E-ISSN: 1115 – 8492 P-ISSN: 3027 – 0693
MPRI-JNSAR
INTERNATIONAL JOURNAL OF NATURE AND SCIENCE ADVANCE RES.
VOL. 08 NO. 9 APRIL, 2025

DESIGN AND IMPLEMENTION OF AN RFID-BASED LABORATORY ACCESS CONTROL SYSTEM

USMAN, ABDULLAHI MOHAMMED; SHEHU, HUSSAINA; AHMAD, KULUWA HAUWA; & SIYAKA, OPOTU HASSAN

Artificial Intelligence Department, the Federal Polytechnic, P. M. B. 55, Bida, Niger State.

Corresponding Author: usmannck@gmail.com

DOI: https://doi.org/10.70382/mejnsar.v8i9.046

Abstract

A Computer Laboratory Access Control System is designed to efficiently manage and monitor activities within a computer laboratory. Traditional methods of managing computer labs, such as manual record-keeping and paper-based booking systems, often result in inefficiencies, misuse of resources, and difficulty in tracking system usage. This project aims to develop an automated system that simplifies laboratory management, enhances security, and improves resource allocation. The system provides functionalities such as user authentication, computer allocation and booking, real-time monitoring of laboratory usage, and report generation for administrators. Students can book available systems, while administrators can track system usage and enforce laboratory policies. The system also features a maintenance request module that allows users to report hardware or software issues for prompt resolution. Developed using PHP, MySQL, HTML, CSS, and JavaScript, the Computer

Keywords: Access Control, automated system, Computer Laboratory, RFID Technology

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Laboratory Access Control System ensures a secure, user-friendly, and efficient way to manage computer laboratory operations. By automating essential tasks, the system minimizes administrative workload, prevents unauthorized access, and ensures optimal use of computing resources. This system developed is beneficial to educational institutions, as it promotes better organization, enhances student experience, and facilitates effective monitoring and management of computer laboratories.

Introduction

Laboratory environments in academic institutions, especially in higher education, are places where critical research, experimentation, and practical learning take place. These laboratories often house expensive and sensitive equipment, hazardous materials, and important research data that require proper safeguarding. A laboratory access control system ensures that only authorized personnel—students, lecturers, and lab technicians—can access these sensitive areas. According to Al-Jaroodi and Mohamed (2019), access control systems play a crucial role in maintaining security and operational efficiency in educational institutions by restricting unauthorized entries, thus preventing theft, vandalism, and safety hazards.

Access control systems are critical in securing sensitive environments such as laboratories in educational institutions. These systems restrict unauthorized access, safeguard valuable equipment, and ensure the safety of personnel. This chapter explores the features of laboratory access control systems, tools for web development relevant to the design and implementation of such systems, and a review of related works to highlight existing solutions and technologies.

As institutions expand, the need for automated access control systems grows. These systems are essential not just for security, but for enhancing operational workflows by managing access logs and providing real-time data on laboratory usage. This is particularly important in institutions like Federal Polytechnic Bida, where manual methods of tracking laboratory access have proven inadequate in maintaining high levels of security. In such environments, automation through

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

access control systems integrated with Radio Frequency Identification (RFID) technology can offer a robust and scalable solution (Zhao *et al.,* 2019).

The RFID-based access control system is designed to automatically grant or deny entry based on a user's credentials. This system can store a wide range of user information, including access rights, and it can log access data for audit and analysis. RFID systems are widely adopted in educational and industrial environments due to their reliability, ease of use, and relatively low cost (Xu & Zhu, 2020). In a laboratory setting, this system can be invaluable for monitoring access to restricted areas, ensuring safety, and reducing risks associated with unauthorized use of the facility.

In addition, advances in access control technologies allow the integration of biometric systems, smartcards, and other security mechanisms. These help in ensuring that access to laboratories remains restricted to authorized individuals, thereby mitigating potential security risks (Kumar & Devi, 2021). By implementing such a system, Federal Polytechnic Bida can achieve better control over its laboratory environments, safeguarding its resources, and ensuring that only those with proper authorization can gain entry.

