IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 13, No. 3, September 2024, pp. 2763~2772
ISSN: 2252-8938, DOI: 10.11591/ijai.v13.i3.pp2763-2772

Securing high-value electronic equipment: an internet of things driven approach for camera security

Siti Aminah Nordin[1,2], Zakiah Mohd Yusoff[1], Muhammad Hanif Faisal[1], Khairul Kamarudin Hasan[1]
[1]School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA (UiTM), Johor, Malaysia
[2]Microwave Research Institute, Universiti Teknologi MARA(UiTM), Selangor, Malaysia

Article Info

Article history:

Received Dec 1, 2023
Revised Feb 14, 2024
Accepted Feb 28, 2024

Keywords:

Arduino
Humidity
Internet of things design
Radio frequency identification
Storage box

ABSTRACT

This article addresses pressing challenge of securing high-value electronic equipment, notably cameras, which face dual threats of damage in high humidity conditions and theft due to their significant market value. To confront these issues, the study introduces innovative internet of things (IoT)-driven approach aimed at strengthening conventional storage box security. Central to this approach is integration of IoT technologies, such as Arduino and ESP32, to develop advanced safety storage box. This enhanced system features essential hardware components, including buzzer, password-protected keypad, radio frequency identification reader, and DHT11 sensor for humidity monitoring. Additionally, mobile alarm system is incorporated to promptly alert owners of any detected movement vibrations, thereby augmenting security measures. By leveraging these components, proposed methodology seeks to mitigate risks associated with camera theft and fungal contamination, thereby advancing electronic device security. The expected outcome is marked enhancement in protection of high-value electronic equipment, particularly cameras, through continuous real-time monitoring and proactive security measures. This research underscore's critical role of IoT technologies in fortifying security measures for valuable electronic assets, contributing significantly to ongoing discourse on innovative strategies in field. Through its comprehensive approach, this study aims to offer practical solutions to mitigate security risks and safeguard electronic equipment against potential threats, thereby addressing critical need in realm of electronic device security.

Corresponding Author:

Siti Aminah Nordin
Department of Electrical Engineering, Universiti Teknologi MARA (UiTM)
Pasir Gudang Campus, Masai 81750, Johor, Malaysia
Email: sitia181@uitm.edu.my

1. INTRODUCTION

Fungus poses a persistent and detrimental threat to optical products, particularly cameras and lenses, not only distorting image quality but also incurring exorbitant recoating costs. The insidious nature of fungus poses an ongoing and severe threat to optical devices, especially cameras and lenses. Fungal infestations not only distort the quality of captured images but also lead to substantial financial implications due to the need for costly recoating procedures [1]. The delicacy and intricacy of optical coatings amplify the challenge, making the process both technically demanding and financially burdensome.

Moreover, the escalating instances of camera theft, even within the second-hand market, exacerbate the challenges faced by photographers. The rising prevalence of camera theft, even in the secondary market, compounds the difficulties confronted by photographers. The second-hand market, typically considered a cost-effective option, is not immune to the pervasive issue of theft. This growing trend heightens the need for robust security measures to protect valuable camera equipment from unauthorized access and potential loss [2]–[4].

In response to these dual challenges, this research introduces an innovative approach that leverages internet of things (IoT) technology to fortify the security and preservation of valuable optical equipment. Recognizing the dual challenges of fungal damage and theft, this research proposes an innovative solution. By harnessing the capabilities of IoT technology, the study aims to enhance the security and preservation of valuable optical equipment. The integration of IoT offers a comprehensive and proactive approach to address both the physical degradation of lenses and the looming threat of thef [5].

The susceptibility of camera lenses to fungal infestations, combined with the persistent threat of theft, emphasizes the imperative for photographers to adopt proactive protective measures. These measures extend beyond conventional practices to embrace innovative solutions capable of addressing the evolving challenges faced by photographers in safeguarding their equipment. Esteemed camera specialists [6], [7], have extensively documented instances where photographers have incurred significant financial losses due to various factors such as fungal growth, dust accumulation, and scratches on lenses. These documented cases underscore the urgent need for effective preventive measures to mitigate the risks associated with optical equipment maintenance.

While conventional storage solutions like the VAMOS DB-25C dry box are recommended by global camera communities, their widespread adoption is impeded by challenges related to affordability and the lack of comprehensive security features. This limitation highlights the necessity for an advanced and cost-effective alternative that can address both the financial and security aspects of camera storage [4]. An innovative solution capable of overcoming these obstacles is urgently needed to ensure the effective protection and accessibility of valuable camera equipment.

To tackle the challenges posed by both fungal damage and theft, this study proposes a paradigm shift by advocating for the integration of IoT systems. The incorporation of IoT technology promises to revolutionize traditional camera storage solutions, offering a dynamic and adaptive approach to security and maintenance [8]–[12]. This innovative solution is engineered to offer timely warnings to users in response to unauthorized access or potential theft. This proactive alert system is facilitated by embedded sensors that detect vibrations, serving as a preemptive measure to safeguard valuable optical equipment. The proposed system ensures comprehensive preservation by incorporating humidity monitoring. Additionally, multi-factor authentication methods, including passwords, radio-frequency identification (RFID) cards [13]–[15], and smartphone-based authentication [16]–[18], are implemented to fortify the security layers, ensuring that only authorized users can access the equipment.

