IoT Enhanced Lost and Found System in FTKEK Using QR Code Technology

Maizatul Alice Meor Said[1*], Mohamad Harris Misran[1], Mohd Azlishah Othman[1], Noor Azwan Shairi[1], Siti Normi Zabri[1,] Eliyana Ruslan[1], Azahari Salleh[1], Mohd Zahid Idris[2]

[1]Centre for Telecommunication Research & Innovation (CeTRI), Fakulti Teknologi dan Kejuruteraan Elektronik dan Komputer (FTKEK), Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100, Durian Tunggal, Melaka, Malaysia.

[2]Marine Engineering and ETO, Abu Dhabi Maritime Academy, 6th Streeet, Musaffah M-14, Abu Dhabi, United Arab Emirates

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.100300289

Received: 12 March 2026; Accepted: 17 March 2026; Published: 04 April 2026

ABSTRACT

The Faculty of Electronics and Computer Engineering (FTKEK) at UTeM faces operational challenges due to a traditional lost and found system reliant on manual, paper-based reporting. These conventional methods are frequently ineffective, leading to unclaimed items, high administrative workloads, and potential disputes over rightful ownership. To address these inefficiencies, this paper presents the development of an IoT-enhanced Lost and Found System utilizing QR code technology and automated hardware. The system architecture integrates a PHP-based web interface with a MySQL database managed via a local XAMPP server to provide real-time tracking and centralized data management. Hardware implementation features an Arduino Uno microcontroller, which interfaces with MG90S servo motors to control secure locker compartments and LED indicators for visual status feedback. The solution employs unique QR codes generated upon item registration to bridge digital records with physical belongings, ensuring secure verification during the recovery process. Experimental results from prototype testing confirm successful database integration and synchronized bidirectional communication between the web server and Arduino hardware at a 9600 baud rate. The outcome is a reliable, automated platform that improves recovery rates, fosters user accountability, and minimizes the risk of wrongful claims within the academic environment.

INTRODUCTION

The rapid development of the Internet of Things (IoT) has enabled the integration of physical objects with digital networks, allowing devices to communicate and exchange information autonomously. IoT technologies are widely applied in smart environments, asset management, and monitoring systems due to their ability to provide real-time data acquisition, connectivity, and automated control mechanisms. In recent years, IoT-based solutions have been increasingly adopted to address challenges related to asset tracking and object management in institutional environments such as universities, hospitals, and corporate organizations.

Internet of Things in Smart Asset and Object Tracking

IoT refers to a network of interconnected devices equipped with sensors, communication modules, and embedded systems that enable them to collect and transmit data through the internet. These devices interact with cloud platforms and databases to support real-time monitoring, automation, and intelligent decision-making processes. In asset tracking and object monitoring applications, IoT technology enables automatic identification and localization of objects, reducing human intervention and improving operational efficiency [1].

Several studies highlight the importance of IoT in improving resource management and asset visibility. Angellia et al. developed an IoT-based inventory management system integrating sensors, cloud computing, and identification technologies to automate monitoring of inventory movement and asset distribution [2]. The study reported that IoT integration significantly improved operational efficiency and enhanced data accuracy compared with manual tracking methods. The system also enabled real-time monitoring and automated recording of inventory transactions, reducing human errors and improving transparency in resource management.

Similarly, IoT-based asset monitoring systems have been implemented to track equipment and resources in various environments. Smart asset tracking solutions integrate communication technologies such as Wi-Fi, Bluetooth, LoRa, and cloud platforms to enable real-time monitoring of assets [3]. These systems provide continuous visibility of asset status and location, enabling organizations to maintain accurate records of equipment usage and movement. The integration of IoT communication networks allows asset information to be transmitted automatically to centralized databases, improving the efficiency of monitoring processes.

In addition, IoT localization technologies have been widely investigated to enhance object tracking capabilities. Location-enabled IoT systems utilize positioning techniques such as GPS, Bluetooth Low Energy (BLE), and radio signal measurements to determine the position of devices and assets in indoor and outdoor environments [4]. These technologies enable organizations to track object movement and monitor asset conditions in real time. Localization techniques also support predictive analysis and operational planning by providing contextual information regarding asset utilization and movement patterns.

QR Code Technology for Object Identification

One of the most widely adopted technologies for object identification and data retrieval in IoT systems is the Quick Response (QR) code. QR codes are two-dimensional matrix barcodes capable of storing a significant amount of information, including URLs, text data, and identifiers that link physical objects to digital databases [5].

QR codes were originally developed for the automotive industry to track vehicle components during manufacturing processes. Unlike conventional one-dimensional barcodes, QR codes encode information both horizontally and vertically, enabling them to store larger amounts of data within a compact graphical structure. In addition, QR codes include built-in error correction mechanisms based on Reed–Solomon algorithms, allowing information to be recovered even if the code is partially damaged or obscured.

