitor specific computers, observe active websites and applications, and apply access restrictions based on laboratory schedules. This study proposes the development of a Web-Based Network Access Monitoring and Control System for Systems Plus College Foundation's Computer Laboratory to provide a centralized approach to managing computer and network access.

The proposed system aims to provide laboratory staff with real-time, per-computer visibility and identity- and schedule-based control over student network and application use. It will include a web-based administrator dashboard that displays the status of laboratory computers, active websites, running applications, bandwidth usage, and user or session information. The system will also incorporate a dynamic access-control mechanism that determines appropriate network and application permissions based on the user's account, program, and assigned laboratory schedule. A lightweight client agent will be installed on each laboratory computer to transmit relevant usage information to the central server and receive authorized commands from the administrator. These commands will include remotely locking a workstation, blocking a specific application, and disabling internet access on a selected computer.

Furthermore, the system will generate usage logs and reports organized according to users, computers, and sessions to support auditing and enforcement of acceptable-use policies. The study will focus on the computer laboratory of Systems Plus College Foundation and will not cover devices outside the designated laboratory or replace the institution's overall network infrastructure. The developed system will undergo testing and evaluation based on functionality, usability, reliability, and security to determine whether it meets the identified requirements and objectives of the study.

Keywords: *Web-Based System, Network Access Monitoring, Access Control, Computer Laboratory, Real-Time Monitoring*

SECTION I — INTRODUCTION (THE PROBLEM AND ITS SETTING)

1.1 Introduction

- Even in institutions that have adopted digital tools, most laboratory management processes, such as scheduling, monitoring of room conditions, and usage reporting, are still carried out manually, which is prone to error and consumes considerable staff time (Firdaus et al., 2026). In response, some network administrators have started moving toward router-based configurations that combine firewall filter rules, hotspot-based user authentication, and bandwidth allocation to manage students' internet access from a single configuration rather than through ad hoc, per-machine adjustments (Bachtiar & Prihanto, 2026). Likewise, some schools have implemented web-filtering firewalls to restrict access to content categories, such as pornography, online gambling, and games, that can distract students from their studies (Ma'mun & Muflih, 2025).

1.2 Background of the Study

- Computer laboratories are important facilities in educational institutions because they provide students with access to computers, network resources, and software needed for academic activities. However, managing shared computer resources requires appropriate mechanisms for monitoring and controlling access. Zapanta et al. (2021) examined an access-control and monitoring system for a computer laboratory, demonstrating the relevance of automated approaches to managing computer laboratory access.

As computer laboratories become increasingly dependent on network-connected resources, monitoring network activity and maintaining visibility of connected devices have also become important. The National Institute of Standards and Technology (NIST) explains that modern network environments require visibility and monitoring capabilities, while traditional network-access solutions may have limitations in addressing device and endpoint security.

Recent studies have also explored technology-based approaches to improve computer laboratory access management. Bucar et al. (2024), for example, developed a smart computer-laboratory access system using barcode-based identification at Bohol Island State University in the Philippines. Their study addressed limitations associated with conventional laboratory access procedures and sought to improve access management and monitoring.

Despite the availability of network security technologies, monitoring a computer laboratory can still be challenging when administrators rely primarily on manual supervision or network-level controls. Conventional network controls may provide information about network traffic without necessarily giving administrators sufficient information about the particular user, computer, application, or session involved. For a computer laboratory, this creates a need for a more centralized approach that can provide visibility at the individual-computer level and support appropriate access control.

1.3 Objectives of the Study

The general objective of the study is to develop a web-based network access monitoring and control system that gives **Systems Plus College Foundation**'s computer laboratory staff real-time, per-

computer visibility and identity- and schedule-based control over student network and application use, going beyond what a conventional firewall can provide.

The specific objectives of the study are:

1. To develop a web-based administrator dashboard that displays the real-time status of every laboratory computer, including active websites, running applications, and bandwidth usage;
2. To design a dynamic access control mechanism that automatically applies different network and application permissions based on the logged-in user's account, program, and the class schedule assigned to the laboratory at that time;
3. To develop a lightweight client agent, installed on each laboratory computer, that reports usage data to the central server and executes remote actions such as locking a workstation, blocking a specific application, or disabling internet access on that machine;
4. To generate usage logs and reports (per user, per computer, and per session) that laboratory staff can use for auditing and enforcing acceptable-use policies.

criteria.