The primary aim of this project is twofold: firstly, to provide robust protection against theft, and secondly, to proactively address fungal growth on lenses. By achieving these goals, the project seeks to alleviate the financial burden linked to lens maintenance. This holistic approach aims to ensure the prolonged longevity and optimal performance of valuable optical equipment, offering a sustainable solution for photographers.

The core focus of this research is to conceptualize, design, and develop a smart storage box distinguished by advanced security features. This entails the creation of a sophisticated storage solution that not only addresses current challenges in the realm of optical equipment security but also sets a benchmark for innovation and effectiveness. Users will be afforded flexible access through a variety of secure means, including password entry, RFID cards, or smartphone authentication.

2. RELATED WORK

2.1. Smart door lock system development prototype using radio-frequency identification technology ID-12

In the pursuit of enhancing room security and unauthorized entrance detection, this study explores the utilization of an ID-12 RFID reader, Arduino Uno R3, 5V buzzer, drop bolt lock, relay module, and LCD, as highlighted in [19], [20]. The RFID technology-based system, grounded in Arduino Uno, proves versatile in securing diverse environments, encompassing homes, buildings, safes, and cars. Traditional lock systems, fraught with vulnerabilities such as key loss, easy duplication, and susceptibility to break-ins, underscore the need for technological advancements. The Arduino Uno, featuring an ATMega microcontroller, stands out for its advantages over alternative microcontroller boards. RFID technology, employing readers and transponders, facilitates data storage and retrieval through a numerical system. The primary objective of this research is to elevate the functionality of an RFID-based smart door lock system, thus contributing to the advancement of digital security technology.

Upon activation by a registered RFID card, the smart door lock system unlocks, displaying relevant information on a 16×4 LCD. Simultaneously, an audible alert sound. In contrast, an unregistered card scan maintains the door in a locked state. Additional functionalities include voltage reduction of the L7805 regulator IC and the ability to conduct RFID card scanning tests. Operational steps involve microcontroller initialization, RFID card scanning, relay module activation, buzzer alerts for unregistered cards, and storage of RFID card ID numbers. The Arduino Uno R3 microcontroller ensures accurate scanning and recognition of RFID cards. The study demonstrates the efficacy of the RFID-based smart door lock system in facilitating user identification through RFID card authentication, coupled with robust door locking mechanisms. The system emerges as a valuable security solution for organizations, boasting efficiency, efficacy, and user-friendly interfaces. Not only does it mitigate administrative costs, but it also simplifies user authentication through a mobile app interface, as highlighted in [19].

2.2. Internet of things radio-frequency identification lock door security system

The utilization of RFID technology in security systems has proven to be a pivotal asset in safeguarding workplace environments [21], [22]. This study delves into the intricate features of RFID-based security system designed to not only fortify workplace security but also provide a seamless and intuitive experience for users. The core of this system lies in its microprocessor module, intricately connected to an ESP-12E module and RFID module. The system orchestrates the functions of a buzzer and a secure door lock, employing advanced hardware components such as an input module, a robust central processing unit (CPU), a relay for efficient control, and a solenoid door lock to ensure physical security.

In an era where data security is paramount, this system adopts a sophisticated approach by securely storing user data in a Google Firebase database. This not only ensures the confidentiality and integrity of user information but also reflects the system's commitment to employing cutting-edge technologies for robust data management. The user-centric design of this RFID-based security system extends to a feature-rich mobile app interface. Users can effortlessly manage credentials and access a comprehensive history of system interactions, enhancing their ability to interact with and control the security system. This emphasis on user-friendly functionalities contribute to the system's effectiveness and practicality.

The RFID-based security system explored in this study stands as a testament to the evolution of workplace security technologies. Its sophisticated integration of hardware components, coupled with secure data management practices and an intuitive mobile app interface, positions it as a comprehensive and user-friendly solution for contemporary security challenges. The RFID-based security system is an effective and user-friendly way to keep a workplace environment secure [21]. It has a microprocessor module that connects to an ESP-12E module, an RFID module, and controls a buzzer and door lock. Data about users is kept in a Google Firebase database. The hardware of the system consists of an input module, a CPU, a buzzer, a relay, and a solenoid door lock. Through a mobile app, users have access to functions like managing credentials and seeing access history, making it simple for them to interact with the system [23].

2.3. Internet of things-based portable smart lock

In response to the escalating significance of security in contemporary society, this research, informed by a comprehensive study [22], introduces a cutting-edge portable smart lock system. This system, designed to meet the demands of heightened security, offers multiple unlocking options, including biometric fingerprint and facial recognition through a mobile application connected via Wi-Fi or Bluetooth. The innovative features include a fingerprint scanner, an Arduino Uno microcontroller, a battery, and a USB connector. Utilizing Bluetooth signals, the smart lock seamlessly connects to a smartphone app, providing users with the convenience of biometric unlocking options while proactively alerting them to unauthorized attempts. Furthermore, the system maintains a secure and accessible record of lock/unlock activities, enabling real-time monitoring from any location. Authentication for the biometric unlocking techniques involves entering biometric information, fingerprint scanning, or capturing a facial photo [22], [24].