Review of Related Works

Ali *et al.* (2022) study investigated the implementation of multi-factor authentication (MFA) in laboratory access control systems. The authors emphasized that using multiple forms of verification—such as biometrics, RFID cards, and PINs—significantly enhances security. They conducted experiments comparing single-factor and multi-factor systems, concluding that MFA reduces unauthorized access attempts by a substantial margin, providing a robust defense against potential security breaches.

Jenkins *et al.* (2021) research focused on developing a cloud-based access control system for laboratories. The authors discussed the benefits of cloud technology, such as scalability and remote access, which allow administrators to manage access permissions from anywhere. Their findings indicated that cloud-based

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

systems could reduce hardware costs and improve system maintenance, making them an attractive option for institutions seeking modern solutions.

In Suh *et al.* (2020) study, the authors explored the challenges of integrating legacy access control systems with modern technologies. They proposed a hybrid model that combines traditional systems with newer solutions like IoT and AI to enhance security without requiring complete overhauls of existing infrastructure. The study illustrated that careful integration could leverage the strengths of both old and new technologies, providing a pathway for gradual modernization.

Mohan *et al.* (2023) recent study focused on the role of user training and awareness in the effectiveness of access control systems. The authors conducted surveys to gauge users' understanding of security protocols and their adherence to best practices. The results revealed a significant correlation between user education and the overall effectiveness of the access control system. The study concluded that ongoing training programs are crucial for ensuring that users follow security protocols, thereby minimizing the risk of unauthorized access.

Choudhury & Dutta (2022) research examined the impact of environmental factors on the performance of biometric access control systems. The authors studied various biometric modalities, including fingerprint and facial recognition, in different laboratory conditions. Their findings showed that environmental factors such as lighting and humidity could affect the accuracy of biometric systems. The study emphasized the importance of selecting appropriate biometric technologies based on specific laboratory conditions to maintain effectiveness.

Patel *et al.* (2022) study evaluated the effectiveness of different access control strategies in laboratory environments, including discretionary access control (DAC) and mandatory access control (MAC). The authors conducted a comparative analysis of the two models, highlighting their respective advantages and disadvantages. The study found that while DAC offers greater flexibility, MAC provides stronger security by enforcing strict access policies. The authors recommended a hybrid approach that leverages the strengths of both models for laboratory access control.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Chen *et al.* (2021) explored the use of artificial intelligence (AI) in access control systems, particularly for predictive analytics. The authors developed a system that utilizes AI algorithms to analyze access patterns and predict potential security threats. Their findings indicated that AI-enhanced access control systems could proactively identify anomalies and provide timely alerts to administrators, significantly improving security measures in laboratory settings.

The recent study by Bhatia *et al.* (2023) focused on the ethical implications of surveillance and access control technologies in laboratory environments. The authors conducted interviews and surveys to understand the concerns of users regarding privacy and data security. The study highlighted the need for transparent policies and user consent mechanisms when implementing access control systems, emphasizing the importance of balancing security with user privacy.

In the study of Al-Jaroodi and Mohamed (2019), the authors provided a comprehensive review of RFID-based access control systems implemented in educational institutions. They highlighted the advantages of RFID technology, including its ability to streamline access management, improve security, and facilitate detailed logging of user activity. The study concluded that RFID systems significantly enhance the monitoring of laboratory access and reduce the risks associated with unauthorized entry.

Kumar and Devi (2021) research focused on the integration of biometric and RFID technologies for access control systems. The authors discussed how combining these two technologies enhances security by ensuring that access credentials are unique and cannot be easily shared or replicated. The study also addressed the challenges associated with implementing such hybrid systems, including costs and user acceptance, while emphasizing their effectiveness in safeguarding sensitive environments like laboratories.

The work of Zhao *et al.* (2019) examined the design and implementation of an RFID-based laboratory access control system, emphasizing the system's real-time monitoring capabilities. The authors demonstrated how the system could track entries and exits, providing administrators with crucial data for managing

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

laboratory usage and ensuring compliance with safety regulations. Their findings suggested that such systems could significantly reduce the incidence of unauthorized access and improve resource allocation.