1.4 Scope and Limitation of the Study

This study focuses on the development of a Web-Based Network Access Monitoring and Control System for the Systems Plus College Foundation Computer Laboratory. The proposed system is intended to provide laboratory staff with a centralized platform for monitoring and managing computer and network access within the laboratory.

The system will include a web-based administrator dashboard that displays the real-time status of laboratory computers, including active websites, running applications, and bandwidth usage. It will also include a dynamic access-control mechanism that applies network and application permissions based on the logged-in user's account, program, and the class schedule assigned to the laboratory.

The study will also cover the development of a lightweight client agent to be installed on each laboratory computer. The client agent will report relevant usage information to the central server and receive authorized commands from the system. These commands will include locking a workstation, blocking a specific application, and disabling internet access on a selected computer.

Furthermore, the system will generate usage logs and reports based on the user, computer, and session. These records are intended to assist laboratory staff in monitoring computer usage, conducting audits, and enforcing acceptable-use policies.

The study is delimited to the computer laboratory of Systems Plus College Foundation and focuses on the monitoring and control of computers and network/application usage within that laboratory. It does not cover monitoring of computers or devices outside the designated laboratory environment. The proposed system is also focused on laboratory computer and network access management and is not intended to replace the institution's entire network infrastructure or general school-wide network management system.

The study will evaluate the developed system based on the criteria identified in the research, particularly functionality, usability, reliability, and security.

1.5 Significance of the Study

- The proposed **Web-Based Network Access Monitoring and Control System for Systems Plus College Foundation Computer Laboratory** is significant because it aims to provide a centralized approach to monitoring and managing computer and network access within the laboratory. The system is expected to support laboratory personnel in monitoring computer activities, applying access-control policies, managing workstations, and maintaining usage records.

Laboratory Administrators and Staff

The proposed system may assist laboratory administrators and staff in monitoring the status and activities of laboratory computers through a centralized web-based dashboard. It may also provide them with tools for applying access permissions, locking workstations, blocking applications, and disabling internet access when necessary. Usage logs and reports may further assist them in reviewing laboratory activities and enforcing acceptable-use policies.

Students

The system may benefit students by providing a more organized and controlled computer laboratory environment. Through user- and schedule-based access control, students may be provided with access appropriate to their assigned laboratory sessions and activities. The system may also promote accountability by associating computer usage with individual users and sessions.

The institution may benefit from having a centralized system for monitoring and managing its computer laboratory resources. The proposed system may provide the institution with usage records that can support laboratory management, auditing, and enforcement of computer and network-use policies.

Future Researchers

This study may serve as a reference for future researchers who intend to develop or improve systems involving computer laboratory monitoring, network access control, remote workstation management, and usage logging. Future researchers may also use the study as a basis for exploring additional features or approaches for managing computer laboratory environments.

Researchers

The study will provide the researchers with practical experience in analyzing, designing, developing, implementing, and evaluating a web-based computer laboratory monitoring and control system. It will also allow them to apply concepts related to system development, network monitoring, access control, and database management in an actual institutional setting.

1.6 Definition of Terms

- **Authorized User** – A person who has been given permission to borrow library books or access library computers according to the rules and requirements of the system.

Centralized System – A system in which library book borrowing records and computer access information are managed and stored in one platform.

Computer Access Control – The process of regulating and managing who is authorized to access library computers.

Computer Access Records – Records containing information about users who access library computers, including relevant access or usage information.

Computer Usage – The activity performed by a user while using a library computer, which may include the user's access session and related usage information.

Network-Based System – A system that uses a computer network to allow connected devices and users to communicate with and access centralized system services.

Real-Time Monitoring – The process of providing current information about book availability, borrowing records, or computer access as activities occur.

System Evaluation – The process of assessing the developed system based on its functionality, usability, reliability, and security, as specified in the objectives of the study.

User Authentication – The process of verifying a user's identity before allowing access to authorized library computer resources or system functions.

SECTION II — LITERATURE REVIEW

2.1 Introduction to the Review

- This chapter presents the review of related literature and studies relevant to the development of the Computer Access Control System. The review focuses on existing technologies, systems, computer access control, network-based systems, and the monitoring of computer laboratories. These related works provide a foundation for understanding how digital and network-based technologies can improve the management, monitoring, and accessibility of students during laboratory time.

