

IoT Security Solutions for Students' Laboratory with RFID-based Attendance Authentication

Rose Mary A. Velasco
rosemary.a.velasco@isu.edu.ph
Isabela State University, Philippines

Abstract: The study aims to secure computer laboratories coupled with smart and automated attendance monitoring. It was designed at Isabela State University Cauayan City Campus, specifically at the Computer Laboratory of the College of Computing Studies Information and Communication Technology. The system is web-based and it can be utilized on any OS platform by specifying the IP Address through a web browser. Its function is a complete user interface for its target user's attendance monitoring and management where it can record teachers' and students' attendance, classroom entry logs, and calculation of tardiness and absences. It has the capability to retain current and previous records which could be used for future educational reference, entry log history, or for security references. The factor of acceptability as to technical support and processes of the system gained a general weighted mean of 4.35 (sd=.490) which means there is an evaluator's agreement with the functionality of the developed system based on ISO 25010 standards. The system does not physically identify the user but will only be registered in the database through scanning of the RFID tag. Furthermore, in order to achieve the objectives, The system used Php and its MySQL Local Database as its application software. Hardware components include RFID Reader and RFID Card Communication, and Arduino Uno to control Solenoid lock devices, providing security and restriction in every Computer Laboratory room.

Keywords: Internet of Things, IoT-based Security Solution, Attendance Monitoring, Smart Laboratory

INTRODUCTION

In recent years, computer laboratories have become an integral part of educational institutions, providing students with the opportunity to enhance their computer skills and access resources needed for their studies. With the growing number of students, it becomes increasingly challenging for institutions to maintain the security and management of these laboratories. Attendance monitoring is a crucial aspect of computer laboratory management, ensuring that only authorized students have access to the laboratory.

A good purpose of IoT applications in universities is that, it offers safer learning environments for students, and also serve as the students' focal point of learning. IoT in school creates smarter university as IoT devices in universities enhanced educational environments for students of all ages, where there are many creative opportunities for IoT applications to make a positive impact in school settings (Creating Smarter Schools: Benefits and Applications of IoT in Education, 2020). IoT connectivity allows for greater control over environments and processes where IoT networks offer customization and automation options that simply aren't available when devices aren't interconnected.

The purpose of the study was to develop an algorithmic prototype that would manage student attendance monitoring focusing on RFID-based Attendance Management System, as well as securing computer laboratories from students who are altering computer software, preventing computer damages due student's delinquency in using the computers in the laboratory. It specifically aimed to evaluate the designed prototype by the IT Experts and Students

stakeholders in terms of: (1) functional suitability; (2) performance suitability; (3) compatibility; (3) usability; (3) reliability; (4) portability; and (5) maintainability.

According to Doucette (2017), IoT in Higher Education has big potential if devices are kept secure by employing some basic security tips. Further, Doucette also discussed that exploring what's possible in IoT also means balancing the need for privacy and protection. IoT can conduct a risk assessment where it can perform checking of connected parts and can scan possible vulnerabilities. Like many system innovations the IoT has huge potential on university campuses if it is deployed strategically, IoT out-weights the security risks.

The integration of RFID and IoT technologies in various applications has the potential to enhance security monitoring (Srivastava et al., 2020) and improve attendance management (Wu et al., 2019) in different settings like laboratory access control (Patel et al., 2018). Some studies and research conducted on the use of RFID and IoT for computer security and attendance authentication are from Elsayed et al., (2020) which showed that the system they developed could improve student attendance rates, can track students' presence and absence in the classroom (Raut et al., 2021), and could provide validation of the access rights of student records (Wibowo & Habib, 2017).

The main purpose of the study is to develop an IoT-based computer laboratory security solutions. To provide its security and at the same time for the purpose of checking attendance, RFID cards were used that can be done by doubling the security to add code by implementing Secure Multiparty Computation (SMC), which performs simple correlations using card patterns. An RFID-based encryption algorithm is proposed to secure communication between the RFID reader and tags that provides a secure and reliable method of attendance monitoring, reducing the risk of identity and unauthorized access of computer laboratories. This process is to increase security and to prevent attendance fraud by students who can use more than one RFID card.

Technical Framework of the System

Problems arise from the vulnerability in classroom attendance and computer laboratory security in a university is the reason for the development of the system. The system revolves around the framework presented in Figures 1 and 2. It begins with the data entry to the master files in the administrator module, master files like course, year, section, laboratory rooms, and system users. The personal information together with their RFID Card/ID of students and faculty will be captured by the system. An Arduino device attached to the server computer will capture the RFID card number. The RFID numbers stored in the database/data repository of the system will be the basis of the laboratory attendance. Laboratory scheduling is based on the students' and faculty schedules for laboratory utilization and attendance.