To overcome the limitations of the local binary pattern histogram (LBPH) algorithm, this proposed system incorporates the modified local binary pattern histogram (MLBPH) algorithm. This enhancement ensures not only portability but also resilience to power failures, accompanied by improved recognition rates. The utilization of MLBPH algorithm elevates the capabilities of the smart lock, contributing to its real-time functionality and enhancing security standards.

2.4. Design of temperature and humidity monitoring terminal system based on android

This study proposes an advanced wireless monitoring system that seamlessly integrates communication and sensor technologies within the Android platform. The primary focus is on monitoring temperature and humidity, with the added advantage of adaptability through portable mobile devices. The front-end sensors within the monitoring system efficiently collect temperature and humidity data, which is then transmitted via ZigBee to a dedicated server. The mobile terminal, in turn, visualizes and displays the acquired data. The server module comprises essential components, including a ZigBee wireless module, an ARM11 CPU [25], a Wi-Fi module, memory, and a power supply.

The uniqueness of this Android-based monitoring system lies in its wireless architecture, eliminating the need for a constant connection at the sensor nodes. This feature ensures measurements are conducted without dead angles, thereby enhancing the system's overall efficiency. Noteworthy advantages include simplicity in form and usage, affordability, stability, and suitability for diverse applications, particularly in scenarios such as temperature and humidity monitoring within drug storage facilities [23]. The monitoring system employs front-end sensors to collect temperature and humidity data, establishing a robust communication link through ZigBee technology. The server module, a key element of the system, comprises crucial components like the ZigBee wireless module, an ARM11 CPU [25], a Wi-Fi module, memory, and a reliable power supply. This combination of components ensures seamless data transmission and processing.

The practicality of this Android-based monitoring system extends beyond its technological features. Its simplicity in form and ease of usage makes it accessible to a wide range of users. The affordability, stability, and adaptability contribute to its practicality, especially in critical applications such as temperature and humidity monitoring in drug storage facilities. The proposed wireless monitoring system presents a significant advancement in the field, particularly for temperature and humidity monitoring. The innovative use of the Android platform, coupled with its wireless capabilities, not only enhances data collection and transmission but also ensures practicality and applicability across diverse scenarios.

3. METHODOLOGY

The initiation of this project commenced with meticulous preparation, focusing on the identification of integral hardware components for the primary functionality of the proposed system. This encompassed the selection and detailed consideration of sensors, main controllers, and actuators. The objective was to ensure that the chosen hardware aligns seamlessly with the envisioned smart storage box. A critical phase of the methodology involved a comprehensive study and concentration on integrating the system with the IoT infrastructure. This step aimed to derive the most optimal configuration by exploring innovative ideas.

Following the hardware identification and IoT system integration, the project underwent a detailed design phase. This involved conceptualizing the entire system and formulating a robust design strategy. Subsequently, a code was developed using the C++ programming language, tailored specifically for the ESP32 microcontroller. This coding process ensured the efficient operation of the system, aligning with the project's objectives.

3.1. System architecture

Figure 1(a) illustrates the comprehensive block diagram of the project, showcasing the intricate integration of components. The system features two essential sensors, namely the vibration and DHT11 sensors, along with a keypad and RFID module. These sensors play a pivotal role in detecting vibrations resulting from any movement of the box and monitoring the humidity levels within. Specifically, the vibration sensor interfaces with the IoT through an ESP32, utilizing the Wi-Fi protocol for seamless communication. The integration of these elements ensures a robust early warning mechanism for users.

An integral aspect of the methodology involved rigorous simulations to validate the functionality and performance of the proposed system. Both individual sensor simulations and a holistic system simulation were conducted to assess and optimize the system's operational capabilities. This dual simulation approach aimed to guarantee the flawless execution of the project. To ensure the project's seamless operation, a meticulous combination of hardware and software simulations was executed. This synthesis not only verified the correct functioning of individual components but also validated the overall system's coherence. The synthesis process served as a critical step in the project's development, providing confidence in its practical implementation.