Dynamic QR codes provide additional flexibility by allowing the encoded destination to be modified without replacing the printed code. In this approach, the QR code contains a redirection link connected to a cloud-based database, enabling administrators to update information associated with an object dynamically [6]. This feature is particularly beneficial in asset management systems where object information may change over time.

Several studies have explored the integration of QR codes in asset management systems. For instance, a QR-code-based asset monitoring system was developed to facilitate identification and tracking of hardware resources within organizations [7]. In this system, users can scan QR codes attached to equipment using mobile applications, allowing real-time access to asset information stored in centralized databases.

Another study proposed a QR-code-based asset management system designed using a human-centered design methodology. Each asset was assigned a unique QR code containing a web address linked to the asset database [8]. When scanned with a smartphone, the QR code automatically retrieves detailed information such as asset location, ownership details, and maintenance history. This approach significantly reduces the time required to retrieve asset data and improves the accuracy of asset records.

The combination of QR codes with IoT platforms enables seamless interaction between physical objects and digital systems. This integration provides the foundation for smart lost-and-found solutions capable of identifying and managing lost items efficiently.

IoT and QR Code Integration for Smart Systems

The integration of IoT technologies with QR codes has been widely explored in various smart applications, including access control, inventory management, and sensor network configuration. By linking QR-code identification with cloud-based IoT platforms, organizations can develop scalable systems capable of managing large numbers of objects efficiently.

One example is the use of QR codes in IoT sensor network deployment for smart buildings. In such systems, QR codes are attached to sensors and network devices to simplify device registration and configuration [9]. When a technician scans the QR code, the system retrieves configuration data from the server and automatically connects the device to the IoT network. This process simplifies the installation and management of large-scale IoT infrastructures.

QR code technology has also been applied in IoT-based security systems. A QR-based smart lock system demonstrates how QR codes can function as authentication tokens for secure access control [10]. The system integrates a microcontroller, QR scanner, and cloud database to verify user credentials in real time, improving both security and operational efficiency.

Similarly, IoT-enabled inventory management systems often employ QR codes for asset identification and monitoring. Each item is assigned a unique QR code containing information such as product ID, quantity, and registration details. When the QR code is scanned, the information is transmitted to a cloud server for processing and storage, enabling real-time monitoring of asset movement [11]. Automated QR scanning can also improve transparency and reduce manual documentation errors.

In logistics and parcel management systems, QR codes are commonly used for automated identification and tracking. During transportation, parcels are scanned to retrieve encoded destination information, allowing automated sorting and monitoring processes [12]. Integration with IoT platforms ensures that parcel information is processed and updated in real time.

These examples demonstrate that QR codes provide an effective mechanism for connecting physical objects with IoT platforms. When integrated with mobile applications and cloud databases, QR codes enable efficient object identification and information retrieval, making them highly suitable for lost-and-found applications.

Lost and Found Systems in Smart Environments

Lost items represent a common issue in public spaces and institutional environments. Universities frequently encounter cases of misplaced belongings such as laptops, student identification cards, laboratory equipment, and personal accessories. Traditional lost-and-found procedures typically rely on manual reporting and physical storage of found items, often resulting in inefficiencies and low recovery rates.

To address these limitations, several digital solutions have been proposed. Web-based lost-and-found systems allow users to report lost or found items through online platforms, enabling administrators to match reports and notify owners. However, these systems still depend heavily on manual input and lack automatic identification mechanisms.

Recent studies have explored the use of identification technologies such as QR codes and RFID to improve lost-and-found processes. A web-based lost-and-found system using QR tagging enables users to attach unique QR codes to personal belongings [13]. When an item is found, the QR code can be scanned to retrieve the owner's contact information through the system database.

Another approach integrates QR codes with IoT platforms to enable automated tracking and reporting of registered objects. Each object is assigned a unique identifier encoded within a QR code and stored in a centralized database. When scanned, the system automatically updates the object's status and location information [11].

Despite these advancements, many existing systems still lack real-time monitoring capabilities and seamless IoT integration. Furthermore, issues related to privacy, data security, and scalability remain significant challenges in implementing digital lost-and-found systems.

METHODOLOGY

The methodology for developing a fingerprint-based vehicle security system involves several critical steps, including circuit design, fabrication, component soldering, and system testing. Each stage is integral to ensuring that the system functions efficiently and reliably, providing an advanced security solution for modern vehicles. The process is broken down into four major phases: circuit design using Proteus, fabrication, soldering of components, and testing and troubleshooting.

Circuit Design Using Proteus

The first step in the development of the fingerprint-based vehicle security system is the design of the electronic circuit. Proteus, a widely used circuit simulation and PCB design tool, is employed to create the circuit schematic. The primary components in this design include the microcontroller, fingerprint sensor, LCD display, motor driver for the door lock mechanism, and relay for controlling the vehicle's ignition system.