2.2 Review of Related Literature and Studies

- Effective management of laboratory resources and equipment is crucial for academic institutions to support teaching and learning activities. At the Federal Polytechnic, Ile-Oluji, Ondo State, the Computer Science Department faced challenges with manual tracking of ICT gadgets and inefficient laboratory resource management, resulting in errors and delays. This study aims to design and implement a Web-Based Laboratory Management System (WBLMS) to automate the processes of reservation, tracking, and inventory management, thereby enhancing operational efficiency and reducing errors in laboratory resource management. The research employed a system development methodology that included requirement analysis, system design,

implementation, and testing. A user-centric approach was adopted to ensure the system meets the specific needs of laboratory staff and students (Adekunle et al., 2024).

2.3 Conceptual Framework

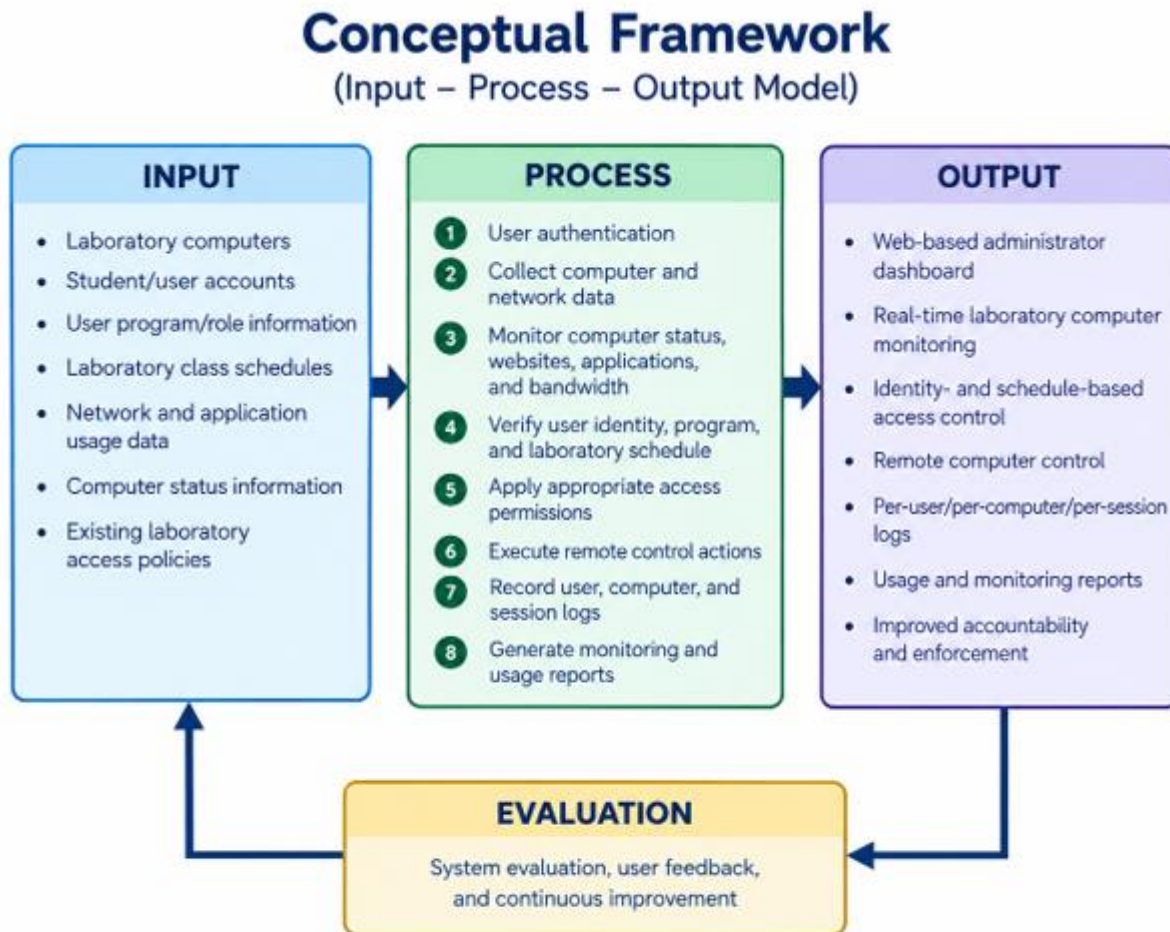


Figure 1. Conceptual Framework

2.4 Synthesis

• The reviewed literature and studies show that the management of computer laboratories is increasingly moving toward automated, centralized, and network-based systems. Firdaus et al. (2026) demonstrated the use of an IoT-based approach for monitoring computer laboratories, while Bachtiar and Prihanto (2026) discussed the use of firewall rules, user authentication, and bandwidth management to manage students' internet access. These studies demonstrate how technology can reduce dependence on manual laboratory management and provide administrators with better control over computer and network resources. However, the reviewed studies also show limitations in conventional network security approaches. Bashir Ismail et al. (2025) explained that traditional firewall configurations primarily rely on network information such as IP addresses, ports, and protocols and may not provide sufficient context about the specific user or

computer responsible for network activity. Similarly, Heino et al. (2022) discussed the need for endpoint-aware inspection because network-level inspection alone may not identify the endpoint or application associated with a connection. These findings indicate that monitoring a network alone may not be sufficient for a computer laboratory where administrators need information about individual computers, users, and applications. Despite these developments, the reviewed literature indicates a gap between network-level access control and detailed computer laboratory monitoring. Existing approaches may provide web filtering, firewall-based restrictions, or general network management, but they do not necessarily provide a centralized view of which student is using a particular computer, which applications or websites are active, whether the computer is being used during the appropriate class schedule, and what actions should be taken on an individual workstation. Our study addresses this gap by proposing a web-based system that combines real-time per-computer monitoring with identity- and schedule-based access control. The proposed system therefore builds upon the strengths identified in previous studies while addressing their limitations. It will provide an administrator dashboard for monitoring the status of laboratory computers, active websites, running applications, and bandwidth usage. It will also use user accounts, program information, and laboratory schedules