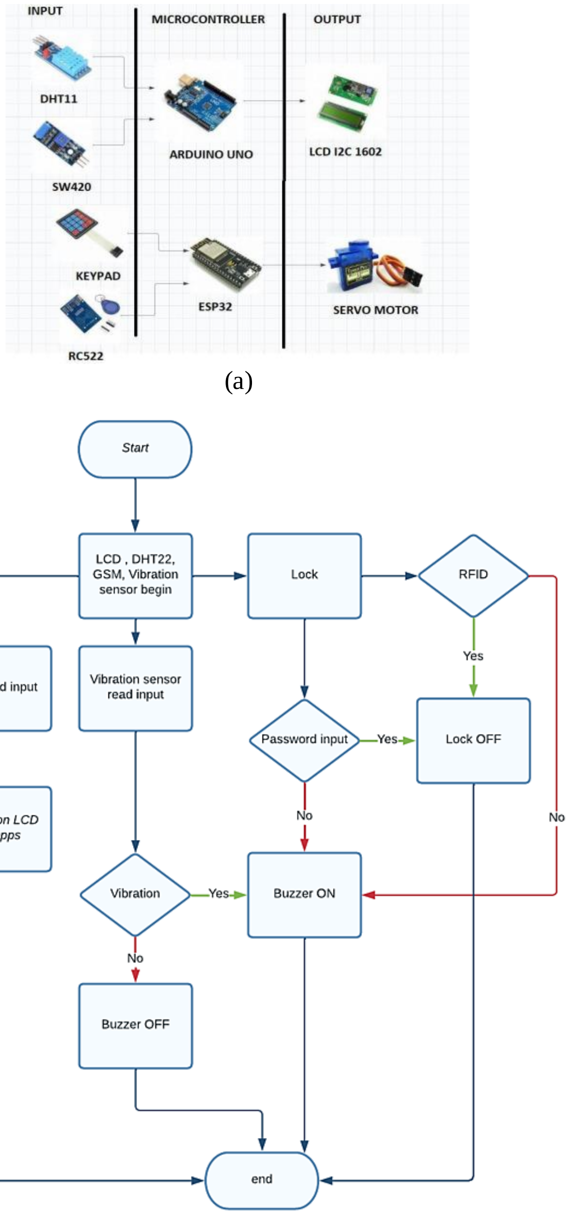
The table presented in Table 1 offers a comprehensive breakdown of the essential components employed in the project, serving as a valuable resource for understanding the hardware elements utilized. Each component is meticulously listed along with its specific function, providing transparency and clarity regarding the system's composition. For instance, the inclusion of components such as the ESP32 microcontroller, DHT22 temperature and humidity sensor, and SW-420 vibration sensor highlights the diverse range of sensors utilized for monitoring environmental conditions and detecting anomalies. Additionally, components like the LCD 1602 display screen and keypad play crucial roles in user interface and interaction with the system, enhancing its usability and functionality. Overall, the detailed listing provided in Table 1 facilitates a deeper comprehension of the project's hardware infrastructure and underscores the meticulous planning and execution involved in its development.

3.2. Project flowchart

Figure 1(b) illustrates the comprehensive flowchart outlining the research methodology employed in this study. The pivotal component of this project is the microcontroller, with the ESP32 selected for its remarkable capabilities. The ESP32 integrates 2.4 GHz Wi-Fi and Bluetooth functionalities [15] within a single chip. Utilizing TSMC's low-power 40 nm technology, it is engineered for optimal power efficiency and RF performance, ensuring adaptability and reliability in various applications and power conditions [16]. For the second function, dedicated to the alarm system, a vibration sensor has been meticulously chosen. This sensor, utilizing an LM393 comparator [17], detects vibrations in its surroundings, maintaining its state with a preset mechanism. A 10 K potentiometer enhances the sensor's sensitivity, optimizing its performance.

Table 1. List of components

Component	Function
ESP32	A microcontroller with a built-in WiFi module for accessing the WiFi network.
DHT22	A temperature and humidity sensor.
SW-420	A vibration sensor that detects abnormal vibrations.
Buzzer	Produces sound when it is in a HIGH condition.
LCD 1602	A 16×4 LCD, or liquid crystal display screen, capable of displaying 16 characters per line and having two lines in total.
GSM module	A circuit is used to establish communication between a mobile device or a computing machine and a GSM or GPRS system.
RF522	An RFID, or radio frequency identification, system consists of two main components: a tag attached to the object to be identified and a reader that reads the tag.
Keypad	A keypad is a set of buttons arranged in rows and columns.
Servo motor	A rotary actuator or linear actuator that allows for precise control of angular or linear position, velocity, and acceleration.



(a)

(b)

Figure 1. System diagram of the proposed work (a) blok diagram and (b) flow chart of the system

The third function addresses the crucial task of monitoring humidity within the box to prevent fungus growth on lenses. A digital sensor capable of sensing both humidity and temperature has been employed for this purpose. Selected for its compatibility with any microcontroller, the sensor incorporates a capacitive humidity sensing element and a thermistor for precise temperature measurements. The DHT11 sensor boasts a temperature range of 0-50 degrees Celsius with a 2-degree accuracy, while its humidity range spans from 20% to 80%, with a 5% accuracy rate. Operating at 1 Hz, it requires 3 to 5 volts, with a maximum current of 2.5 mA. In conjunction with the vibration sensor in the second function, a buzzer has been chosen for its alarm capabilities. Buzzers, serving as auditory signaling devices, are integrated with electronic transducers and a DC power source. Their versatile applications range from alarm clocks to user input feedback in electronic devices.

The main objective of this project is to secure cameras and electrical devices through an efficient locking system. To serve as the unlocking component, the MRC522 was chosen. Leveraging low-cost wireless technology known as RFID [21], this module enables the linking of numerous devices, facilitating interactions, transactions, and product authentication. The RC522, operating at 13.56 MHz, is based on the MFRC522 controller from NXP semiconductors. It supports I2C, SPI, and UART and is typically shipped with an RFID card and key fob.

