DisKURSO INTERNATIONAL MULTIDISCIPLINARY RESEARCH JOURNAL
E-ISSN: 3116-3106 | P-ISSN: 3116-3084

Synchronized Electronic Device Control System

[1]John Uriel J. Antigua*, [1]Reymark S. Dahili, [1]Zaljelyn Y. Wapin, [1]Jason G. Abellanosa, [1]Michael L. Lopez, [1]Mark R. Nambatac
[1]Tagoloan Community College, Philippines
*Corresponding Author's Email Address: irdc2025@gmail.com

DOI: 10.63941/DisKURSO.2025.1.1.10

Article Information

Received: July 26, 2025

Accepted: October 2, 2025

Published: November 13, 2025

Keywords

Control System; Energy Efficiency; Biometric Access Control; Automatic Door Lock; Ultrasonic Sensors; Educational Institutions; Laboratory Management

ABSTRACT

This study focuses on the development and evaluation of a Synchronized Electronic Device Control System to enhance energy efficiency and security in laboratory environments at educational institutions. Conducted during the second semester of the 2023-2024 academic year, it involved six engineering department instructors and 14 college engineering students. A descriptive research design with surveys and Likert scale questionnaires was employed to assess the system's functionality, reliability, and craftsmanship. The system integrates biometric access control, automatic door lock mechanisms, and real-time synchronization of laboratory appliances like lights and fans, using ultrasonic sensors for occupancy detection. This ensures appliances operate only when the laboratory is occupied, optimizing energy usage and reducing unnecessary power consumption. Rigorous testing demonstrated the system's effectiveness in reducing electricity costs and preventing unauthorized access. The findings advocate for the system's widespread implementation across the entire school campus to promote sustainability, reduce operational costs, and ensure secure, efficient laboratory environments. This study addresses the specific needs outlined by educational governing bodies, such as the Commission on Higher Education (CHED), ensuring laboratories remain exclusive and dedicated to scientific research. The successful integration of these technologies not only provides a practical solution to existing challenges but also sets a precedent for future innovations in educational infrastructure. The study concludes with a recommendation for adopting this system campus-wide to foster a culture of innovation, energy efficiency, and enhanced security.

INTRODUCTION

In recent years, the increasing demand for energy efficiency and security in educational institutions has prompted the need for innovative solutions to address challenges like high electricity bills and unauthorized access to laboratory facilities. Educational institutions, particularly schools and universities, often grapple with soaring electricity costs due to human errors such as the failure to turn off electrical appliances, especially lights and fans. These errors not only strain financial resources but also contribute to unnecessary energy waste and a heightened carbon footprint. Dyussembekova, Westküste, Temirgaliyeva, Umyshev, and Shavdinova (2023).

As published by CMO No. 25, Series of 2005, maintaining the security and exclusivity of laboratory rooms in accordance with the guidelines set by educational governing bodies like the Commission on Higher Education (CHED) is of paramount importance. CHED regulations stipulate that laboratory rooms should remain free from unauthorized access, maintaining their sanctity as spaces dedicated to scientific research and experimentation.

Implementing this study can enhance security and convenience for authorized personnel, while students benefit from hands-on learning, interdisciplinary skill development, and exposure to

innovation, and preparation for emerging industry trends. Bekele & Atakara (2023) investigated the importance of energy-efficient building automation systems in reducing energy consumption and costs. Their study emphasized the need for intelligent systems that can automatically manage and control electronic devices, such as lighting and HVAC, to reduce electricity consumption. The findings highlight the potential of a synchronized electronic device system to optimize energy usage, addressing one of the primary issues faced by educational institutions, including high electronic bills.