to determine appropriate network and application permissions. Through a lightweight client agent, the system will additionally support remote actions such as locking a workstation, blocking applications, and disabling internet access, while generating logs and reports based on users, computers, and sessions. Overall, the reviewed literature and studies provide a foundation for developing a Web-Based Network Access Monitoring and Control System for Systems Plus College Foundation's Computer Laboratory. The synthesis suggests that combining centralized monitoring, user authentication, schedule-based access control, remote control, and usage logging can provide a more comprehensive approach to managing laboratory computers and network access.

SECTION III — METHODOLOGY

3.1 Research Design

- This study will employ a developmental research design to guide the development of the proposed Web-Based Network Access Monitoring and Control System for Systems Plus College Foundation's Computer Laboratory. The design is appropriate because the study focuses on designing, developing, and evaluating a system that addresses the identified problems in monitoring and controlling laboratory computer and network access. The proposed system will provide real-time monitoring of laboratory computers, identity- and schedule-based access control, remote computer control, and usage logging and reporting.

The development process will involve identifying the requirements of the computer laboratory, designing the system based on the identified requirements, developing the web-based monitoring and control system, and testing its functions. The system will be evaluated based on its ability to monitor computer status, websites, applications, and bandwidth usage; apply appropriate access permissions; perform remote control actions; and generate user, computer, and session logs. These functions are based directly on the specific objectives of the study.

The study will also incorporate system evaluation to determine whether the developed system meets the intended requirements. The evaluation will focus on the system's functionality, usability, reliability, and security, consistent with the study's goal of providing laboratory staff with a centralized means of monitoring and controlling computer and network access.

3.2 System Development Methodology

- The proposed system will utilize web-based and network technologies to provide centralized monitoring and control of the computer laboratory. The system will consist of an administrator dashboard, central server, database, and client agent installed on each laboratory computer. These components will work together to collect computer usage information and allow authorized laboratory personnel to monitor and control connected workstations. The system will also incorporate role-based access control (RBAC) to manage permissions according to the user's assigned role. RBAC has been applied in educational information systems to provide differentiated access to system resources based on user roles (Kabier et al., 2023).

3.3 Requirement Specification and Analysis

- **User Authentication** - The system shall authenticate authorized laboratory staff and users before providing access to system functions.

Computer Monitoring - The system shall display the real-time status of laboratory computers.

Website Monitoring - The system shall display active websites being accessed through laboratory computers.