In the process, the instructor will be the first to tap his ID on the IoT device to unlock the door security of the laboratory room. Once the door is unlocked, students can cast their attendance using their ID. The attached IoT device is connected directly to the computer server via a wireless connection. If the door is locked, unlocking is done by pressing the security key attached to the other side of the door opposite the attendance device. Students and faculty can only utilize the laboratory during their assigned schedule. Hence, both students and faculty are not allowed to utilize the computer laboratory outside their assigned schedule.

All attendances will be processed by the system to automatically generate a laboratory utilization form which can be accessed and printed by the system's administrator.

Figure 2 presents two parties involved in the system, the student and the laboratory instructor, meaning two RFID Cards will come from the student and faculty member's cards. Tapping needs to be executed first by the instructor before the students validate the secret codes hidden in the RFID for them to enter their laboratory classes. The instructor will tap his or her RFID card into the RFID reader first to have initial access to the laboratory room. Each RFID reader will be controlled by one Arduino Microcontroller. This Arduino Microcontroller is connected to a database.

In this system flowchart, the RFID tag of the teacher will be compared in the database system. Access is granted if the RFID tag matches go with the RFID tag of the students. The database system will compare and if the RFID tag is match or enrolled, Access Granted.

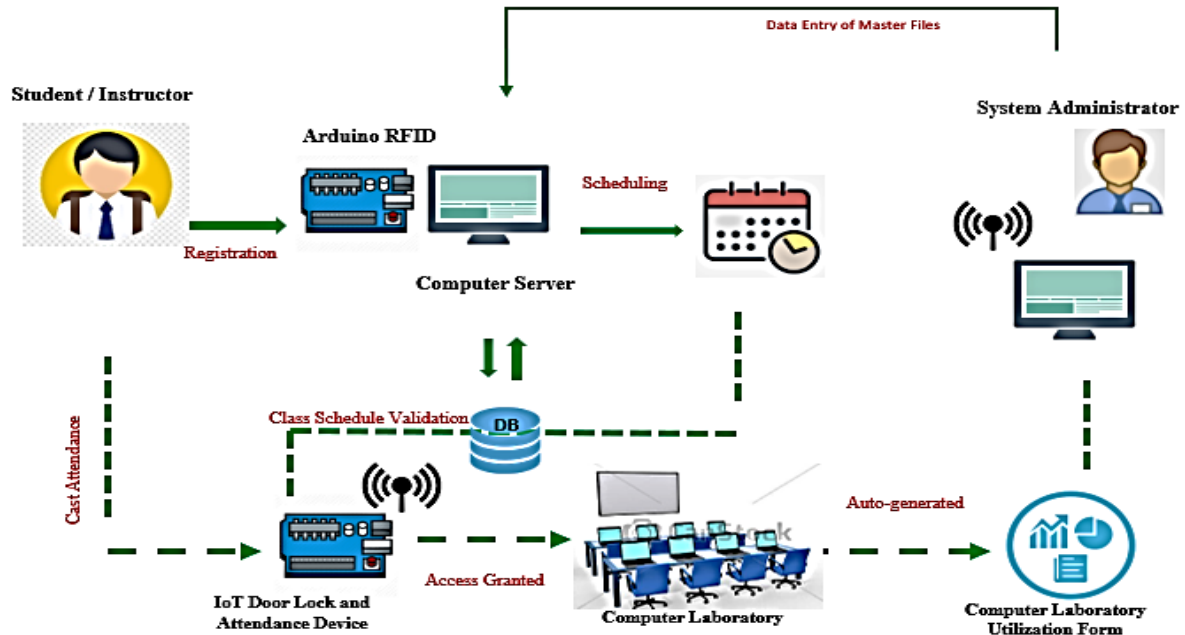


Figure 1. Technical Framework of an IoT Security Solutions for Students' Laboratory with RFID-based Attendance Authentication