4. RESULTS AND DISCUSSIONS

The simulation, as depicted in Figure 2, was meticulously executed through the utilization of Proteus software. This simulation served as a critical phase in the project, providing a controlled virtual environment to assess the seamless interaction and functionality of key components. The inclusion of a 4×3 keypad, LCD, Arduino Uno microcontroller, light emitting diode (LED), power supply, buzzer, and servo motor reflect a comprehensive approach to replicating real-world scenarios within the digital realm.

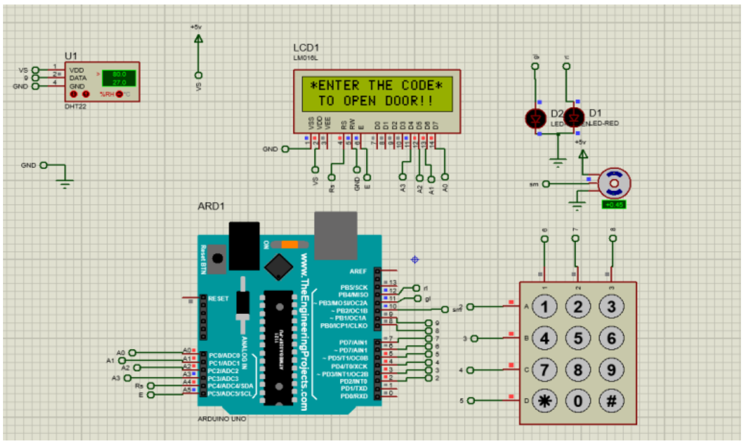


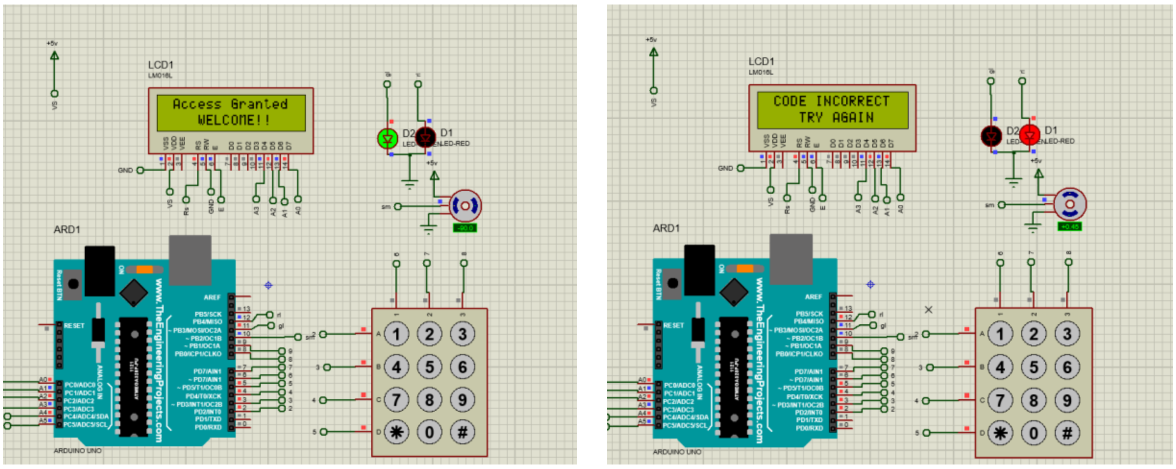
Figure 2. Simulation circuit

The 4×3 keypad, a fundamental input device, mimicked the user interface for password entry, enabling the evaluation of the system's responsiveness to user inputs. The LCD, an integral output display, provided visual feedback, crucial for user interaction and system transparency. The Arduino Uno microcontroller, acting as the brain of the system, executed programmed logic and facilitated communication between various components. The LED and buzzer, serving as output indicators, played a pivotal role in conveying system states, while the servo motor simulated a physical response, enhancing the realism of the simulation. The overarching goal of this comprehensive simulation was to validate not only individual component functionalities but also their seamless interaction within a controlled environment. The simulated scenarios encompassed various user inputs, allowing for a dynamic assessment of the system's responsiveness and reliability.

Figure 3 provides a comprehensive overview of the simulation results for both correct and wrong passwords. Figure 3(a) showcases the system's response to the successful entry of the correct password, presenting a detailed visual representation of the outcome. The LCD displays the message "access granted," accompanied by the activation of the green LED for 1 second, Figure 3(b) offers insights into the system's response when an incorrect password is entered. The LCD promptly displays "access denied," while the red LED is activated for 1 second.

Figure 3(a) offers a detailed visual representation of the outcome, specifically showcasing the system's response to the successful entry of the correct password. This pivotal moment in the simulation triggers a series of coordinated actions designed to communicate the authentication success to the user. Upon the validation of the correct password, the LCD assumes a central role in conveying the affirmative message. The LCD is programmed to illuminate the screen with the reassuring message "access granted," serving as a clear visual indicator of the system's recognition of the authorized user. This responsive display on the LCD provides immediate feedback, contributing to the overall user experience and system transparency. In conjunction with the LCD's affirmative display, the simulation orchestrates the activation of the LED for a precisely calibrated duration of 1 second. The synchronized illumination of the green LED serves as an additional visual cue, enhancing the user's awareness of successful authentication. This dual visual confirmation, through both the LCD and the green LED, ensures a robust and user-friendly feedback mechanism, reinforcing the system's responsiveness and effectiveness. This result not only validates the functionality of the password entry process but also highlights the integration and seamless coordination of hardware components in the system. The deliberate design choices, such as the duration of the green LED activation, contribute to the overall efficiency and user-centric nature of the simulated access control system.