Application Monitoring - The system shall display applications currently running on laboratory computers.

Bandwidth Monitoring - The system shall monitor and display bandwidth usage for laboratory computers.

User Identification - The system shall associate computer usage with the logged-in user.

Schedule-Based Access Control - The system shall apply permissions based on the user's account, program, and assigned laboratory class schedule.

Application Control - The system shall allow authorized laboratory staff to block a specific application.

Workstation Control - The system shall allow authorized staff to remotely lock a laboratory workstation.

Internet Control - The system shall allow authorized staff to disable internet access on a selected workstation.

Usage Logging - The system shall record usage information based on the user, computer, and session.

Report Generation - The system shall generate usage logs and reports for auditing and enforcement of acceptable-use policies.

These requirements are directly connected to our specific objectives, particularly the administrator dashboard, dynamic access control, client agent, remote actions, and usage reports.

2. Non-Functional Requirements

Usability - The system should provide a clear and understandable interface that laboratory staff can use to monitor and control computers.

Reliability - The system should consistently collect and record computer and usage information during normal operation.

Security - The system should restrict monitoring and control functions to authorized personnel.

Performance - The system should provide monitoring information and execute authorized control commands with minimal delay.

Availability - The monitoring system should remain accessible to authorized laboratory personnel during laboratory operations.

Maintainability - The system should allow authorized personnel to maintain and update system components when necessary.

Scalability - The system should be capable of supporting the laboratory's connected computers and additional computers when required.

our research specifically intends to provide centralized monitoring and enforcement while reducing reliance on manual patrolling and improving accountability through usage logs.

3. Requirements Analysis

3.1 Real-Time Computer Monitoring

The study identifies the need for laboratory personnel to have better visibility of individual computers. Conventional firewalls primarily inspect network traffic based on information such as IP addresses, ports, and protocols, which may not provide sufficient context regarding the specific student or computer responsible for the activity

Therefore, the proposed system requires a monitoring function capable of displaying the status of individual laboratory computers, including active websites, running applications, and bandwidth usage.

3.2 Identity-Based Access Control

The system requires user identification because network-level filtering alone does not necessarily establish who is using a particular computer. The proposed system will use the user's account, program, and assigned laboratory schedule when determining appropriate permissions.

3.3 Schedule-Based Access Control

Laboratory access can vary according to the class assigned to the laboratory at a particular time. Therefore, the system needs to consider the laboratory schedule when applying permissions.

For example:

User account → Program → Class schedule → Appropriate access permissions

This allows the system to dynamically determine which access rules should apply during a particular laboratory session. This requirement directly follows the second objective of the study.

3.4 Client Agent

A client agent is required because the system needs information from the individual laboratory computers. The proposed agent will report usage information to the central server and receive authorized commands from it.

3.5 Remote Control

The system requires remote-control functionality because manual intervention can be time-consuming and dependent on the physical presence of laboratory personnel. Your study identifies manual and non-centralized enforcement as one of the existing problems.

The proposed system will therefore allow authorized personnel to:

- Lock a workstation / specific computer
- Block a specific application
- Disable internet access

3.6 Logging and Reporting

The system requires centralized logging because laboratory staff need documented records of computer usage. The proposed system will generate logs and reports organized according to user, computer, and session.

3.4 System Design Specification

The proposed Web-Based Network Access Monitoring and Control System will use a centralized architecture composed of an administrator dashboard, central server, database, and client agent installed on each laboratory computer. These components will communicate through the laboratory network to monitor computer activities, apply access-control policies, execute authorized remote commands, and store usage records. Your paper already identifies these four main components under System Development Technology.

1. Administrator Dashboard

The administrator dashboard will serve as the main interface for laboratory staff. It will display

the real-time status of laboratory computers, active websites, running applications, bandwidth usage, and user or session information. It will also allow authorized personnel to manage access permissions and perform remote actions such as locking a workstation, blocking an application, and disabling internet access.

2. Central Server

The central server will act as the main communication and processing component of the system. It will receive usage information from the client agents, process access-control rules, and transmit authorized commands from the administrator to selected laboratory computers.

3. Database

The database will store important system information, including user accounts, computer information, laboratory schedules, access permissions, and usage logs. The stored records will allow laboratory staff to retrieve information according to the user, computer, and session for auditing and reporting.

