RFID-BASED SECURE STORAGE SYSTEM FOR SCHOOL LIBRIARIES

2024/2025 ACADEMIC SESSION

DEPARTMENT OF MECHATRONICS ENGINEERING

UNIVERSITY OF BENIN

AGHADUNO HENRY IKENNA	**ENG2002526**
OSONDU FAVOUR CHUKWUEBUKA	**ENG2002584**
GODSMARK NWAKONOBI ORISAKWE	**ENG1905730**

SUPERVISED BY:

PROF. SUFIANU AUDU ALIU,

DEPARTMENT OF MECHANICAL ENGINEERING.

FACULTY OF ENGINEERING

CERTIFICATION

This is to certify that this research project titled: RFID-Based Secure Storage System was carried out by the students listed above under the supervision of Prof. Sufianu Audu Aliu

……. **Date: .....**

Prof. Sufianu Audu Aliu

Project Supervisor

……. **Date: .....**

Engr. **Godspower** **Ojariafe**

Project Coordinator

…….. **Date: .....**

Prof. **Engr.** **Ebunilo**

Head of Department

DEDICATION

We dedicate this report to God Almighty, whose grace has granted us the strength to accomplish all that was necessary for the success of this project. To our families, whose unwavering support and encouragement have been the foundation of our academic journey. To the Department of Mechanical Engineering, whose guidance and commitment to equipping us through extensive training and lectures have been pivotal in shaping us into who we are today.

ACKNOWLEDGEMENT

We wish to express our profound gratitude, first and foremost, to God Almighty.

Our heartfelt thanks go to our families for their constant love, support, and patience. Their encouragement and wise counsel have been a source of strength during the challenges we faced along the way.

We are deeply appreciative of our supervisor, Prof. Sufianu Audu Aliu for his exceptional mentorship, consistent support, and insightful feedback. His dedication played a pivotal role in making this project both educational and rewarding. We also extend our gratitude to the Department of Mechanical Engineering, University of Benin, for granting us the platform to carry out this project. The department's commitment to excellence has equipped us with the skills and knowledge necessary to undertake such an endeavor.

Likewise, we are thankful to the Faculty of Engineering for cultivating a learning atmosphere that encourages innovation, critical thinking, and professional growth. Finally, we sincerely thank all those who, in one way or another, contributed to the success of this project.

We would especially like to recognize Engr. Godspower Ojariefe, our project coordinator, whose guidance, dedication, and encouragement were invaluable throughout the project journey.

ABSTRACT

The increasing incidence of theft and mismanagement of personal belongings in school libraries has underscored the need for a reliable and secure storage solution. This project presents the design and implementation of an RFID-Based Secure Storage System developed specifically for the John Harris Library, University of Benin. The system leverages Radio Frequency Identification (RFID) technology to provide an automated, user-friendly, and efficient means of storing and retrieving students' personal items while ensuring security and accountability.

A combination of hardware and software design methodologies was adopted. The development process involved three major stages: a user perception survey, system simulation, and physical implementation. The user survey established the need for improved storage security and confirmed students' willingness to adopt an RFID-driven solution. The simulation phase, conducted using Proteus ISIS Professional, validated the system's logic, data flow, and component integration before hardware assembly. The physical prototype was implemented using an ESP32 microcontroller, RC522 RFID reader, servo-based locker mechanism, and a dual power system supported by a Battery Management System (BMS) for stable operation under varying power conditions.

Testing results revealed an average system response time of approximately two seconds and 100% tag recognition accuracy, confirming both reliability and efficiency. The dual power design eliminated voltage interference between the control unit and servo motors, while the BMS ensured safe and continuous functionality during power fluctuations. The system's performance was evaluated using theoretical frameworks such as the Technology Acceptance Model (TAM), Security Theory, and Socio-Technical Systems Theory, all of which validated its usability, security, and integration of human and technical subsystems.

The developed RFID-Based Secure Storage System successfully met its objectives of providing an automated, secure, and scalable storage solution for school libraries. It demonstrates how mechatronic engineering principles and RFID technology can be effectively combined to enhance campus security infrastructure, improve operational efficiency, and promote user trust in academic environments.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

School libraries serve as vital hubs for academic engagement, providing students with resources and spaces to foster learning and intellectual growth. However, a persistent challenge in these environments is the secure storage of personal belongings, such as bags, laptops, and books, particularly during high-traffic periods like examinations. At the Engineering Library, University of Benin, Edo State, students frequently face difficulties securing their possessions due to inadequate or manual storage systems, which increase the risk of theft, loss, or mismanagement. These issues disrupt the learning environment and detract from the library's role as a conducive space for study.

To address this challenge, this project proposes the development of an RFID-Based Secure Storage System for school libraries, leveraging Radio Frequency Identification (RFID) technology to provide an automated, secure, and user-friendly solution. By integrating RFID authentication, automated compartment assignment, and robust error-handling mechanisms, the system aims to enhance security and streamline storage management. Additionally, the project explores a pay-as-you-use service model to ensure financial sustainability, making the solution accessible to students while supporting maintenance costs. This chapter outlines the background, problem statement, objectives, research questions, scope, limitations, significance, and structure of the project, laying the foundation for the proposed system's development and evaluation.