Figure 3(b) provides a critical insight into the simulation's response when an incorrect password is entered. The orchestrated system reaction is designed to effectively communicate the denial of access to the user. In this scenario, the LCD plays a pivotal role by promptly displaying the unequivocal message "access denied." This immediate and explicit feedback on the LCD serves as a crucial indicator of the system's response to an unauthorized attempt, contributing to the overall security and transparency of the access control mechanism. Concurrently, the simulation activates the red LED for a precisely timed duration of 1 second. The illumination of the red LED serves as a visual deterrent, reinforcing the denied access status. This coordinated interplay of the LCD and red LED ensures a swift and unambiguous response to incorrect password entries, aligning with the system's security objectives.



(a) (b)

Figure 3. Simulation result for (a) correct password and (b) wrong password

Table 2 provides a detailed record of temperature and humidity data collected using the DHT11 sensor. The table showcases a time-series dataset with timestamps indicating when each measurement was recorded, alongside corresponding temperature and humidity readings. The data, meticulously logged in Microsoft Excel through Microsoft data streaming, reflects the sensor's ability to capture environmental parameters consistently and accurately over time. For instance, the recorded temperatures range from 27.5 to 29.1 degrees Celsius, while humidity levels vary between 85.2% and 93.6%. These measurements demonstrate the sensor's reliability in monitoring environmental conditions within the simulated setting. The seamless integration of this data into Table 2 underscores the sensor's effectiveness in providing valuable insights into temperature and humidity variations, thus validating its suitability for environmental monitoring applications.

Table 2. Simulation data using DHT11

Time	Temperature	Humidity
08:45:56	29.1	85.2
08:48:15	27.8	90.9
08:49:41	27.6	92.3
08:50:06	27.7	93.5
08:50:32	27.7	93.5
08:58:34	27.5	92.9
08:59:32	27.6	93.6

Table 3 provides a concise summary of troubleshooting results obtained during the observation of the system's embedded coding. Each row in the table corresponds to a specific password entered into the system, along with the resultant actions observed on the LCD display and the corresponding movement of the servo motor. The data illustrates the system's response to different password inputs, reflecting its ability to accurately process and execute commands. For instance, when the password "2345" is entered, the system grants access, displaying "access granted" on the LCD and initiating a servo motor movement of 180 degrees. Conversely, entering the passwords "1234" or "4532" results in "access denied" messages on the LCD display with no corresponding servo motor movement. This detailed record of system responses demonstrates the effectiveness of the embedded coding in accurately interpreting user inputs and executing corresponding actions, reaffirming the reliability and functionality of the coding infrastructure within the project.

Table 3. Troubleshoot result

Password entered	LCD	Servo motor movement
2345	Access granted	Move 180 degree
1234	Access denied	No movement
4532	Access denied	No movement

Figure 4 presents a graphical depiction illustrating the humidity and temperature values collected from the DHT11 sensor. The graph showcases a significant variation in humidity values, a deliberate outcome of systematic testing conducted within the specified time to evaluate the sensor's functionality. The substantial fluctuations in humidity values are attributed to the thorough testing regime applied during the simulation. Despite the simulated nature of the testing, the DHT11 sensor demonstrated commendable performance, consistently providing accurate and responsive data throughout the evaluation period. This graph serves as a visual testament to the reliability and effectiveness of the DHT11 sensor within the simulated environment. The sensor's capability to accurately capture and reflect changes in humidity, even during simulated testing, reaffirms its robust performance and aligns with the high standards set for the project.