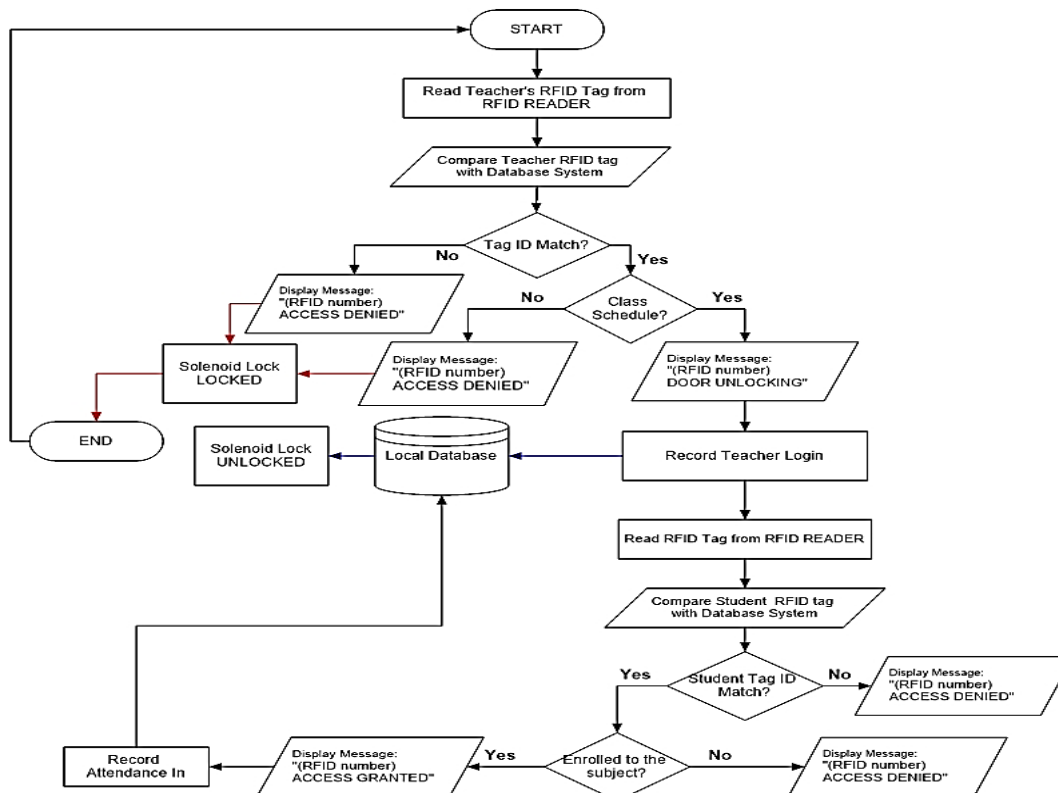


Figure 2. The System Flowchart of an IoT Security Solutions for Students' Laboratory with RFID-based Attendance Authentication

RESEARCH DESIGN & METHODS

Architecture Requirements

RFID Card

RFID cards are presented in Figure 3, student ID's are used to pair with the RFID card for the instructor for his class attendance and monitoring. RFID cards has a microchip that can store information, including user identification (UID) containing a unique code. Communication between the tag and the reader occurs wirelessly, using radio frequency technology, hence the name RFID (Putrada and Abdurohman, 2020). The communication between the tag and the reader is validated for authentication, and the proper way of authentication is to tap the RFID card to the RFID reader.

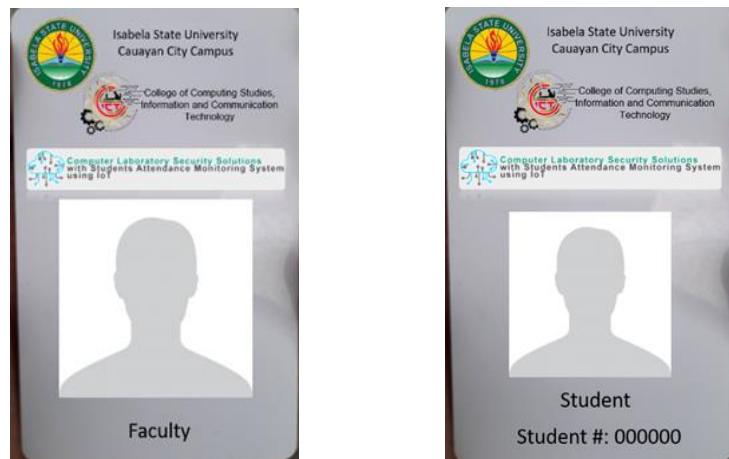


Figure 3. RFID Card used for IoT Security Solutions for Students' Laboratory with RFID-based Attendance Authentication