As studied by Cobo, Cabaravdic, and Žiga (2023), the researcher made an automated door as a smart device that presented in this paper delves into the augmentation of traditional home devices by integrating smart technologies. It focuses on the development of a smart door control system accessible through a web interface, enabling remote control from any Internet-connected device. A pivotal component of this system is the servo motor, intricately constructed through a combination of software and mechanical elements. The software component comprises a PID controller and a web server, while the mechanical aspect involves the integration of an electric motor and electronic components. The use of the ESP32 microcontroller and Arduino platform, along with HTML, CSS, JavaScript, and "web socket" technologies, facilitates the creation of a user-friendly interface for two-way communication. The paper also emphasizes the consideration of privacy and data exchange speed, highlighting the advantages of direct device-user connections. The implementation of this automated door drive element not only enhances convenience through remote control but also offers insights into potential challenges and drawbacks associated with smart devices in home automation. The comprehensive exploration of both advantages and disadvantages contributes to a nuanced understanding of the implications of integrating such technologies into our daily lives.

In response to these challenges, the researchers introduce the concept of a "synchronized electronic device system." This system combines biometric authentication technology with smart control of doors and electrical appliances, with the goal of enabling authorized personnel to seamlessly access laboratory rooms while ensuring energy efficiency and security.

MATERIALS AND METHODS

Project Design

The goal of this research is to develop and implement an innovative, secure, and energy-efficient solution for laboratory rooms within school institutions, utilizing biometric access control to synchronize the activation and deactivation of electronic devices, with a primary focus on lights and fans. The overarching aim is to enhance security, promote energy conservation, and address the challenge of high electronic bills caused by human errors while ensuring compliance with regulatory requirements for laboratory exclusivity.

The project design illustrates how the project operates using a block diagram, as shown in Figure 1.

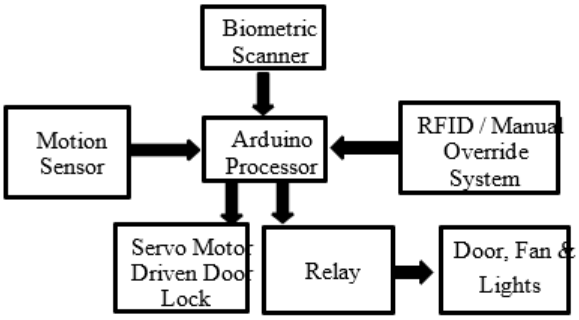

Figure 1. Block diagram of Synchronized Electronic Door System with Biometric

Figure 1 shows the operation of the synchronized electronic device control system. A biometric scanner, motion sensor, and RFID override system are devices that send data or signals to the Arduino processor, and the servo motor-driven door lock and relay are controlled by the Arduino processor. A biometric scanner identifies the specific user to be allowed to use the laboratory; a motion sensor detects movement inside the laboratory; and an RFID override system is an electronic code that is also used for security purposes. These devices send an input signal to the Arduino processor, which then performs the task that is programmed with it. The servo motor-driven door lock is used as the main lock for the doors of the laboratory, and the relay controls the electricity that is supplied to the fans and lights in order to save electrical energy. Both of these devices will work according to the Arduino program.

Project Development Procedures

The figure below depicts the development of the research, the method to be followed, and the validation of the final product of the synchronized electronic door control system with biometrics.