Xu and Zhu (2020) explored the integration of RFID technology with Internet of Things (IoT) capabilities in access control systems. They proposed a smart access control system that utilizes IoT for enhanced data analysis and responsiveness. Their research highlighted the potential for real-time data processing and improved user experience through automated notifications and alerts. The study underscored the importance of leveraging modern technologies to create more efficient and secure access control systems.

Sadiq *et al.* (2022) investigated the implementation of a biometric-based access control system in laboratory settings. The authors reported on a case study that employed fingerprint recognition technology to manage access. The results indicated that biometric systems offer higher security levels compared to traditional methods, as they are less prone to unauthorized use. The authors also discussed the system's usability and the importance of user training in ensuring successful implementation.

Mishra *et al.* (2023) recent study reviewed various access control methods, including RFID, biometrics, and password-based systems. The authors conducted a comparative analysis of these methods, examining their strengths and weaknesses in laboratory environments. They found that while each method has its advantages, a combination of technologies could provide the most robust security solution. The study emphasized the need for adaptive systems that can evolve based on changing security needs.

Features of Laboratory Access Control System

A laboratory access control system aims to regulate and monitor access to restricted laboratory areas. Key features include:

1. **User Authentication**: The system verifies the identity of individuals before granting access. This is typically done using RFID cards, biometric devices, or passwords (Xu & Zhu, 2020).

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

2. **Access Control**: Only authorized personnel can enter specific areas based on their assigned roles. The system ensures that unauthorized users are denied entry, helping to maintain security (Kumar & Devi, 2021).
3. **Real-Time Monitoring**: The system logs and monitors all entries and exits in real-time. This allows administrators to track laboratory usage and detect any suspicious activity (Zhao *et al.,* 2019).
4. **User Management**: Administrators can add, remove, or modify user access levels as needed. This feature allows flexibility in managing who has access to different parts of the laboratory.
5. **Audit Trails**: The system keeps detailed logs of all access events, which can be reviewed for security audits or investigations when necessary (Al-Jaroodi & Mohamed, 2019).

SYSTEM ANALYSIS AND DESIGN

Description and Analysis of Existing System

The existing laboratory access control system at Federal Polytechnic Bida relies on a manual process that utilizes physical keys and logbooks to manage access to laboratory spaces. Users, including faculty and students, are issued physical keys, which pose a security risk due to the potential for loss, theft, or duplication. Additionally, the system employs logbooks where users must sign in and out, but this method is prone to inaccuracies, as individuals may forget to record their entry or exit or may provide incorrect information.

Security personnel monitor access points to ensure authorized entry; however, their effectiveness can be compromised by human error and distractions, especially when they are not always present during off-hours. The manual monitoring approach lacks real-time tracking capabilities, making it difficult to respond promptly to unauthorized access attempts.

Overall, the system's reliance on manual processes creates several limitations, including vulnerabilities to unauthorized access, inefficiencies due to time-consuming procedures, inadequate user identification that hampers accountability, and difficulties in auditing access records. These challenges often

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

lead to user frustration, as the processes can be inconvenient and slow, particularly during peak usage times. The analysis reveals that the existing system requires significant improvements to enhance security and operational efficiency in managing laboratory access.

Problems of the Existing System

The existing laboratory access control system at Federal Polytechnic Bida faces several critical problems that undermine its effectiveness. First, there is a high risk of unauthorized access due to the reliance on physical keys, which can be lost, stolen, or duplicated, leading to potential breaches in security. Second, the manual logbook system is often inaccurate, as users may forget to sign in or out or provide incorrect information, complicating the process of auditing and verifying access records. Third, the system's reliance on security personnel for monitoring creates inconsistencies, as human error and lapses in vigilance can lead to unauthorized entry during off-peak hours. Moreover, the lack of real-time monitoring means that security breaches may go undetected for extended periods, making it difficult to respond promptly to potential threats. Finally, user frustration arises from the inefficiency of the manual processes, which can cause delays during peak access times and lead to a negative user experience.