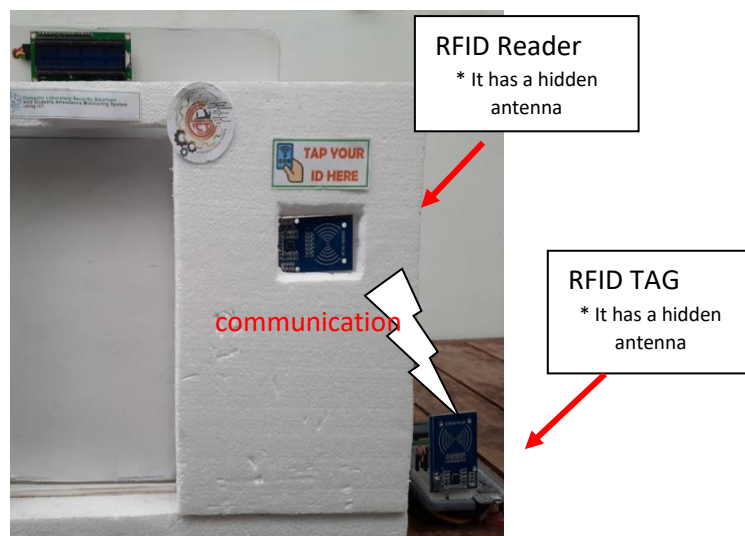


Figure 4. RFID Reader and Tag wireless communication

RFID systems have two parts, an RFID Reader serves as the key in the RFID authentication system attached to an entrance door where instructors and students will tap their RFID cards to unlock the solenoid door lock. RFID

Reader is usually a peripheral for a computer (Tan, et. al, 2018). It consists of a microprocessor or microcontroller and an antenna (Andriansyah and Subali, 2017). Fig. 4 gives an overview of an RFID reader. Another part is the antenna functions as a transmitter and receiver of radio frequency signals between RFID readers and RFID tags. RFID tags have a compact form so that this antenna is not visible (Rao, et. al, 2005). RFID card communication is passive, meaning that this card receives power from the emission of an RFID Reader signal to send data.

RESULTS AND DISCUSSIONS

The study was conceptualized to give security to computer laboratories in the university. In addition, it will eradicate the time consumed for attendance checking. The IoT-based computer laboratory security solutions will not only automate the checking of attendance but also, secures computer laboratories from students who are altering computer software. It also prevents computer damage due to students' delinquency in using computers in the laboratory.

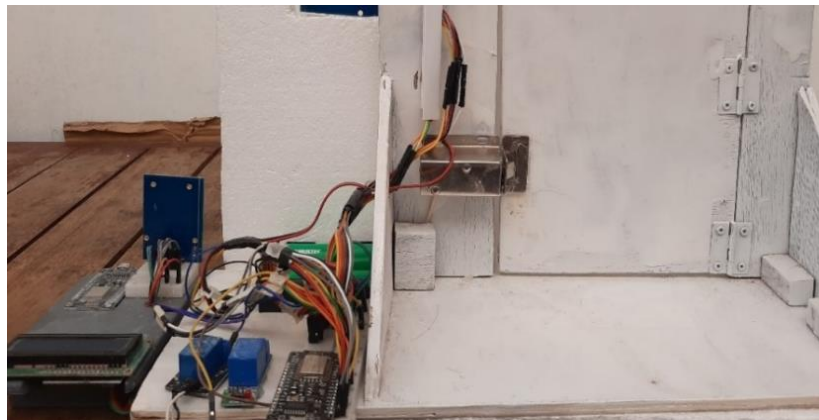


Figure 5. The prototype model of an IoT Security Solution for Students' Laboratory with RFID-based Attendance Authentication