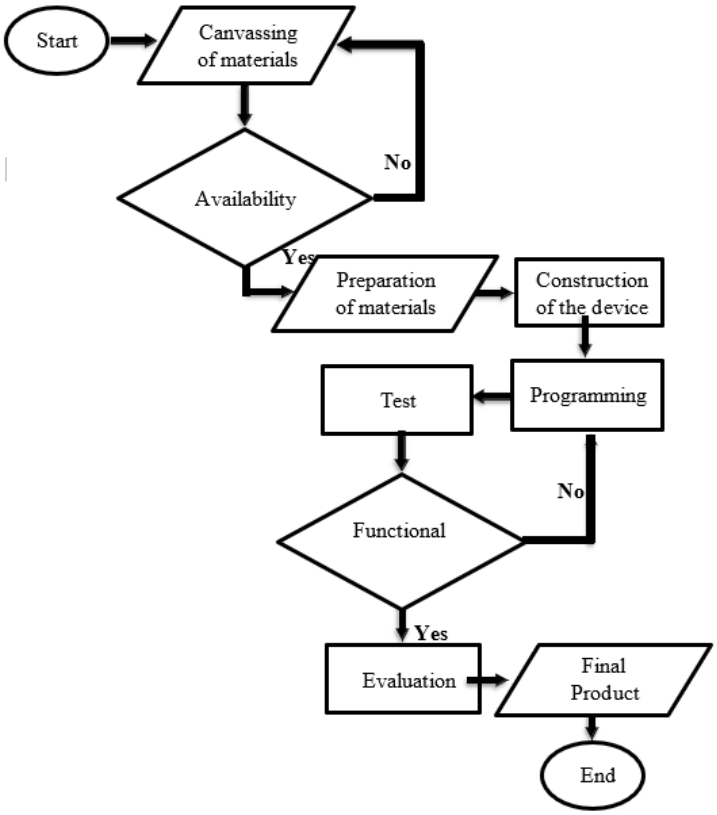

Figure 2. Flow chart for Project Development of innovation of Synchronized Electronic Device Control System with Biometric

Step 1: Canvassing of materials for the innovation of a synchronized electronic door control system with biometrics. The materials needed are an Arduino processor, a biometric scanner, a motion sensor, an RFID, a servo motor-driven door lock, and a relay.

Step 2: The availability of materials is needed for making informed decisions on how to allocate available resources to different production lines or orders efficiently.

Step 3: After the materials are available, preparation is the next thing to do, which includes purchasing all the materials for device construction.

Step 4: After the materials are purchased, next is the construction process: assembling the connections, installing automatic locks on doors, and relays controlling the laboratory's electricity supply to the wall fans and lights.

Step 5: Next is the programming process, which synchronizes all the devices controlled by the Arduino processor.

Step 6: The test process is then followed to determine if the device is functional.

Step 7: If the device is functional, it will undergo evaluation, and if not, it should be reviewed for construction and programming.

Step 8: The evaluation process takes place after it is already functional to determine its durability. The output symbol then shows the final product.

Testing and Operating Procedure

In this section, the researchers conducted testing and operating procedures to assess the reliability, functionality, and craftsmanship of the components and operations. They encountered problems along the way, which led to revisions until the project reached a good and acceptable performance level. The main objective of this project was to improve the efficiency of the synchronized electronic device control system.

Testing Procedure

The researcher is going to use a multi-tester to check the output of the synchronized electronic device system and also to check its current.

Test Run and Installation

Step 1: Power on the entire system, including the associated electronic components.

Step 2: Test the biometric access control mechanism to ensure accurate user authentication. Verify that only authorized personnel can gain access to the controlled area.

Step 3: Initiate tests to synchronize electronic devices, such as lights and fans. Confirm that devices activate upon authorized personnel entry and deactivate when the area is unoccupied.

Step 4: Evaluate the energy efficiency features by monitoring the power consumption of devices in different modes (active and inactive). Verify that energy is conserved by automatically turning off devices when the area is unoccupied.

Step 5: Verify that the system complies with regulatory requirements, particularly those related to laboratory exclusiveness and access control.

Step 6: Confirm that users, both administrators and end-users, can easily navigate and operate the system.

Step 7: Simulate various error scenarios, such as incorrect biometric input or device synchronization failure.

Step 8: Assess the system's scalability by testing its performance with an increased number of connected devices or users. Confirm that the system remains reliable and responsive as the scale increases.

Step 9: Conduct comprehensive testing to ensure that all components of the system work seamlessly together. Verify that the synchronization, access control, and energy efficiency features operate cohesively.

Step 10: Engage potential users in usability testing to gather feedback on the overall user experience. Identify areas for improvement in terms of user interactions and system responsiveness.

Step 11: Engage potential users in usability testing to gather feedback on the overall user experience.

Step 12: Identify areas for improvement in terms of user interactions and system responsiveness.

Step 13: Assess the overall performance of the system by measuring response times, data processing speeds, and other relevant performance metrics.

Operating Procedure

Step 1: Ensure all system components, including the electronic devices, are powered on.

Step 2: Initiate the biometric authentication process for authorized personnel. Prompt users to authenticate using the biometric system.

Step 3: Verify the biometric data against the authorized personnel database. Grant access upon successful authentication; deny access otherwise.

Step 4: Ensure that lights and fans turn on automatically when the user enters the controlled area.