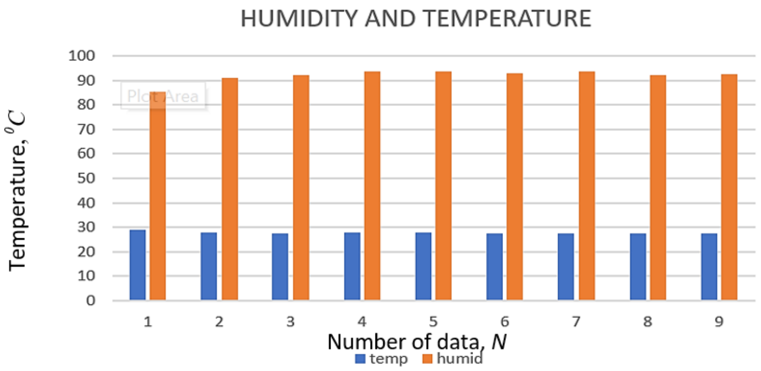


Figure 4. Graph for temperature and humidity

5. CONCLUSION

The project aimed to bolster the security of high-value electronic equipment, particularly cameras, by introducing an innovative smart storage solution. This sophisticated smart box, as demonstrated through meticulous simulation and testing, integrates vibration sensing, RFID technology, and password unlocking capabilities, offering a robust defense against unauthorized access. The inclusion of vibration sensors proves pivotal in swiftly detecting tampering attempts, while the incorporation of RFID and password systems adds personalized access management. The comprehensive simulation results, validate the effectiveness of the smart box in providing immediate feedback to users, enhancing overall security and user experience. Looking ahead, future research endeavors could explore further enhancements to the smart box's functionality and security features. For instance, investigating advanced encryption methods or integrating biometric authentication could further fortify access control mechanisms. Moreover, conducting real-world testing and user trials would provide valuable insights into usability and practicality in various environments. By continually refining and iterating upon the smart box's design and functionality, future research can ensure its relevance and effectiveness in addressing evolving security needs. In summary, the innovative smart box presented in this project offers a reliable and practical storage solution for safeguarding high-value electronic equipment. Its adaptability and cutting-edge technology position it as a highly sought-after option, providing customers with peace of mind regarding the security of their valuable possessions while also paving the way for future advancements in electronic equipment security.

ACKNOWLEDGEMENTS

The authors express their gratitude to the School of Electrical Engineering, Universiti Teknologi MARA (UiTM), Cawangan Johor, Kampus Pasir, for their support and assistance throughout this research endeavor. Furthermore, they acknowledge the financial backing provided through Grant Bestari (Grant No: 600-TNCPI 5/3/DDN (01) (004/2022)), which significantly contributed to the successful completion of this study.

REFERENCES

[1] A. Hanif *et al.*, "Assessing the impact of image quality on deep learning classification of infectious keratitis," *Ophthalmology Science*, vol. 3, no. 4, 2023, doi: 10.1016/j.xops.2023.100331.

[2] V. Nallarasan and K. Kottilingam, "Enhanced security in IoT networks using ensemble learning methods-a cognitive radio approach," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 8, pp. 4405–4412, 2020, doi: 10.30534/ijeter/2020/59882020.

[3] R. Jiao, Y. Wan, F. Poiesi, and Y. Wang, "Survey on video anomaly detection in dynamic scenes with moving cameras," *Artificial Intelligence Review*, vol. 56, no. S3, pp. 3515–3570, 2023, doi: 10.1007/s10462-023-10609-x.

[4] I. Salehin *et al.*, "IFSG: intelligence agriculture crop-pest detection system using IoT automation system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 2, pp. 1091–1099, Nov. 2021, doi: 10.11591/ijeecs.v24.i2.pp1091-1099.

[5] V. A. Kusuma, H. Arof, S. S. Suprapto, B. Suharto, R. A. Sinulingga, and F. Ama, "An internet of things-based touchless parking system using ESP32-CAM," *International Journal of Reconfigurable and Embedded Systems*, vol. 12, no. 3, pp. 329–335, Nov. 2023, doi: 10.11591/ijres.v12.i3.pp329-335.

[6] S. M. -D. L. Torre, S. L. Jacobson, M. Chodorow, M. Yindee, and J. M. Plotnik, "Day and night camera trap videos are effective for identifying individual wild Asian elephants," *PeerJ*, vol. 11, 2023, doi: 10.7717/peerj.15130.

[7] Z. Zhao, Z. Feng, J. Liu, and Y. Li, "Stand parameter extraction based on video point cloud data," *Journal of Forestry Research*, vol. 32, no. 4, pp. 1553–1565, 2021, doi: 10.1007/s11676-020-01173-z.

[8] F. A. Akgun, G. Soytürk, and M. Dede, "A new IoT system for non-contact body temperature sensing and warning," *Sigma Journal of Engineering and Natural Sciences*, vol. 41, no. 5, pp. 892–899, 2023, doi: 10.14744/sigma.2022.00070.

[9] M. Knyva, D. Gailius, G. Balčiūnas, D. Pratašius, P. Kuzas, and A. Kukanauskaitė, "IoT sensor network for wild-animal detection near roads," *Sensors*, vol. 23, no. 21, Nov. 2023, doi: 10.3390/s23218929.

[10] A. Bhardwaj, K. Kaushik, S. Bharany, and S. K. Kim, "Forensic analysis and security assessment of IoT camera firmware for smart homes," *Egyptian Informatics Journal*, vol. 24, no. 4, 2023, doi: 10.1016/j.eij.2023.100409.

[11] M. F. A. Jalil, Z. Muhammad, N. A. M. Leh, S. A. Hamid, and Z. M. Yusoff, "Water pipeline monitoring system (WPMS) via IoT," *Journal of Mechanical Engineering*, vol. 10, no. 1, pp. 293–306, 2021.

[12] Z. M. Yusoff, Y. Yusnoor, A. M. Markom, S. A. Nordin, and N. Ismail, "Fingerprint biometric voting machine using internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 699–706, 2023, doi: 10.11591/ijeecs.v30.i2.pp699-706.