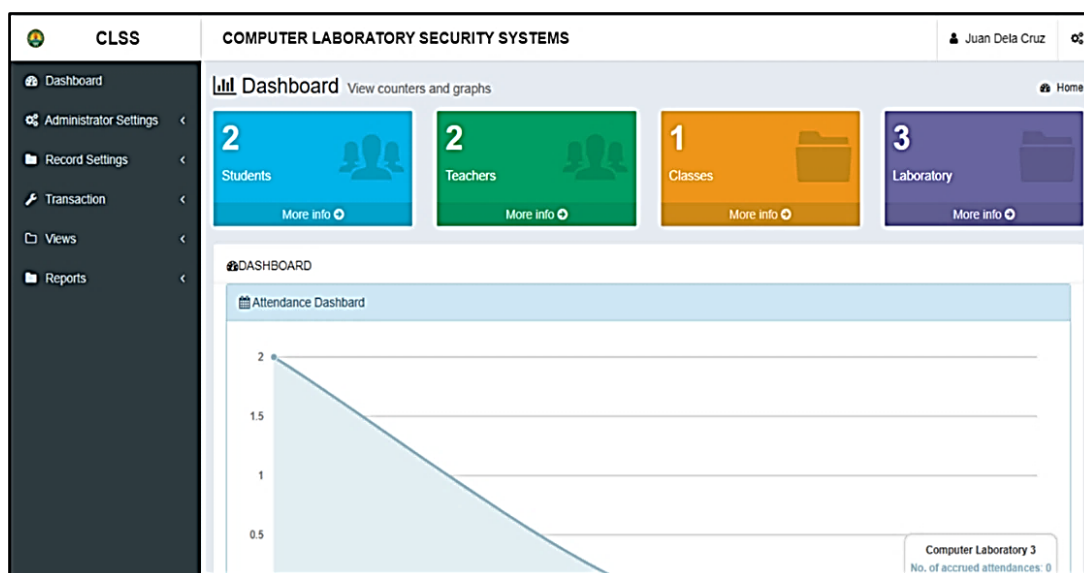
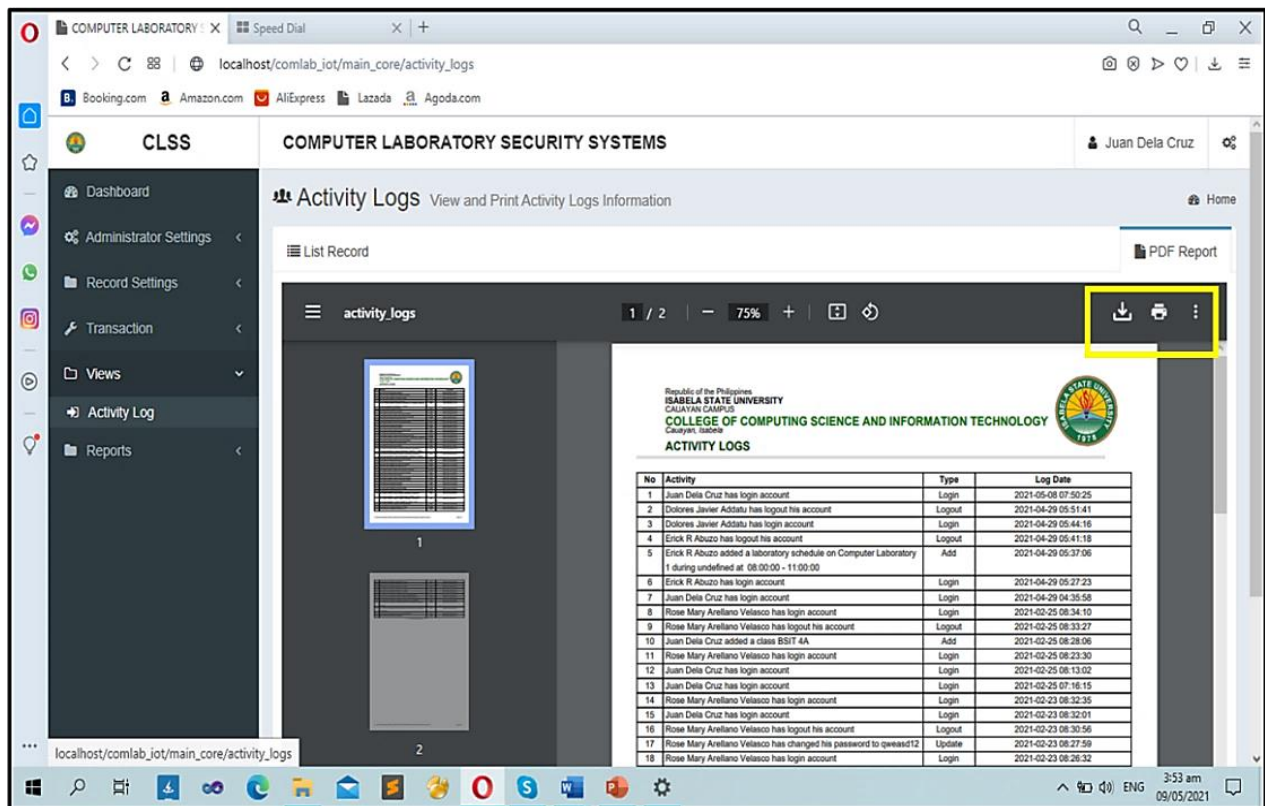


Figure 6. System Dashboard

The System Homepage

Figures 6 and 7 show the System Dashboard Access. The system has three (3) levels of security access, the Administrator level, in which admin can access all forms, the College Dean level, which can view teacher's records, classes, and schedules, and lastly, the instructor's level, which allows teachers to modify and manipulate student records such as subject and course schedule. Viewing of Reports is presented in Figure 7. These windows allow users especially the admin, dean, and teacher to view, download and print the students' attendance.