Step 5: Monitor the energy efficiency mode to automatically turn off devices when the controlled area is unoccupied. Confirm that the system optimizes energy consumption.

Step 6: Verify that the system complies with regulatory requirements, especially regarding laboratory exclusiveness and access control.

Step 7: Interact with the user interface to navigate through system features. Confirm the user-friendliness of the interface for both administrators and end-users.

Step 8: Monitor the security features to prevent unauthorized access. Ensure that the system maintains the security and exclusivity of the controlled environment.

Step 9: Simulate error scenarios, such as incorrect biometric input or device synchronization failure. Observe how the system handles errors and provides feedback.

Step 10: Test the system's scalability by adding more connected devices or users. Verify that the system remains reliable and responsive with increased load.

Step 11: Engage users in usability testing to assess their experience with the system. Collect feedback on user interactions and the overall usability of the system.

Step 12: Measure and evaluate the overall performance of the system. Assess response times, data processing speeds, and other relevant performance metrics.

Step 13: Conduct end-to-end testing to validate the entire system's functionality, from user authentication to device control.

Step 14: Refer to system documentation, including user manuals and technical guides, for any operational guidance.

Project Evaluating Procedure

In this phase, the evaluation of the overall performance of the project had to be done to determine the project's reliability, validity, and craftsmanship, which also served as the basis for project improvement. The expert evaluator and the projected end-users of the project were the most important actors in this aspect. The researcher evaluated the project development using descriptive statistics, utilizing the Likert scale to measure acceptability in terms of the functionality, craftsmanship, and reliability of the final project outcome.

By employing these evaluation criteria, the researcher aimed to assess the project's strengths and areas for improvement comprehensively. The evaluation process involved gathering input from expert evaluators and potential end-users, ensuring a well-rounded assessment of the project's performance.

Step 1: The researchers asked for permission from the Dean of the College of Engineering Technology.

Step 2: The researchers gathered 20 respondents to answer the survey questionnaire.

Step 3: An orientation was conducted by the researchers to guide the respondents on the proper way of answering the questionnaire.

Step 4: The respondents answered the questionnaire.

Step 5: After completing the questionnaire, the researchers collected the survey questionnaires from the respondents.

Step 6: The researchers analyzed the responses.

Step 7: A report summarizing the survey results was written by the researchers.

The Synchronized Electronic Devise System underwent testing procedures, and door lock will be evaluated using the humidity sensor and multi-tester. Descriptive statistics were utilized to evaluate the Synchronized Electronic Devise System in terms of functionality, reliability, and craftsmanship.

RESULTS

Evaluation Results

The Specific Components

The materials to use in the project's development came across a variety of options. Most of the material was based on economic choice; however, the researcher did not compromise on the quality of the project.

The Design of the Project

Design a synchronized electronic device system that can accurately and securely identify authorized personnel and grant access to the laboratory. The system integrates advanced biometric identification technologies, such as fingerprints, to ensure precise and reliable authentication of authorized individuals. The design prioritizes user-friendliness and seamless integration with existing laboratory infrastructure while maintaining a high level of security and reliability.

Project Development

This process entails meticulous planning, precise component selection, and rigorous testing to ensure seamless integration with the overall system. The researcher faces challenges such as

optimizing the door lock mechanism for reliability and security, integrating it with the control system's software, and ensuring compatibility with existing hardware. However, overcoming these challenges presents opportunities for innovation and refinement, ultimately contributing to the realization of a sophisticated and efficient access control solution tailored for laboratory environments.

Functional Test Result

Several trials were being employed during functional testing and were adjusted and calibrated until the result was finally achieved.

Project Evaluation Results

The results of the reliability, functionality, and craftsmanship of the synchronized electronic device system.

- The reliability testing results show that the overall product is perceived as highly reliable by a vast majority (82%) of respondents. Similarly, questions 2 and 3 were rated as extremely reliable by 75% of respondents, respectively. Question 4 received slightly lower marks, with 65% rating it extremely reliable. Question no. 4 also has the highest standard deviation (0.845), indicating a wider range of responses compared to the other questions.
- The tables show the results of a functionality test on five questions. The majority of respondents found all questions to be extremely functional or functional. Question 4 received the highest mean rating (4.45) and question 1 received the lowest (4.3). The standard deviation for all questions ranged from 0.73 to 0.79.