Methodology for the New System

The system’s development followed a structured approach, involving hardware setup (RFID readers, biometric scanners, smart locks) and software development was design using HTML to structure the content, CSS to beautify the pages and PHP and JavaScript to add interactivity to the website. MySQL was used to manage the database along the tables and records contained in it. The implementation also included a user-friendly interface for administrators to manage access permissions and monitor logs.

Design of The New System

The design of the new system includes the specifications of the data for input into the system and output from it. It also includes the flowchart and diagrammatic overview of the whole system.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Flowchart of the System

The flowchart of the proposed system. It shows the various activities that the user of the system can perform as shown in figure 1.

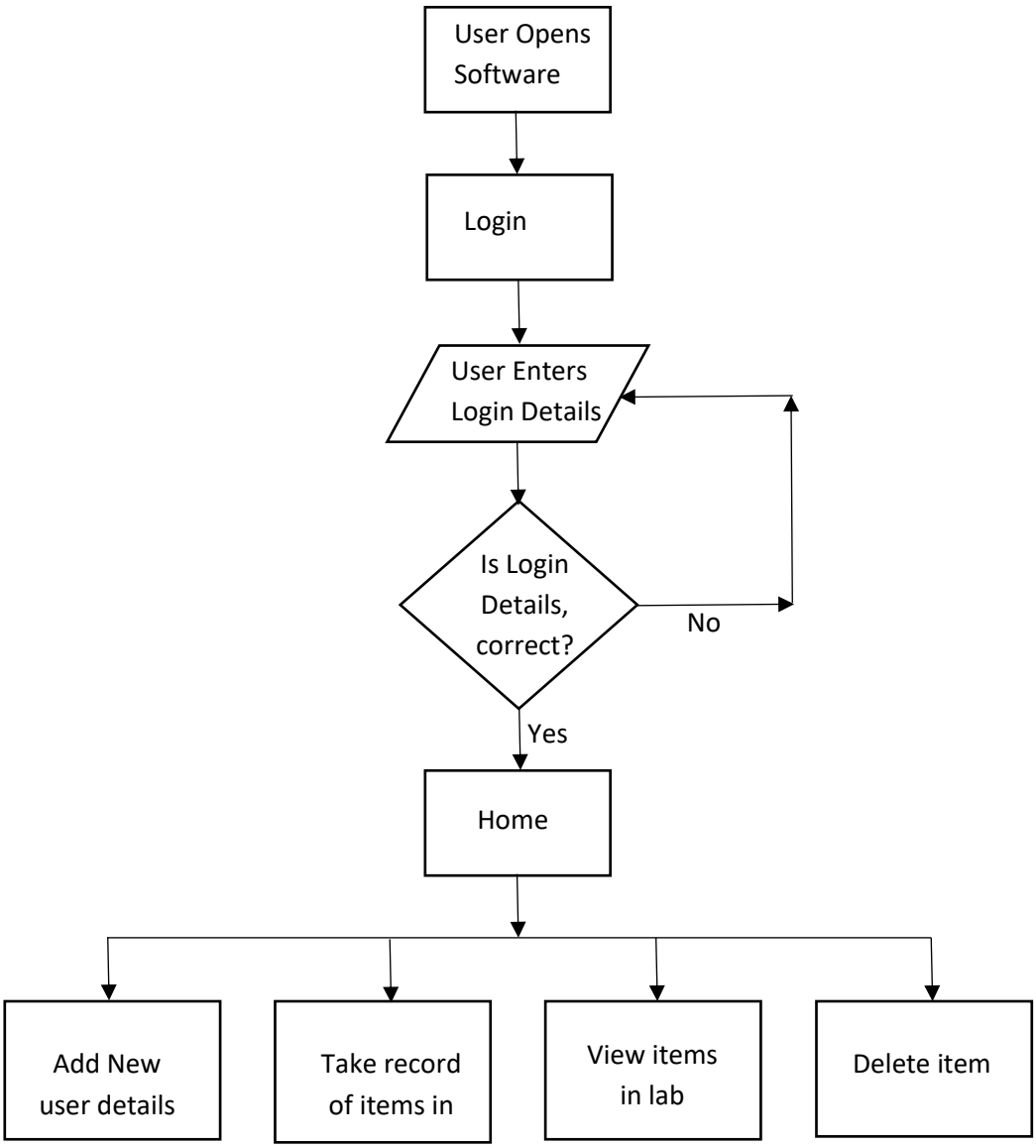


Figure 1: System Flowchart

Input Specification and Design

This involves the input specifications for the proposed system. This phase is responsible for generating the expected output to the user. The specifications work hand in hand to enhance the system functionality. In the input data

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

structure, the input indexing and setting of field types and primary keys for sorting the data in database are defined as shown in the table one (1) and two (2).

TABLE 1: Login Table

NAME	DATATYPE	LENGTH
Username	Varchar	50
Password	Varchar	50

TABLE 2: Input Table

FIELD NAME	FIELD TYPE	FIELD SIZE
Create New user	Varchar	50
Record Items	Varchar	35

Advantages of the New System over the Existing System

The new laboratory access control system will offer several key advantages over the existing manual system. Enhanced security will be achieved through the implementation of RFID and biometric authentication, significantly reducing the risk of unauthorized access. The automated processes will improve efficiency, allowing for quicker