No	Activity	Type	Log Date
1	Juan Dela Cruz has login account	Login	2021-05-08 07:50:25
2	Dolores Javier Addatu has logout his account	Logout	2021-04-29 05:51:41
3	Dolores Javier Addatu has login account	Login	2021-04-29 05:44:16
4	Erick R Abuzo has logout his account	Logout	2021-04-29 05:41:18
5	Erick R Abuzo added a laboratory schedule on Computer Laboratory 1 during undefined at: 08:00:00 - 11:00:00	Add	2021-04-29 05:37:06
6	Erick R Abuzo has login account	Login	2021-04-29 05:27:23
7	Juan Dela Cruz has login account	Login	2021-04-29 04:35:58
8	Rose Mary Arellano Velasco has login account	Login	2021-02-25 08:34:10
9	Rose Mary Arellano Velasco has logout his account	Logout	2021-02-25 08:33:27
10	Juan Dela Cruz added a class BSIT 4A	Add	2021-02-25 08:28:06
11	Rose Mary Arellano Velasco has login account	Login	2021-02-25 08:23:30
12	Juan Dela Cruz has login account	Login	2021-02-25 08:13:02
13	Juan Dela Cruz has login account	Login	2021-02-25 07:16:15
14	Rose Mary Arellano Velasco has login account	Login	2021-02-23 08:32:35
15	Juan Dela Cruz has login account	Login	2021-02-23 08:32:01
16	Rose Mary Arellano Velasco has logout his account	Logout	2021-02-23 08:30:56
17	Rose Mary Arellano Velasco has changed his password to qweasd12	Update	2021-02-23 08:27:59
18	Rose Mary Arellano Velasco has login account	Login	2021-02-23 08:26:32

Figure 7. Viewing of Reports

Acceptability Evaluation of the System as to Technical Support and Process

Evaluation of the system developed was done by the seven (7) IT experts and university administrators, and thirty-two (32) students. Data were analyzed utilizing frequency count, percentages, weighted mean distribution, t-value, p-value, and standard deviation. In determining the functionality of the system, the following arbitrary scale was applied shown in Table 1.

This Internet of Things (IoT) technology has been increasingly utilized in education, including the use of RFID-based attendance authentication systems in student laboratories. In a study by Khalid et al. (2021), the authors designed and implemented an IoT-based system for attendance tracking using RFID technology. The system was found to be highly efficient, with a success rate of 98.3% and a processing time of less than a second. Another study by Alharthi et al. (2021) explored the use of IoT in laboratory safety and security, utilizing RFID technology for asset tracking and access control. The authors found that the system was able to provide real-time monitoring and enhance laboratory safety. The authors found that the system was highly efficient and effective in ensuring laboratory safety and preventing unauthorized access. These studies demonstrate the potential of IoT security solutions in enhancing performance efficiency in students' laboratories with RFID-based attendance authentication.

Table 1

Technical Evaluation of the Students and IT Experts of the College on the Developed Prototype

Factors	Type of Respondent	Mean	Standard Deviation	t-value	p-value
Functional Suitability	Student	4.463	.411	.644	.525 ^{ns}
	IT Experts/Admin	4.333	.408		
Performance Efficiency	Student	4.391	.422	.889	.382 ^{ns}
	IT Experts/Admin	4.200	.505		
Compatibility	Student	4.348	.647	1.219	.234 ^{ns}
	IT Experts/Admin	3.900	1.140		
Usability	Student	4.384	.472	-.218	.829 ^{ns}
	IT Experts/Admin	4.433	.365		
Reliability	Student	4.315	.434	1.100	.281 ^{ns}
	IT Experts/Admin	4.050	.716		
Security	Student	4.377	.441	1.171	.252 ^{ns}
	IT Experts/Admin	4.067	.894		
Maintainability	Student	4.272	.426	-1.098	.282 ^{ns}
	IT Experts/Admin	4.500	.395		
Portability	Student	4.478	.439	.821	.419 ^{ns}
	IT Experts/Admin	4.300	.447		
Overall	Student	4.379	.379	.513	.442^{ns}
	Instructor	4.223	.520		

Results have no significant difference. It shows the mean rating of both respondents has the same view about functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability.

The students rated the factor performance efficiency with a mean of 4.391 (sd=.422) while the instructor rated it with a mean of 4.200 (sd=.505). Therefore, no significant difference was found between the two ratings. Both respondents had a similar view of the system and find it to be efficient.

The functional suitability means rating from students is 4.463 (sd=.411) while the instructor gave a mean rating of 4.333 (sd=.408). No significant difference was found between the two ratings, meaning both respondents have the same view about the system in terms of functional suitability.

Several studies have explored the functional suitability of IoT security solutions in educational institutions. A study by Chouhan and Choudhary (2021) evaluated the effectiveness of an IoT-based security system in a university laboratory. The system utilized RFID-based attendance authentication to secure access to the laboratory. The authors found that the system was effective in preventing unauthorized access to the laboratory and improving the overall security of the laboratory.