4. Client Agent

A lightweight client agent will be installed on every laboratory computer. It will collect and transmit relevant computer and usage information to the central server. It will also receive and execute authorized commands from the administrator, including workstation locking, application blocking, and internet disabling.

5. Access Control Module

The access-control module will determine the appropriate permissions for each user based on their user account, program, and assigned laboratory schedule. This allows the system to dynamically apply network and application permissions according to the current laboratory session.

6. Monitoring Module

The monitoring module will provide real-time information about individual laboratory computers, including computer status, active websites, running applications, and bandwidth usage. This addresses the limitation of relying only on network-level information such as IP addresses, ports, and protocols.

7. Remote Control Module

The remote-control module will allow authorized laboratory personnel to remotely lock a workstation, block a specific application, or disable internet access on a selected computer.

8. Logging and Reporting Module

The system will automatically record computer usage information and organize the records according to users, computers, and sessions. It will generate reports that can support laboratory auditing and enforcement of acceptable-use policies.

3.5 Implementation

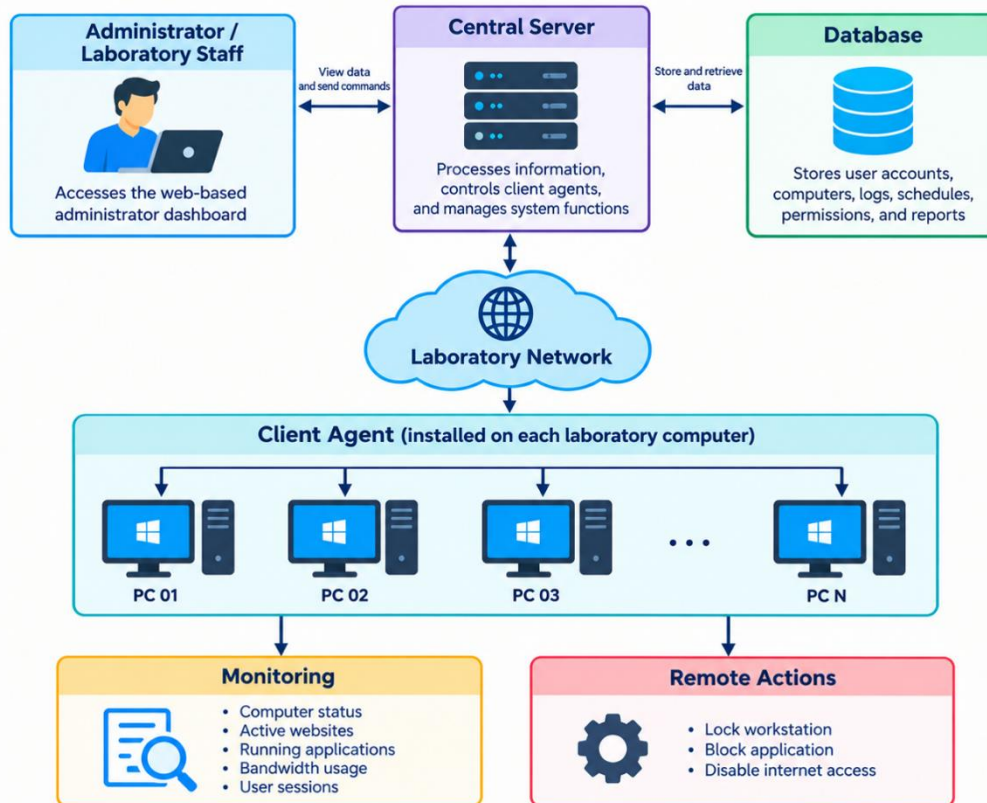


Figure 2. Simple Implementation Flow

3.6 Testing and Evaluation

• After the development and implementation of the proposed Web-Based Network Access Monitoring and Control System, the system will undergo testing and evaluation to determine whether it meets the identified requirements and objectives of the study. Testing will focus on the administrator dashboard, access-control mechanism, client agent, remote-control functions, and logging and reporting features. The administrator dashboard will be tested to verify whether it can properly display the current status of laboratory computers, active websites, running applications, bandwidth usage, and user or session information. The access-control mechanism will be tested using different user accounts, programs, and laboratory schedules to determine whether the system applies appropriate permissions and restrictions based on the user's information and assigned schedule. The client agent will also be tested to verify its communication with the central server, transmission of computer and usage information, receipt of administrator commands, and execution of authorized actions. The remote-control functions will be tested individually to verify whether the system can successfully lock a workstation, block a specific application, and disable internet access on a selected computer. The logging and reporting functions will be tested to determine whether usage information is correctly recorded and retrieved based on the user, computer, and session, and whether the generated reports contain accurate and relevant information.