The tables show results from craftsmanship testing for three questions. The respondents rated the questions on a scale likely ranging from excellent to poor. Question 1, 3, and 5 all received similar ratings, with a mean around 4.35 and a standard deviation around 0.73, though question 5 had a higher percentage of excellent ratings (60%) compared to questions 1 and 3 (50%).

DISCUSSION

The researcher’s investigation into the Synchronized Electronic Device System, conducted collaboratively by engineering instructors and students, aimed to assess user perceptions of its reliability, functionality, and craftsmanship. We employed a descriptive approach through surveys and Likert scale assessments during the second semester of the academic year (January–May 2024). The following section will summarize the key findings based on the specific objectives of the research, with a particular focus on the data presented in Tables 4.5 through 4.16.

Project Components

The researchers learned during the project's development that it would have been preferable to choose an already-assembled biometric rather than assemble it yourself.

Project Design

The designed system demonstrates its capability to fulfill the specified objectives, providing a sophisticated yet user-centric solution for access control in laboratory environments.

Project Development

Since the project was intended to automatically turn on and off, the researchers chose to utilize a type of sensor in the development of the door lock to detect whether there is movement, which suggests that there is someone inside.

Project Functionality test

Before finalizing the wiring in the product, it is best to test it to ensure that it functions.

Project Evaluation

Based on the findings of the study, the following conclusions are made:

1.1. In terms of the functionality of the product, the result was 4.7 in terms of product functionality. The interpretation is that the product is extremely functional; therefore, the automatic door lock is easy to operate properly.

1.2. In terms of reliability, the product result was 4.3, indicating that its representation was extremely reliable, making it easy to troubleshoot.

1.3. In the objective of craftsmanship, the result was 4.45, and its interpretation is excellent. The product incurs cost efficiency, and the output design is properly molded.

REFERENCES

Aman, S. (2021). Internet of Things-based intelligent smart home control system. *International Journal of Engineering Research & Technology, 2021*, Article ID 9928254. https://doi.org/10.1155/2021/9928254

Antonius, S., & Hugeng, E. (2023). Automatic door lock using microcontroller. *International Journal of Application on Sciences Technology and Engineering, 1*(1), 361–364. https://doi.org/10.1016/j.jmat.2023.05.030

Bekele, A., & Atakara, S. (2023). The impact of building on the future of architecture: A review. *II-International European Conference on Interdisciplinary Scientific Research*. Retrieved from https://ieeexplore.ieee.org/document/9928254

Cobo, D., Cabaravdic, F., & Žiga, S. (2023). Construction of an automated door as a smart device. In *New Technologies, Development and Application VI* (pp. 213-220). https://doi.org/10.1007/978-3-030-03213-7_25

Dyussembekova, Z., Westküste, M., Temirgaliyeva, B., Umyshev, A., & Shavdinova, E. (2023). Assessment of energy efficiency measures' impact on energy performance in the educational building of Kazakh-German University in Almaty. *Energy Efficiency Journal.* https://doi.org/10.1007/s12053-023-08121-6

Felisilda, D., Teodoro, M., & Julian, R. (2019). Advanced automated door lock. *Journal of Automation and Control Engineering, 7*(6), 74-80. https://doi.org/10.1093/jace/jay056

Mishra, S., Mohite, V., & Kharat, M. (2022). Smart door lock using Arduino. *International Research Journal of Modernization in Engineering Technology and Science*, 4(6), 18–22. https://doi.org/10.1093/engtec/ijrmes.2022.0123

Motwani, P., Seth, R., Dixit, A., Bagubali, S., & Rajes, K. (2021). Multifactor door locking systems: A review. *Materials Today: Proceedings, 46*(5), 350–358. https://doi.org/10.1016/j.matpr.2021.02.134

Sahu, A., Singh, N., Arya, R., & Nirala, S. (2022). Smart home automation lighting system and smart door lock using Internet of Things. *Journal of Electronics and Communication Engineering, 3*(3), 122-128. https://doi.org/10.1109/JECE.2022.1083409