The compatibility mean rating from students is 4.348 (sd=.647) while the instructor gave a mean of 3.900 (sd=1.140) in terms of compatibility. No significant difference was found between the two ratings.

A study by Tavana et al. (2021) investigated the compatibility of IoT security solutions in a university laboratory setting. The authors found that the use of standard protocols and open-source software was critical to ensuring compatibility between different IoT security systems. The study also emphasized the importance of testing and evaluation to identify and address any compatibility issues before full-scale implementation. These studies suggest that compatibility is an important consideration when implementing IoT security solutions in student laboratories with RFID-based attendance authentication and highlight the need for careful planning and testing to ensure successful implementation.

The students gave the factor usability a mean of 4.384 ($sd=.647$) and the instructor gave a mean rating of 4.33 ($sd=.365$). There is no significant difference between the two ratings. This may be because they have the same interpretation of the system in terms of usability.

The usability of Internet of Things (IoT) security solutions is an important consideration for their successful implementation in student laboratories with RFID-based attendance authentication. In a study by Kim and Huh (2020), the authors evaluated the usability of an IoT-based laboratory security system utilizing RFID-based attendance authentication. The authors found that the system was highly usable, with users reporting high satisfaction with the system's interface and ease of use. Another study by Zhang et al. (2020) evaluated the usability of an IoT-based laboratory management system, which utilized RFID technology for attendance tracking and asset management. The authors found that the system was highly usable and effective in improving laboratory management and student learning outcomes. Similarly, a study by Attri et al. (2021) investigated the usability of an IoT-based laboratory management system for a chemistry laboratory, which utilized RFID-based attendance authentication and other features such as remote monitoring and control. The authors found that the system was highly usable, with users reporting high satisfaction with the system's features and ease of use. These studies highlight the importance of considering usability in the design and implementation of IoT security solutions in student laboratories with RFID-based attendance authentication to ensure their effective adoption and use.

The students gave the factor reliability a mean of 4.315 ($sd=.434$) while the instructor gave a mean rating of 4.050 ($sd=.716$). There is no statistically significant difference between the two ratings. Both respondents have a similar interpretation of the system in terms of reliability.

Reliability is an important factor to consider when implementing IoT security solutions in student laboratories with RFID-based attendance authentication. In a study by Al-Saffar et al. (2020), the authors evaluated the reliability of an IoT-based security system for a university laboratory. The system utilized RFID-based attendance authentication, and the authors found that the system was highly reliable, with minimal errors or malfunctions reported over an extended period of use. Similarly, a study by Al-Mamun et al. (2021) investigated the reliability of an IoT-based attendance management system for a school laboratory. The system utilized RFID technology, and the authors found that the system was highly reliable, with minimal errors or malfunctions reported over a period of several months. In another study by Chen et al. (2021), the authors evaluated the reliability of an IoT-based laboratory security system utilizing RFID technology for access control and attendance management. The authors found that the system was highly reliable, with high accuracy rates and minimal errors or malfunctions reported over a period of several months. These studies highlight the importance of reliability in IoT security solutions for student laboratories with RFID-based attendance authentication and suggest that careful planning and testing are essential to ensure their successful implementation.

The students gave the factor security a mean of 4.377 ($sd=.441$) while the instructor gave a mean rating of 4.067 ($sd=.894$). Therefore, no significant difference was found between the two ratings. Both respondents have similar understanding of the system in terms of security.

The students rated the factor maintainability with a mean of 4.272 ($sd=.426$) while the instructor rated it with a mean of 4.500 ($sd=.395$). No significant difference was found between the two ratings. This may be because they have similar insights about the system.

While the use of RFID technology can improve security and streamline processes in student laboratories, it is important to consider maintainability and portability in the design and development of IoT solutions. Cheng et al. (2018) emphasize the need for IoT systems to be easily maintainable to ensure they continue to function properly and to avoid any potential security breaches. This is particularly important for solutions such as the RFID-based attendance authentication system, where any technical issues or security breaches could significantly impact the safety and security of the students and the laboratory itself.

The students gave the portability a mean of 4.478 ($sd=.439$) while the instructor gave a mean rating of 4.300 ($sd=.447$). Therefore, no significant difference was found between the two ratings. This may be because they have a similar understanding of the system, it is portable to both respondents.

The portability of IoT solutions is another critical factor that needs to be considered in the design and development of these systems. A study by Liu et al. (2019) highlights the importance of ensuring that IoT solutions are easily portable across different platforms to ensure that they can be implemented and used effectively in different environments. In the context of student laboratories, this means that the IoT solution needs to be portable across different devices and operating systems to ensure that it can be easily used by students and faculty members regardless of their device preferences or technical expertise.