The completed system will be evaluated based on functionality, usability, reliability, and security, consistent with the software quality concepts identified in ISO/IEC 25010:2023. The evaluation will involve functional testing, identification and correction of errors, retesting of

affected functions, and assessment by the intended users or evaluators. The researchers will then compile and analyze the evaluation results to determine whether the developed system satisfies the intended requirements and objectives of the study.

REFERENCES

Reference Guidelines

Zapanta, D. B., Jr., Talirongan, H., & Talirongan, F. J. B. (2021).

Access control and monitoring: A system for computer laboratory. *Mediterranean Journal of Basic and Applied Sciences*, 5(1), 18–27. [Access Control and Monitoring: A System for Computer Laboratory | Request PDF](#)

NIST Publishes SP 800-215: Guide to a Secure Enterprise Network Landscape. [NIST Publishes SP 800-215: Guide to a Secure Enterprise Network Landscape | NIST](#)

Bucar, J. I. O., Manabat, T., Doria, M., & Cardaña, D. (2024).

Development of smart personal computer access for computer laboratories using Arduino Uno. *National Conference on Computing, Education and Business 2024*. [\(PDF\) Development of Smart Personal Computer Access for Computer Laboratories using Arduino Uno](#)

Bachtiar, A., & Prihanto, A. (2026). Simulasi management akses pengguna internet sekolah menggunakan firewall filter rule dan bandwidth management queue tree [Simulation of school internet access management using firewall filter rules and bandwidth management queue tree]. *Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi*, 4(1), 155–165. <https://doi.org/10.61132/neptunus.v4i1.1509>

Bashir Ismail, A., Ibrahim Hussaini, M., Abba Abubakar, S., & Ahmad, A. (2025). Efficacy and limitations of firewall configurations in preventing network attacks: A conceptual review of architectures and rule sets. *FUDMA Journal of Sciences*, 9(12), 20–25. <https://doi.org/10.33003/fjs-2025-0912-4049>

Cybersecurity and Infrastructure Security Agency. (2023). Zero trust maturity model (Version 2.0). U.S. Department of Homeland Security. <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>

Firdaus, I., Maisarah, M., Urfiyati, N., Nurhuda, Y. A., & Firdaus, G. A. A. (2026). Rancang bangun sistem monitoring laboratorium komputer berbasis IoT [Design and development of an IoT-based computer laboratory monitoring system]. *Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi*, 4(1), 125–136. <https://doi.org/10.61132/neptunus.v4i1.1502>

International Organization for Standardization. (2023). Systems and software engineering — Systems and software quality requirements and evaluation (SQuaRE) — Product quality model (ISO/IEC 25010:2023).

Kabier, M. K., Yassin, A. A., & Abduljabbar, Z. A. (2023). Towards for designing educational system using role-based access control. *International Journal of Intelligent Engineering and Systems*, 16(2), 50–64. <https://doi.org/10.22266/ijies2023.0430.05>

Ma'mun, A. S., & Muflih, G. Z. (2025). Implementasi web filtering firewall untuk keamanan pada jaringan internet di Pondok Pesantren Al Hidayah Kebumen [Implementation of web filtering firewall for internet network security at Al Hidayah Kebumen Islamic boarding school]. *SKANIKA*, 8, 46–59. <https://doi.org/10.36080/skanika.v8i1.3298>

Mpamugo, E., & Ansa, G. (2024). Enhancing network security in mobile applications with role-based access control. *Journal of Information Systems and Informatics*, 6(3), 1872–1899. <https://doi.org/10.51519/journalisi.v6i3.863>

Adekunle, A. A., Abolore, B. L., Mutiu, G., & Olalekan, A. M. (2024).

Design and implementation of a web-based laboratory management system for efficient resource tracking. [Design and Implementation of a Web-Based Laboratory Management System for Efficient Resource Tracking | Asian Journal of Electrical Sciences](#)