1.2 Background of the Study

Libraries have long been recognized as essential components of educational institutions, providing students with access to knowledge and quiet spaces for focused study. However, the lack of secure storage facilities in many school libraries poses a significant barrier to creating an optimal learning environment. Students often carry valuable items, such as laptops, textbooks, and personal belongings, which require safekeeping during study sessions. In high-traffic periods, such as examination seasons, the demand for secure storage intensifies, exacerbating the limitations of existing systems. Manual storage solutions, such as open shelves or lockers managed by librarians, are prone to mismanagement, theft, or unauthorized access, while traditional lock-and-key systems are cumbersome and inefficient.

Radio Frequency Identification (RFID) technology offers a promising solution to these challenges. RFID enables contactless identification and tracking through electromagnetic fields, making it widely used in applications such as access control, inventory management, and asset tracking. In educational settings, RFID has been applied to library book management and student attendance systems, but its potential for secure storage remains underexplored. By integrating RFID readers, tags, and automated locking mechanisms, a storage system can provide secure, efficient, and scalable management of students' belongings.

At the John Harris Library, University of Benin, preliminary observations indicate that students face significant storage-related challenges, particularly during examination periods when library usage peaks. The absence of an automated, secure storage system not only risks the loss of valuable items but also places additional burdens on librarians tasked with manual oversight. This project builds on the capabilities of RFID technology to address these issues, proposing a system that enhances security, reduces manual intervention, and aligns with the needs of students and library staff.

1.3 Problem Statement

The lack of secure and automated storage systems in school libraries, such as the John Harris Library, creates significant challenges for students. Current storage solutions, often manual or inadequate, fail to provide reliable protection for personal belongings, leading to risks of theft, loss, or mismanagement. During peak usage periods, such as examinations, these issues are amplified, as students compete for limited secure spaces, resulting in disruptions to the learning environment. Furthermore, existing systems lack scalability and user-centric features, such as automated access and financial sustainability, which are critical for long-term adoption in resource-constrained educational settings. This project seeks to address these gaps by developing an RFID-based secure storage system that ensures security, efficiency, and accessibility while exploring a pay-as-you-use model to support its sustainability.

1.4 Objectives of the Study

The primary goal of this project is to design and implement an RFID-based secure storage system that addresses the storage challenges faced by students in school libraries. The specific objectives are:

1. To design and develop an RFID-based storage system for secure and efficient management of students' personal belongings in school libraries.

2. To validate the demand for such a system through a user study conducted during peak library usage periods, such as examinations.
3. To evaluate student acceptance of a pay-as-you-use service model to ensure the system's financial sustainability.
4. To develop a reliable prototype with robust error-handling mechanisms to address operational challenges, such as power outages, hardware faults, and user errors.

1.5 Research Questions

To guide the development and evaluation of the proposed system, this project addresses the following research questions:

1. What are the primary storage-related challenges faced by students at the John Harris Library during peak usage periods?
2. To what extent do students support the implementation of an RFID-based secure storage system in school libraries?
3. Are students willing to adopt a pay-as-you-use model for a secure storage service, and what are their preferred payment mechanisms?
4. How can an RFID-based storage system be designed to ensure reliability, security, and user-friendliness in a library environment?
   These questions align with the project's objectives and will be answered through user studies, system development, and prototype testing.

1.6 Scope and Limitations

1.6.1 Scope

This project focuses on the design, development, and testing of an RFID-based secure storage prototype system for the John Harris Library at the University of Benin, Edo State. The system targets small to medium-sized school libraries, with a modular design that supports scalability. The system's workflow involves user registration, RFID-based compartment assignment, automated locking, and status tracking, with a focus on user-friendliness and security.

1.6.2 Limitations

While the project aims to deliver a robust solution, certain limitations must be acknowledged:

I. The study is limited to the John Harris Library, and findings may not fully generalize to other institutions with different library setups or student demographics.
II. Budget constraints necessitate the use of cost-effective components, which may limit advanced features, such as real-time mobile app integration or cloud-based tracking.
III. Potential operational challenges, such as power outages or hardware faults, may affect system performance, though mitigated through backup batteries and error feedback mechanisms.
IV. Time constraints may restrict long-term testing of the prototype in a real-world library setting, limiting insights into its durability and scalability.
These limitations provide opportunities for future research and system enhancements.