CONCLUSION

IoT Security Solutions for Students' Laboratories with RFID-based Attendance Authentication paved the way to eliminate the illegal entry of students not enrolled in a particular subject, thereby maximizing the use of the computers in every class laboratory. Parallel to the laboratory solutions, automatic checking of attendance once RFID cards were tapped creating a daily database of attendance is an added formula to eliminate extra time in manually checking attendance. The university has much to do during the pandemic time, as this project formulated a model to give solutions to perennial problems of monitoring computer laboratories.

RECOMMENDATIONS

From the high results and positive responses from evaluators, it is strongly recommended that the system would further be developed and implemented in all computer laboratories of the CCSICT Cauayan Campus. Further, the system should provide access to students by viewing and monitoring their attendance in the web browser. Moreover, the system should have another platform for accessing and viewing the students' attendance such as Mobile Application (APK); and the system should also send notifications via SMS to remind the students' status in their respective course/subject using GSM Module.

REFERENCES

- Alharthi, R., Alzahrani, A., & Hussain, F. K. (2021). An IoT-based laboratory security and safety system using RFID and wireless sensor network. *Journal of Ambient Intelligence and Humanized Computing*, 12(5), 4895-4911.
- Al-Mamun, M. A., Bhuiyan, M. A. H., Uddin, M. R., & Islam, M. S. (2021). Design and implementation of an IoT-based attendance management system for school laboratories. *Journal of Sensors*, 2021.
- Andriansyah, M., Subali, M., Purwanto, I., Irianto, S. A., & Pramono, R. A. (2017). E-KTP as the basis of home security system using Arduino Uno. *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*. <https://doi.org/10.1109/caipt.2017.8320693>
- Al-Saffar, A. A., Ali, N. A., & Al-Sharafi, A. M. (2020). Evaluation of reliability of an IoT-based security system for a laboratory. *Journal of Physics: Conference Series*, 1575, 012036.
- Attri, R., Rani, R., & Varun. (2021). Design and development of an IoT based remote laboratory management system for chemistry lab. *IEEE Transactions on Education*, 64(1), 79-88.
- Chen, C., Luo, Y., Li, X., Li, Y., Li, X., & Yuan, L. (2021). An IoT-Based laboratory security system with RFID attendance management. *Journal of Sensors*, 2021.
- Cheng, Z., Zhang, L., & Wang, B. (2018). Research on the maintainability of the Internet of things based on system engineering. *Journal of Physics: Conference Series*, 1093(1), 012067. doi:10.1088/1742-6596/1093/1/012067.
- Chouhan, A., & Choudhary, A. (2021). IoT Based Security System for University Laboratory, *3rd International Conference on Computing, Communication, and Security (ICCCS)* (pp. 1-6). IEEE.
- Kim, J., & Huh, J. (2020). A usability evaluation of the IoT-based laboratory security system using RFID. *Sustainability*, 12(19), 7966.
- Khalid, M. A., Zafar, M. I., Rizwan, M., & Butt, A. R. (2021). IoT-based attendance system using RFID technology. *Journal of Information Science and Engineering*, 37(4), 1093-1103.
- Liu, Q., Cui, L., Li, S., & Chen, Y. (2019). A portable and expandable IoT platform for smart home applications. *IEEE Access*, 7, 1915-1925.
- Patel, P. R., Shah, N. P., & Thakkar, J. (2018). RFID based attendance system for computer laboratory. *International Journal of Innovative Research in Computer and Communication Engineering*, 6(2), 182-188.
- Putrada, A. G., & Abdurrohman, M. (2020). Increasing the security of RFID-based classroom attendance system with Shamir Secret Share. *International Journal on Information and Communication Technology (IJOICT)*, 6(1), 10. <https://doi.org/10.21108/ijoint.2020.61.480>



- Rao, K. V. Pavel, S., Nikitin, V., and Sander F. Lam, S. F. (2005). Antenna design for UHF RFID Tags: A review and a practical application, *IEEE Trans. Antennas Propag.*, 53(12), 3870.
- Srivastava, S., Singh, R., & Jain, A. (2020). RFID based attendance system with secure communication. *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp.1-5). IEEE.
- Tavana, M., Soleimani, H., & Saeedizadeh, E. (2021). An IoT-based smart laboratory framework for real-time data acquisition and compatibility enhancement. *Computers & Electrical Engineering*, 87, 106888.
- Wibowo, F. W., & Habib, M. (2017). A low-cost entry door using database based on RFID and microcontroller. ARPN
- Zhang, C., Li, Y., Li, H., Wang, C., Li, X., & Li, R. (2020). Development of an IoT-based laboratory management system for improving laboratory management and student learning outcomes. *IEEE Access*, 8, 157715-157726.