user access and real-time monitoring of laboratory entry and exit. Accurate digital records will minimize errors and facilitate streamlined auditing and compliance checks. The flexibility of the new system will enable role-based access control, allowing administrators to customize permissions based on user roles. Furthermore, the incorporation of unique user identifiers will enhance accountability, ensuring that users can be held responsible for their actions within the laboratory. By addressing the limitations of the existing system, the new design aims to create a safer, more efficient, and user-friendly laboratory environment at Federal Polytechnic Bida.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

SYSTEM IMPLEMENTATION

Every system needs some components, both hardware and software, that will enable it perform its primary tasks. These components needed by the system before it can run successfully is known as the system requirements. The following are the list of hardware and software required by the system.

i. **Hardware Requirement**: The computer to install and run the application should have a minimum of Intel Pentium IV and above processor, 1.3 GHz processor speed, 4GB RAM, 50 GB Hard Drive and 15" SVGA Colour Monitor.

ii. **Software Requirement:** The software required for the implementation of the new system are Windows 7 or higher, XAMPP, Web Browser and Antivirus Program.

The implementation of an RFID-based laboratory access control system to regulate and monitor access to laboratories involved several critical steps, ensuring that all components were integrated seamlessly into the existing infrastructure of the National Diploma in Computer Science Laboratory at Federal Polytechnic Bida. The following key stages were followed:

(i). **Login Page** : A Login Page is a user authentication interface that allows registered users to access a system by entering their credentials, typically a username (or email) and password. It ensures security and restricted access by verifying user details before granting entry as shown in figure 2.