The microcontroller is the heart of the system, responsible for processing the fingerprint data and controlling the ignition and door-lock mechanisms. In this case, the ATmega328P microcontroller is selected due to its versatility, sufficient I/O pins, and compatibility with the required sensors. The microcontroller will handle tasks such as interfacing with the fingerprint sensor, controlling the output devices (ignition relay and motor driver), and displaying system status on the LCD.

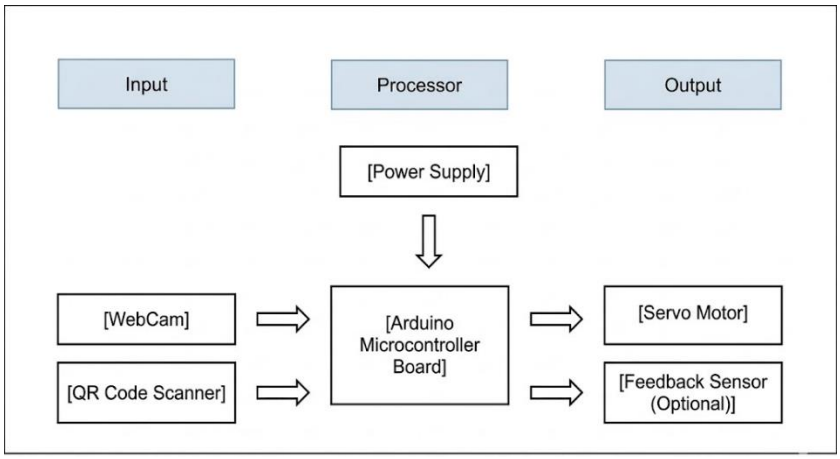


Figure 1: System framework

The microcontroller is programmed to execute several sequential operations in order to ensure reliable system functionality. The operational workflow includes the following processes:

- Initialize the QR code scanner module and establish a wireless connection to the IoT server or cloud database.
- Capture the QR code information when a user scans the tag attached to a lost item.
- Decode the QR code data to extract the unique item identification number or URL link associated with the database record.
- Transmit the scanned data to the cloud server for verification and retrieval of item information.
- Display the retrieved information on the web or mobile interface, allowing authorized personnel or users to identify the owner of the item.

The circuit in Figure 2 shows the hardware configuration of the IoT Enhanced Lost and Found System prototype. The system uses an Arduino Uno microcontroller, which acts as the central controller for processing signals and controlling output devices. The Arduino Uno, based on the ATmega328P, provides multiple digital input and output pins that allow it to interface with various electronic components in the system.

In this circuit, several LED indicators and buzzers are connected to the Arduino's digital pins. The LEDs function as visual indicators to show the status of the system, while the buzzers provide audible alerts. When a QR code is successfully verified in the lost-and-found system, the green LED lights up and the buzzer activates briefly to indicate a successful identification. Conversely, if the scanned QR code is invalid or the item is not registered in the database, the red LED lights up, indicating an error or unsuccessful verification. LEDs are commonly used as indicators in microcontroller circuits, while buzzers generate sound signals to notify users about system events.