[13] P. S. Kumar, A. Kumar, R. Agrawal, and P. S. Rathore, "Designing a smart cart application with zigbee and RFID protocols," *Recent Advances in Computer Science and Communications*, vol. 15, no. 2, pp. 196–206, 2020, doi: 10.2174/2666255813999200818134319.

[14] N. D. Harrison and E. L. Kelly, "Affordable RFID loggers for monitoring animal movement, activity, and behaviour," *PLoS ONE*, vol. 17, no. 10 October, 2022, doi: 10.1371/journal.pone.0276388.

[15] M. D. Tran *et al.*, "Performance analysis of automatic integrated long-range RFID and webcam system," *SN Computer Science*, vol. 3, no. 6, Sep. 2022, doi: 10.1007/s42979-022-01365-w.

[16] J. Kraushaar and S. B. -Joschko, "Smartphone use and security challenges in hospitals: a survey among resident physicians in Germany," *International Journal of Environmental Research and Public Health*, vol. 19, no. 24, 2022, doi: 10.3390/ijerph192416546.

[17] E. Morton *et al.*, "Use of smartphone apps in bipolar disorder: An international web-based survey of feature preferences and privacy concerns," *Journal of Affective Disorders*, vol. 295, pp. 1102–1109, 2021, doi: 10.1016/j.jad.2021.08.132.

[18] E. Rhee and J. Cho, "Security system using mobile image processing and color recognition for the visually impaired," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 3, pp. 1363–1368, 2022, doi: 10.11591/ijeecs.v28.i3.pp1363-1368.

[19] S. Aisyah, Y. Ali, K. Saharja, S. Suhendra, and A. Sani, "Smart door lock system development prototype using RFID technology Id-12," *Jurnal Riset Informatika*, vol. 4, no. 4, pp. 379–384, Sep. 2022, doi: 10.34288/jri.v4i4.433.

[20] C. P. Ohanu, U. O. Christiana, U. C. Ogbuefi, and T. Sutikno, "Implementation of a radio frequency identification and detection technology based digital class attendance system for university students," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 2, pp. 1206–1214, Nov. 2023, doi: 10.11591/ijeecs.v32.i2.pp1206-1214.

[21] M. K. Al-Gburi and L. A. A. -Rahaim, "Secure smart home automation and monitoring system using internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 28, no. 1, pp. 269–276, 2022, doi: 10.11591/ijeecs.v28.i1.pp269-276.

[22] J. Guntur, S. S. Raju, T. Niranjan, S. K. Kilaru, R. Dronavalli, and N. S. S. Kumar, "IoT-enhanced smart door locking system with security," *SN Computer Science*, vol. 4, no. 2, 2023, doi: 10.1007/s42979-022-01641-9.

[23] M. S. Z. M. Zabidi *et al.*, "IoT RFID lock door security system," *Journal of Physics: Conference Series*, vol. 2312, no. 1, p. 12092, 2022, doi: 10.1088/1742-6596/2312/1/012092.

[24] K. K. Rout, D. P. Mishra, and S. R. Salkuti, "Deadlock detection in distributed system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 24, no. 3, pp. 1596–1603, 2021, doi: 10.11591/ijeecs.v24.i3.pp1596-1603.

[25] K. Aravindhan, S. K. B. Sangeetha, K. Periyakaruppan, K. P. Keerthana, V. Sanjaygiridhar, and V. Shamaladevi, "Design of attendance monitoring system using RFID," in *2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS 2021*, IEEE, 2021, pp. 1628–1631. doi: 10.1109/ICACCS51430.2021.9441704.

BIOGRAPHIES OF AUTHORS

Siti Aminah Nordin is a distinguished senior lecturer currently affiliated with UiTM Pasir Gudang. She earned both her master's and Ph.D. degrees in Electrical Engineering from UiTM Shah Alam in 2014 and 2022, respectively, showcasing her commitment to academic excellence. With a specialized focus in the realm of Electrical Engineering, her research interests are notably centered around microwave filters, antennas, and electromagnetic wave area. She can be contacted at email: sitia181@uitm.edu.my.

Ts. Dr. Zakiah Mohd Yusoff is a senior lecturer who is currently working at UiTM Pasir Gudang. She received the B.Eng. in Electrical Engineering and Ph.D. in Electrical Engineering from UiTM Shah Alam, in 2009 and 2014, respectively. In May 2014, she joined UiTM Pasir Gudang as a teaching staff. Her major interests include process control, system identification, and essential oil extraction system. She can be contacted at email: zakiah9018@uitm.edu.my.

Muhammad Hanif Faisal was born in Malaysia who is currently persue his studies as an undergraduate student majoring in Electrical Engineering at UiTM Cawangan Johor, Kampus Pasir Gudang. He can be contacted at email: haniffaisal2003@gmail.com.

Khairul Kamarudin Hasan is currently a lecturer under School of Electrical Engineering, College of Engineering, UiTM, Cawangan Johor. She received her Ph.D. in Electronic Engineering from Universiti Teknikal Malaysia Melaka (UTeM) in October 2023. His research interest includes wireless power transfer, power electronics converters, and control system. He can be contacted at email: khairul@uitm.edu.my.