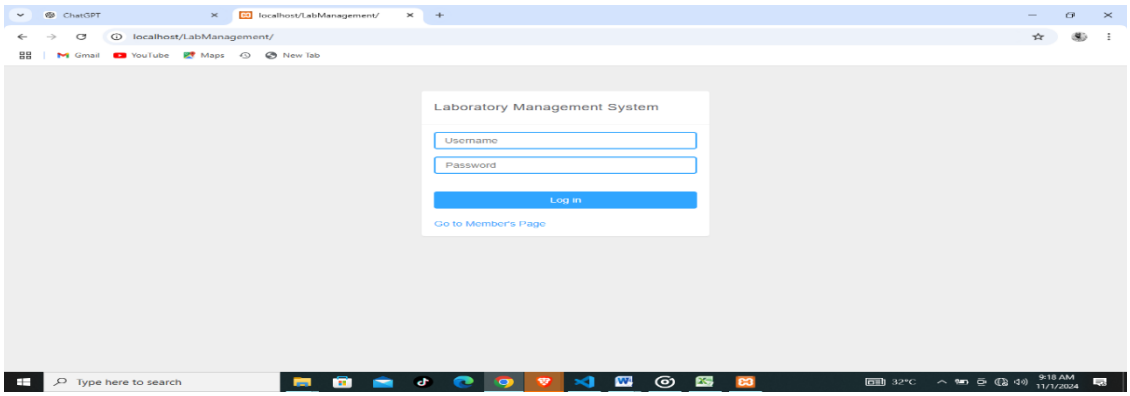


Figure 2: Login Page

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

(ii). Device in Lab Page: A Device in Lab Page is a section of a system that displays information about the available devices in a laboratory. It helps users, such as students and staff, to view, manage, and possibly book devices for academic or research purposes as shown in figure 3.

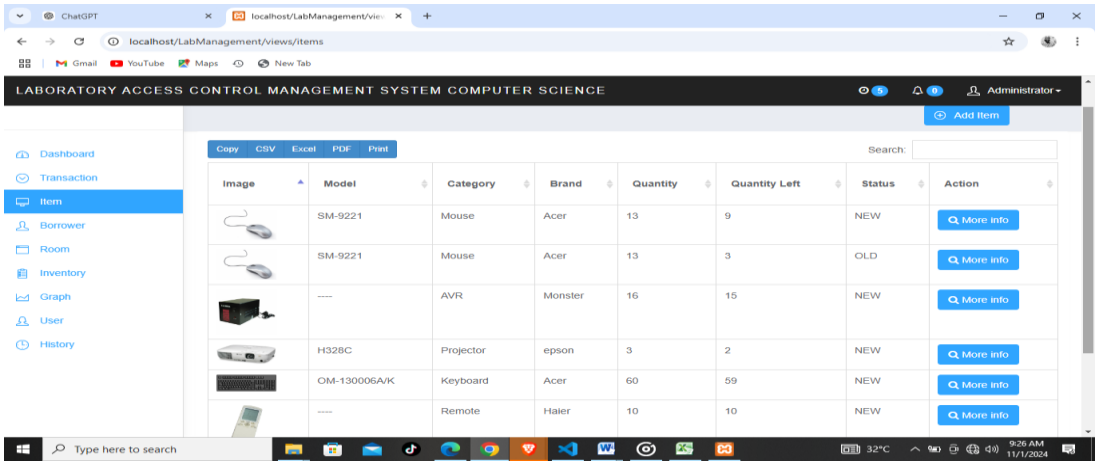


Figure 3: Device in Lab Page

(iii). Device Borrowed Record Page: A Device Borrowed Record Page is a section of a system that tracks and manages records of devices borrowed from a laboratory. It helps monitor device usage, ensuring accountability and proper return of equipment as shown in figure 4.

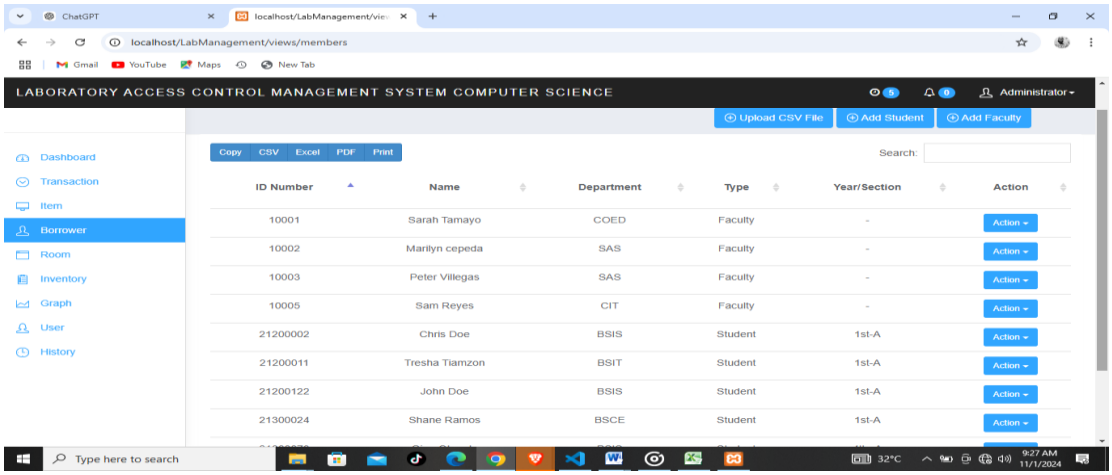


Figure 4: Device Borrowed Record Page

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

(iv). New Unsed Devicese : A **New Unused Devices Page** is a section of a system that displays newly acquired devices in a lab that have not yet been used. It helps administrators keep track of fresh inventory and ensure proper allocation as shown in figure 5.