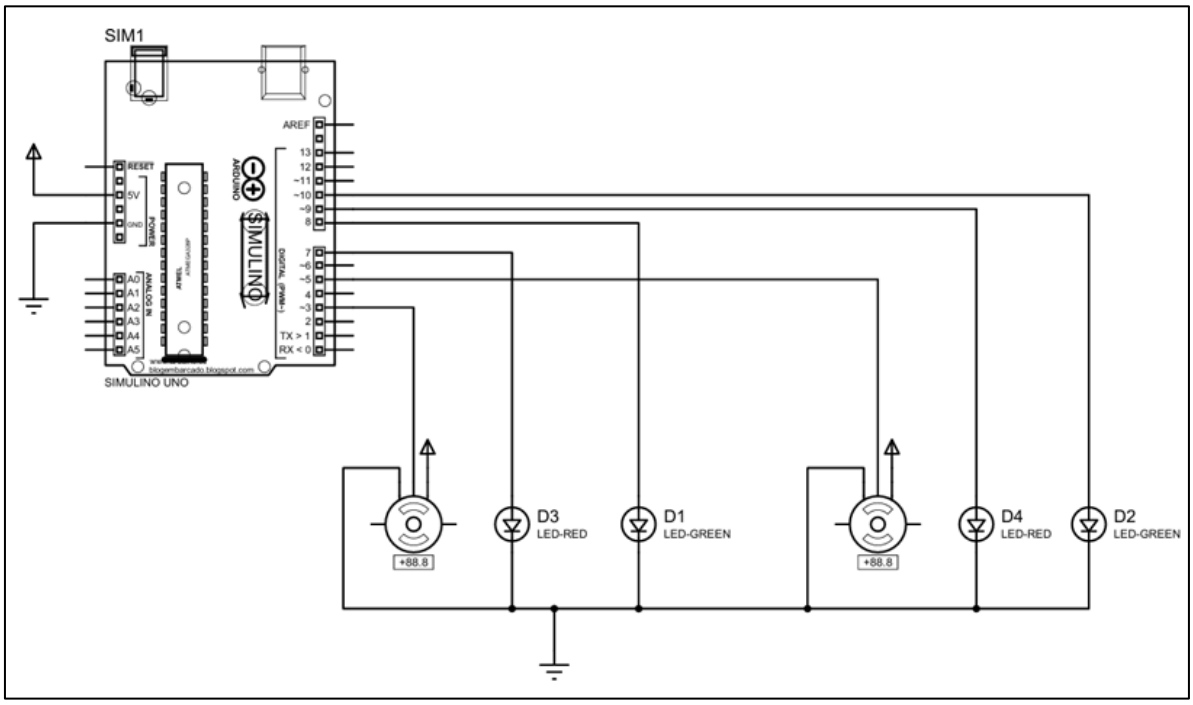


Figure 2: Proteus Software Interface

After designing the circuit schematic in Proteus, the system undergoes simulation within the Proteus environment. This simulation step allows for early detection of errors and verification of the system's functionality before physical implementation. During simulation, the behavior of the fingerprint sensor, microcontroller, motor driver, and relay is tested. The system is checked for fingerprint recognition accuracy, correct door lock operation, and ignition system control.

Prototype Design

The prototype design for this project represents the physical realization of the "Lost and Found Item using QR Code with a Safety Box" system. The design incorporates various components, including two MG90s servos, LEDs, a camera module for QR code detection, and a microcontroller to control the system's functionality. The red LED serves as the default indicator, staying on when no QR code is detected, signifying the system is idle and awaiting user input. The servos are strategically placed to interact with the safety box, moving based on QR code matches in the database.

Each locker in the system is designed to securely store a single item, ensuring its safety and minimizing the risk of theft. By assigning one item to one locker, the system guarantees that each item is isolated and accessible only to authorized users. The locker mechanism is controlled by a servo motor, which only turns on when a valid QR code is spotted and matches the database. This assures that only the rightful owner or authorized personnel can retrieve the object, further reducing the possibility of theft or tampering.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue III March 2026

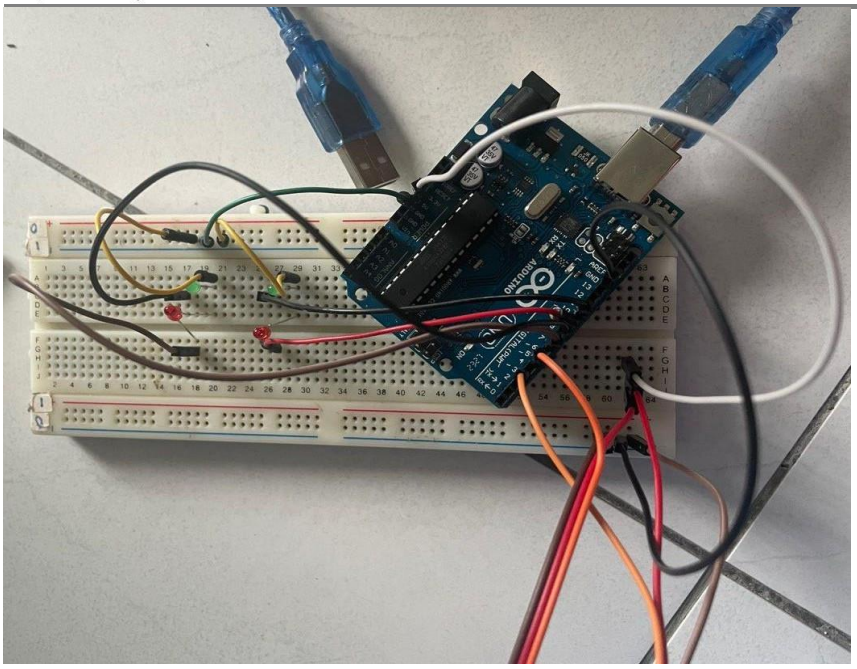


Figure 3: Circuit layout

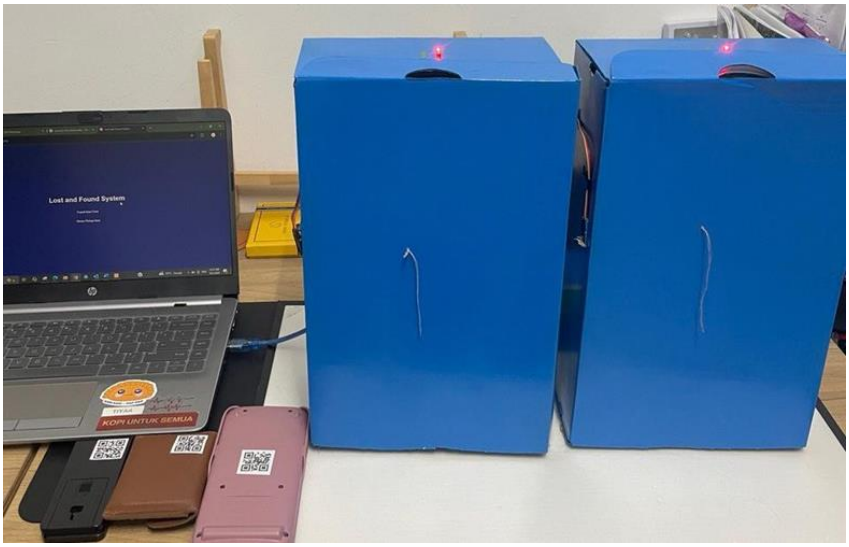


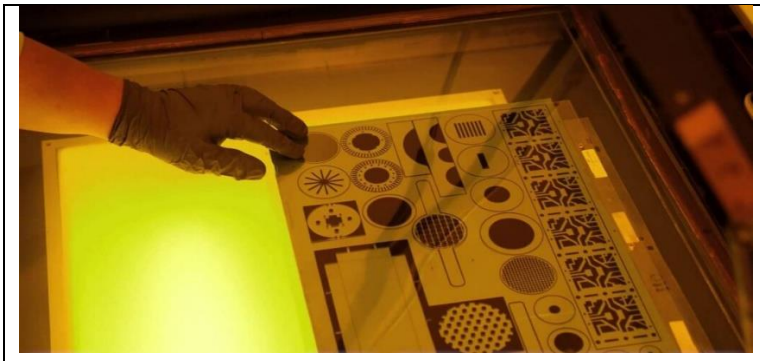
Figure 4: The design of the prototype model

As shown in Figure 4, The system integrates with a laptop, visible in the background, which presumably acts as the central control unit, running software to manage QR code scanning and database verification. The interaction between the hardware components, including LEDs, servos which acts to open and close the door lockers, and the software interface, ensures a secure and efficient item management system. The faculty can use this system to securely manage, and store found items until the rightful owner comes to claim them. This design is simple, easy to use, and reliable, making it suitable for use in a faculty environment.

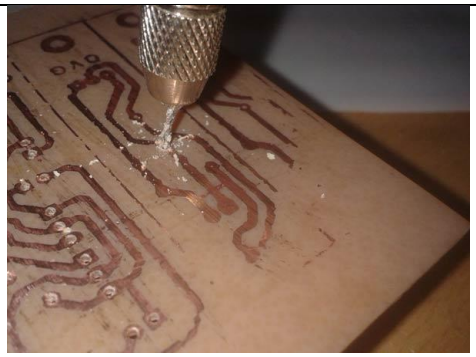
Once the circuit design has been verified through simulation, the next stage is the development of the physical hardware by designing a Printed Circuit Board (PCB) based on the circuit schematic. The PCB provides a structured platform that connects all electronic components using conductive copper traces.

The PCB layout is created using dedicated design software such as EAGLE or KiCad. In this stage, the schematic diagram is transferred into the PCB design environment, where each component is positioned and connected through routing paths. Proper component placement and trace routing are essential to ensure reliable signal transmission and to minimize electrical interference between components. Careful layout planning also improves signal integrity and overall circuit performance.

Additionally, the power supply section of the PCB is carefully designed to provide stable voltage distribution to all system components. This includes the microcontroller, QR code scanning module, and other supporting devices used in the IoT-enhanced lost and found system. After completing the layout design, the PCB files are exported for fabrication, where the circuit pattern is transferred onto copper-clad boards through processes such as etching, drilling, and solder mask application.



(a)



(b)

Figure 5: (a) Fabrication and (b) drilling process of PCB Board

After completing the PCB design, the finalized layout is sent to a PCB manufacturer for fabrication. The board is commonly produced using FR4 material due to its durability, electrical insulation properties, and cost effectiveness. During fabrication, copper layers are patterned to form conductive traces that connect the electronic components. A solder mask layer is applied to protect the copper traces from oxidation and short circuits, while a silkscreen layer is added to label component positions and circuit information. After fabrication, the PCB undergoes inspection and quality checks to ensure there are no manufacturing defects before the assembly of electronic components begins.

Testing and Troubleshooting

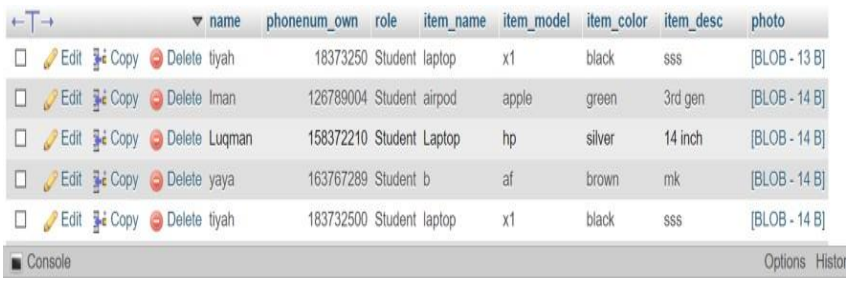
After the hardware and software implementation of the IoT Enhanced Lost and Found System in FTKEK using QR Code Technology, a comprehensive testing procedure is conducted to ensure that the system operates according to the design specifications. In IoT systems, testing is typically divided into verification and validation, where verification ensures that the hardware and software are built correctly, while validation confirms that the system performs its intended function in real operating conditions .