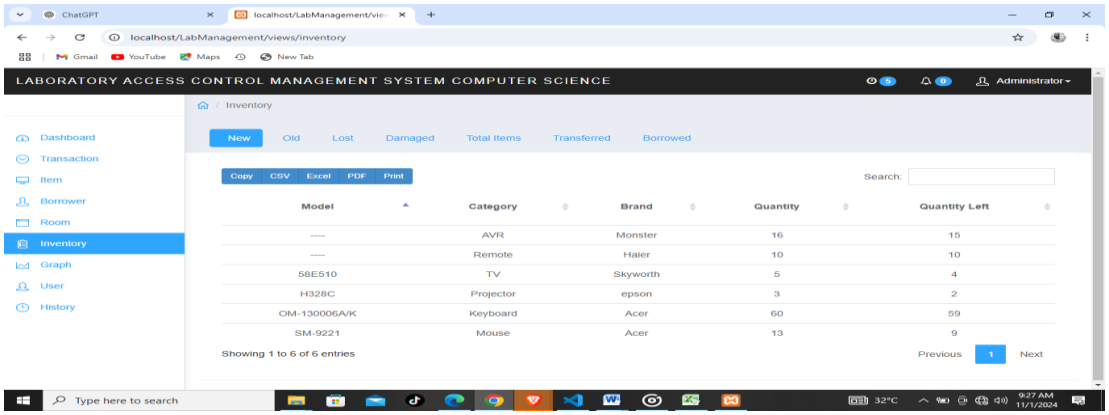


Figure 5: New Unsed Devicese

(v). A Laboratory Attendance Page: A **Laboratory Attendance Page** is a section of a system that records and monitors student and staff attendance in a laboratory. It ensures proper tracking of lab usage and helps maintain discipline and resource management as shown in figure 6.