The first stage of testing is hardware verification. In this stage, the PCB and electronic components such as the Arduino microcontroller, LEDs, buzzers, and QR code scanner module are powered and checked individually. Electrical connections, voltage levels, and signal responses are measured to ensure that each component functions correctly. The LEDs and buzzer are activated through test firmware to verify that the microcontroller output pins are operating properly.

The second stage is module testing, where each subsystem is evaluated separately. The QR code scanning module is tested by scanning several QR codes to confirm that the encoded data can be correctly read and transmitted to the microcontroller. The microcontroller is then tested to ensure that it processes the received data and triggers the appropriate output indicators.

The final stage is system integration testing. In this stage, all components are combined to evaluate the complete workflow of the system as shown in Table 1. A QR code attached to an item is scanned, and the system verifies whether the code exists in the database. If the code is valid, the green LED and buzzer are activated, indicating successful identification. If the code is invalid, the red LED is triggered to notify the user.

Through these testing procedures, the reliability, functionality, and overall performance of the IoT-based lost and found system can be verified before deployment in the FTKEK environment.

No	Command	Status
1	Registrant information. 	Success
2	Found information 	Success

RESULT

Figure 7 shows the system flowchart of the lost and found system using QR code. The provided flowchart delineates the systematic operational logic of an automated "Lost and Found" management system, specifically designed to bridge the gap between digital database management and physical hardware execution. This architecture is built to facilitate two primary user journeys: the registration of a found item and the secure retrieval of an item by its rightful owner. By utilizing a combination of software validation and Arduino-based physical control, the system ensures a high degree of autonomy and security.

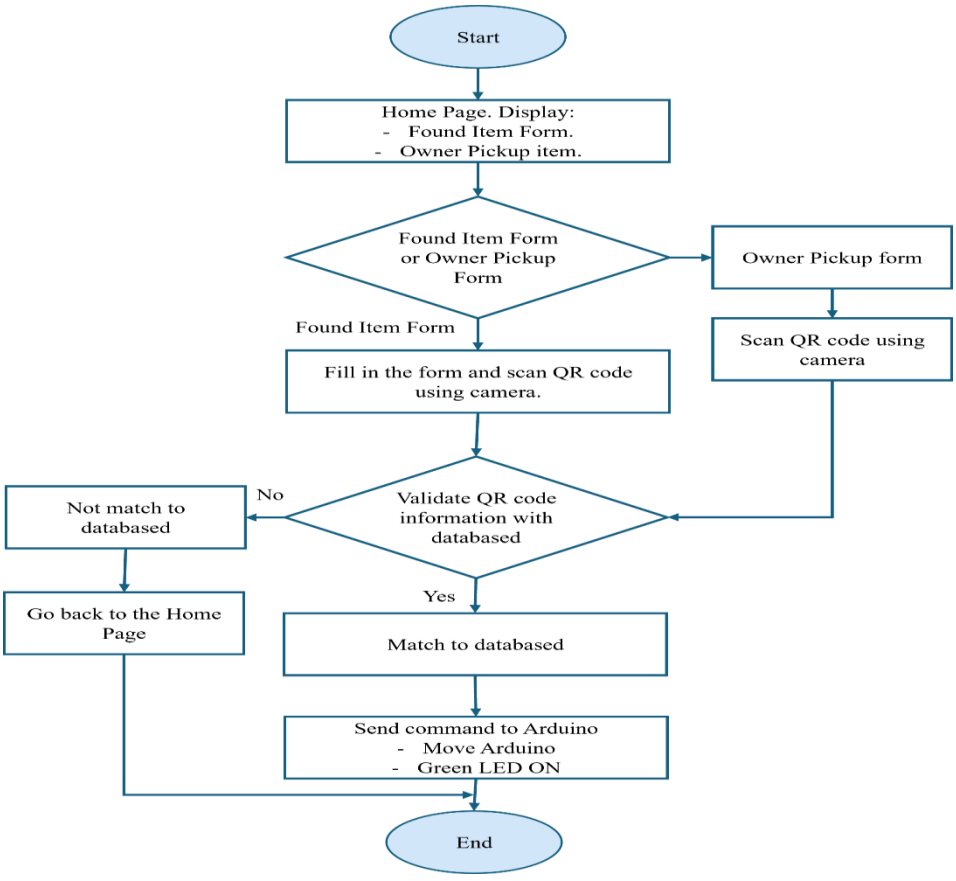


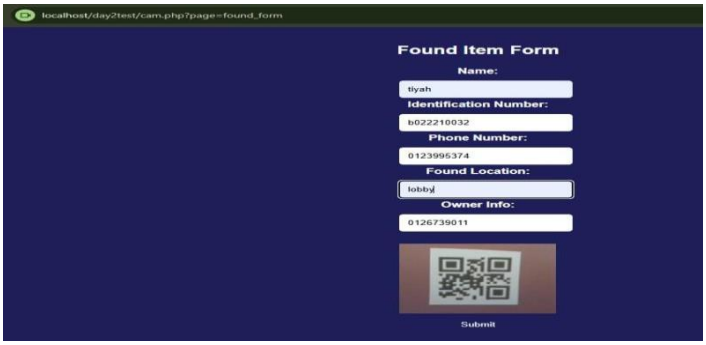
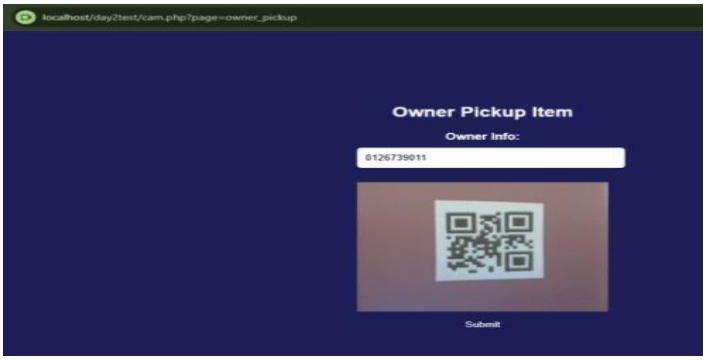
Figure 7: System Flowchart

The workflow initiates at the Start terminal, which represents the activation of the system's software environment. From this point, the user is directed to the Home Page, which serves as the primary Graphical User Interface (GUI). This interface is critical as it categorizes the user's intent into two distinct functional paths:

- Found Item Form: This path is dedicated to individuals who have discovered a lost object and intend to log it into the system for safekeeping.
- Owner Pickup Item: This path is reserved for individuals who have already been notified of a found item and possess the necessary credentials for retrieval.

The clarity of this initial stage is essential for a seamless user experience, ensuring that the subsequent data entry and validation steps are contextually relevant to the user's specific needs.

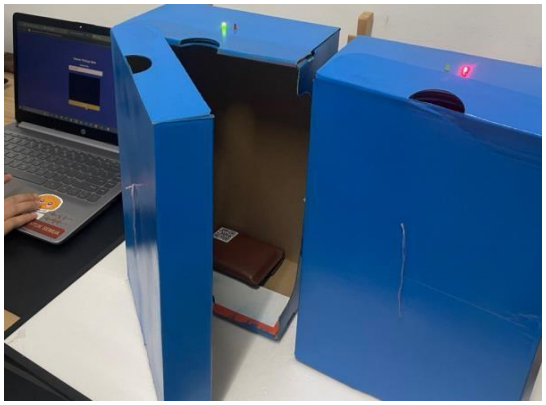
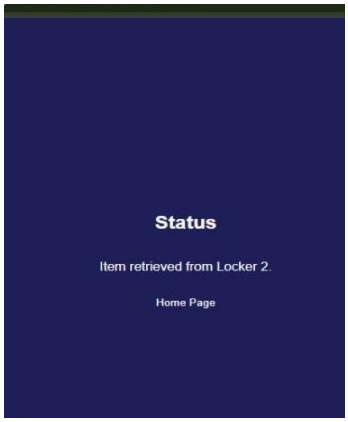
Once a selection is made at the primary decision diamond, the system enters the data acquisition phase. This phase heavily relies on the hardware components identified in the system architecture, specifically the WebCam and the QR Code identification system.

No	Command	Status
1	Register form 	Success to generate the QR code.
2	Found form 	Success to read the QR code.
3	Owner form 	Success to read the QR code.

When a user selects the "Found Item Form," they are required to perform two specific tasks:

- Form Completion: The user fills in descriptive metadata regarding the found item, such as category, color, or location found.
- QR Scanning: The user must use the integrated camera to scan a QR code. In this context, the QR code likely acts as a unique identifier for the storage locker or a tracking tag attached to the item.

If the user is an owner attempting to retrieve property, the workflow skips the descriptive form and moves directly to the Scan QR code using camera step. Here, the QR code serves as a digital "key" or claim check that was previously generated by the system when the item was first logged. This reliance on computer vision via the WebCam ensures that the input is digitized and ready for processing by the central controller.

No	Command	Status
5	First item pickup.  	Not success, the locker is not open.
6	Second item pickup  	Success, the locker is open.