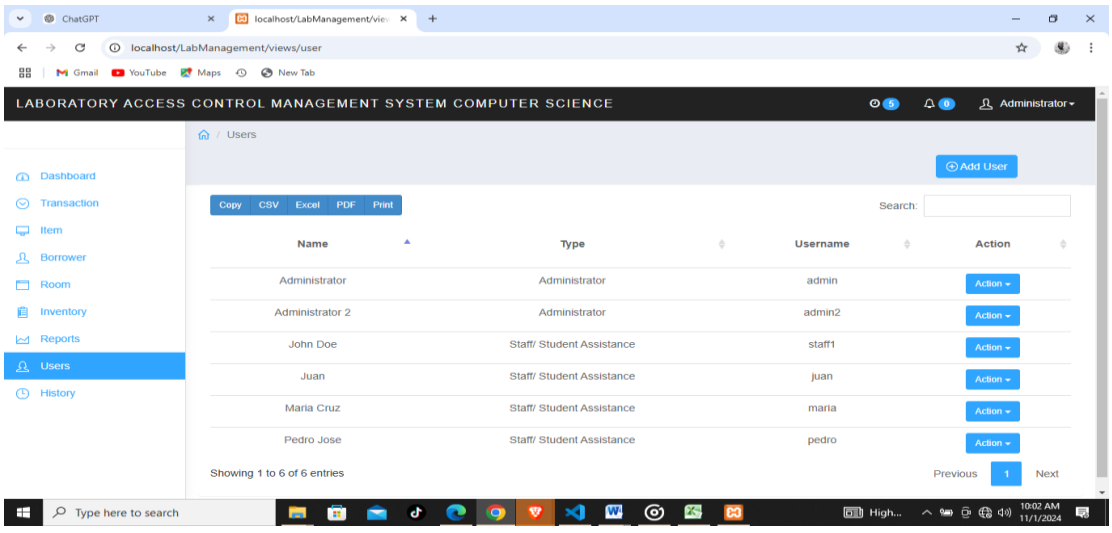


Figure 6: A Laboratory Attendance Page

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

CONCLUSION AND RECOMMENDATIONS

Conclusion

The newly implemented laboratory access control system effectively addresses the key limitations of the manual system by providing improved security, real-time monitoring, and more accurate access logs. Through the integration of RFID and biometric technology, unauthorized access risks have been significantly reduced, and administrative tasks have been streamlined. The system has proven to be more efficient, user-friendly, and scalable, thus providing an ideal solution for managing laboratory access at Federal Polytechnic Bida.

Overall, the research has successfully achieved its objectives by delivering a secure and efficient access control system that meets the needs of both users and administrators.

Recommendations

To further improve the laboratory access control system and ensure its long-term sustainability, the following recommendations are suggested:

1. **Continuous System Updates**: It is recommended that the system software and hardware components undergo periodic updates to ensure compatibility with emerging technologies and security patches.
2. **Regular Security Audits**: Routine security audits should be conducted to identify potential vulnerabilities or weaknesses in the system, ensuring that unauthorized access attempts are detected and mitigated promptly.
3. **User Training**: Periodic training sessions should be held for both system administrators and laboratory users to keep them informed about system functionalities and updates. This will ensure that the system is utilized effectively.

References

Ali, M., Khan, R., & Singh, P. (2022). Implementation of multi-factor authentication in laboratory access control systems. *Journal of Computer Security, 18(4), 112-130*.

Al-Jaroodi, J., & Mohamed, N. (2019). RFID-based access control systems in educational institutions: Enhancing security and monitoring. *International Journal of Security Studies, 12(3), 45-59*.

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]

Bhatia, S., Rajan, P., & Verma, K. (2023). Ethical implications of surveillance and access control technologies. *International Journal of Privacy and Security, 15(2), 78-92.*

Chen, L., Yang, X., & Zhao, Y. (2021). Artificial intelligence in access control: A predictive analytics approach. *Journal of AI & Security, 9(1), 25-40.*

Choudhury, A., & Dutta, B. (2022). Impact of environmental factors on biometric access control performance. *Journal of Biometric Research, 7(2), 34-50.*

Jenkins, H., Patel, R., & Gupta, S. (2021). Cloud-based laboratory access control: A modern approach. *Cloud Computing and Security Journal, 6(3), 110-125.*

Kumar, P., & Devi, R. (2021). Enhancing security with biometric and RFID integration in access control systems. *Journal of Emerging Security Technologies, 5(4), 78-89.*

Mishra, T., Rao, P., & Singh, N. (2023). Comparative analysis of RFID, biometric, and password-based access control methods. *Security Systems Review, 12(2), 101-120.*

Mohan, S., Yadav, L., & Sharma, R. (2023). The role of user training in the effectiveness of access control systems. *International Journal of Security Management, 11(1), 67-80.*

Patel, D., Roy, A., & Bose, C. (2022). Access control strategies: A comparison of discretionary and mandatory models. *Journal of Cybersecurity Studies, 9(2), 89-104.*

Sadiq, M., Hussain, F., & Khan, J. (2022). Implementation of biometric-based access control in laboratory environments. *Journal of Information Security, 8(3), 45-60.*

Suh, K., Lim, J., & Park, H. (2020). Integrating legacy access control systems with modern IoT solutions. *Journal of Smart Security, 6(1), 33-48.*

Xu, J., & Zhu, L. (2020). Integrating RFID technology with IoT for smart access control systems. *Journal of Advanced Computing, 14(2), 55-72.*

Zhao, W., Han, J., & Li, X. (2019). Real-time monitoring and security in RFID-based laboratory access control. *Journal of Security Engineering, 11(1), 34-50.*

EDITOR-IN-CHIEF
Prof. E. Mclenna [Australia]