The communication protocol relies on a consistent baud rate of 9600, ensuring that data is transmitted at the same speed from both ends, minimizing errors or mismatches in the information flow. Commands generated from the PHP web server are sent to the Arduino via the serial connection, where they are interpreted and executed, such as controlling the servo for locker operations or managing LED indicators. Similarly, the Arduino sends real-time feedback or status updates back to the web server, which can then reflect these updates in the user interface. This bidirectional communication ensures a highly synchronized interaction between the hardware and software, resulting in a responsive and efficient system.

The security of the lockers in this system is a significant concern, particularly as they will be placed in public spaces where they are susceptible to misuse and damage. One key vulnerability is the potential for individuals

to open a locker without depositing an item, undermining the system's intended purpose. To address this, authentication measures such as unique QR codes or one-time PINs can ensure that only authorized users access the lockers. Additionally, weight sensors or cameras inside the lockers could verify that an item has been deposited, preventing unauthorized use. These technological safeguards would enhance the system's reliability and discourage improper behaviour.

CONCLUSIONS

The implementation of this automated item management system represents a significant advancement in the integration of computer vision, centralized database management, and electromechanical control. By bridging the gap between a high-level digital interface and low-level hardware execution, the project successfully addresses the logistical challenges inherent in "Lost and Found" operations, effectively minimizing human intervention while maximizing security. The core of the system's success lies in its architectural synergy, where every digital input from the Home Page is meticulously processed and validated before a physical action is permitted. This creates a closed-loop environment where the Processor serves as the authoritative controller, ensuring that the Arduino board only triggers mechanical outputs when specific criteria are met.

A critical achievement of this work is the deployment of a dual-path workflow that accommodates both the registration of found items and the retrieval of lost property by its owner. By utilizing a WebCam to interpret QR Code data, the system transforms a physical object's identity into a digital credential that can be instantaneously cross-referenced against a database. This automated validation process acts as a sophisticated security gatekeeper; if the scanned data does not result in a match, the system prevents unauthorized access by redirecting the user back to the starting interface. This method provides a level of accountability and accuracy that traditional manual logging systems cannot match, as it relies on unique, encrypted identifiers to manage the chain of custody for every item processed.

Furthermore, the project demonstrates the practical feasibility of using accessible hardware, such as Servo Motors and LEDs, to achieve complex industrial-grade results. The Arduino board effectively translates software-based "Yes" or "No" decisions into physical reality, moving the motor to grant access and illuminating a Green LED to provide the user with immediate, positive reinforcement of a successful transaction. Supported by a dedicated Power Supply, this hardware configuration ensures the reliability and durability required for high-traffic environments. Ultimately, this system establishes a scalable and reproducible framework for smart-locker technology, proving that the combination of real-time validation and physical automation is the most efficient path forward for modern inventory and asset management solutions.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Centre for Research and Innovation Management (CRIM) and Universiti Teknikal Malaysia Melaka (UTeM) for their invaluable support throughout this project. Their resources, guidance, and encouragement played a crucial role in the successful development and implementation of this fingerprint-based access control system.

REFERENCE

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
2. Angellia, R. T. Yunardi, and F. Rahman, "IoT-based inventory management system for asset monitoring," *International Journal of Smart Technology and Management*, vol. 5, no. 2, pp. 45–52, 2021.
3. S. Shukla and A. Yadav, "IoT-based real-time tracking systems: Enhancing efficiency in dynamic supply chains," *Journal of Ad-hoc Network and Mobile Computing*, vol. 2, no. 1, pp. 1–9, 2024.
4. H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 37, no. 6, pp. 1067–1080, Nov. 2007.
5. Denso Wave Inc., "QR Code essentials," *Denso Technical Review*, vol. 13, no. 1, pp. 1–9, 2008.

6. Pesik, K. Tumiwa, and E. Edwin, "Development of QR code labeling application for fixed asset accounting information systems," *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 9, pp. 1–10, 2023.
7. P. Moonsrikaew, S. Pannakkong, and P. Torteeka, "QR code based asset management system for organizational resource monitoring," *International Journal of Computer Applications*, vol. 176, no. 21, pp. 15–21, 2020.
8. J. M. Delos Santos and R. M. S. De Guzman, "Asset management information and tracking system with QR code based on the human-centred design method," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 11, pp. 312–320, 2021.
9. S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
10. M. K. Hasan, M. M. Rahman, and M. S. Hossain, "Design of QR code based smart lock security system using IoT," *International Journal of Computer Applications*, vol. 182, no. 44, pp. 22–27, 2019.
11. P. Singh and A. Sharma, "IoT-based inventory and asset monitoring system using QR code identification," *International Journal of Research and Technology Innovation*, vol. 5, no. 4, pp. 120–126, 2023.
12. Y. Chen, Z. Li, and H. Wang, "IoT-based parcel tracking and logistics monitoring system using QR code identification," *IEEE Access*, vol. 8, pp. 134873–134882, 2020.
13. R. Patel and S. Shah, "Web-based lost and found management system using QR code tagging," *International Journal of Computer Science and Information Security*, vol. 19, no. 7, pp. 35–42, 2021.