1.7 Significance of the Study

The proposed RFID-based secure storage system offers multiple benefits for students, librarians, and educational institutions:

I. **Enhanced Security:** RFID authentication ensures that only authorized users can access assigned compartments, significantly reducing the risk of theft or unauthorized access.
II. **Efficiency:** Automated compartment assignment and status tracking minimize manual intervention, saving time for librarians and improving the user experience for students.
III. **Scalability:** The modular design allows the system to be adapted for small to medium-sized libraries, with potential for broader adoption in other educational institutions.
IV. **User-Centric Innovation:** The pay-as-you-use model aligns with student budgets, making the system accessible while generating revenue to support maintenance and scalability.
V. **Educational Impact**: By creating a secure and conducive study environment, the system supports uninterrupted learning, particularly during critical academic periods like examinations.
Beyond its practical benefits, the project contributes to the growing application of RFID technology in educational settings, offering a replicable model for addressing storage challenges in resource-constrained environments. The findings from user studies and prototype testing will provide valuable insights for researchers, library administrators, and technology developers seeking to enhance library services.

VI.

CHAPTER TWO
LITERATURE REVIEW

2.1 THEORETICAL FRAMEWORK

The theoretical framework forms the academic backbone of any research project, serving as the lens through which the study is guided, interpreted, and evaluated. For this project on an RFID Based Secure Storage System for School Libraries, the theoretical underpinning rests on multiple strands of scholarship, including information systems theory, security theory, technology adoption models, and innovation diffusion theory. These theories not only explain the functionality and relevance of RFID in organizational contexts but also highlight the factors that influence acceptance, sustainability, and efficiency of technology-driven solutions in educational settings.

2.1.1 Information Systems (IS) Theory

Information Systems Theory explains how organizations leverage information technologies to achieve operational efficiency, competitive advantage, and value creation. According to Laudon and Laudon (2020), an information system is a coordinated set of people, processes, software, and hardware designed to collect, process, store, and distribute information. The theory emphasizes that the value of technology lies not in its standalone functionality but in its ability to integrate seamlessly into organizational workflows.

In school libraries, RFID technology can be understood as a subsystem within the broader library information system. The RFID tags attached to books and storage devices act as data acquisition tools, feeding information to RFID readers. These readers transmit data to a middleware platform, which filters and forwards it to the library's database management system. Librarians and students then interact with this processed information through user interfaces for borrowing, returning, and monitoring materials. This cycle represents the input-process-output model described in IS theory, where RFID improves the speed, accuracy, and security of transactions (O'Brien & Marakas, 2019).

An essential implication of IS theory is that a technological upgrade like RFID does not operate in isolation. Its effectiveness depends on its integration with existing catalog systems, user management databases, and institutional policies. For instance, a library with outdated or fragmented database architecture may struggle to fully harness RFID's capabilities, while one

with a centralized and automated database will experience significant efficiency gains. This resonates with the IS theory principle that the *quality of information systems is directly tied to the harmony between technology, processes, and people.*

Furthermore, IS theory recognizes feedback loops in system operation. RFID systems generate real-time reports on book circulation, user activity, and potential breaches of storage security. This feedback enables library administrators to make data-driven decisions about inventory management, policy adjustments, and budget allocations. Thus, RFID is not merely a tracking tool but an enabler of strategic information management within libraries.

2.1.2 Security Theory

Security theory provides a critical framework for analyzing how systems safeguard assets against risks. Traditionally grounded in the confidentiality, integrity, and availability (CIA) triad, security theory emphasizes that effective systems must protect information and resources against both internal and external threats (Whitman & Mattord, 2021).

1. **Confidentiality**: Within a school library, confidentiality implies that sensitive data, such as student borrowing histories and administrative records, are accessible only to authorized personnel. RFID systems support confidentiality by incorporating encryption protocols in tag-to-reader communication and implementing authentication mechanisms that prevent unauthorized readers from extracting information.
2. **Integrity**: Integrity ensures that data stored in the system remains accurate and unaltered. For RFID-based storage, this means that inventory records must reflect the real-time status of library materials. Unauthorized attempts to modify records—such as falsifying borrowing logs—would compromise the integrity of the system. RFID middleware can incorporate integrity checks by logging every transaction with timestamps and user identifiers, thereby reducing opportunities for manipulation.
3. **Availability**: RFID systems must remain consistently operational to ensure that library activities, such as check-ins, check-outs, and theft prevention, are not disrupted. This requires redundant infrastructure, robust maintenance schedules, and backup power systems to guarantee high availability.

Expanding beyond the CIA triad, contemporary security theory introduces concepts such as defense-in-depth and zero-trust architecture (IEEE, 2020). Defense-in-depth suggests layering

multiple security measures such as physical barriers, surveillance cameras, RFID access restrictions, and database firewalls—to make systems resilient against breaches. Zero-trust models argue that no user or device should be trusted by default; instead, continuous verification should govern all access attempts. In a school library, this could translate into requiring librarians to authenticate through RFID badges and students to verify identities before accessing secure storage.

By applying security theory, the RFID based system is conceptualized not only as an operational improvement but also as a critical infrastructure for protecting intellectual property, physical assets, and personal data within educational institutions.

2.1.3 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis (1989), remains one of the most influential frameworks in understanding user acceptance of new technologies. TAM posits that the two primary determinants of technology adoption are perceived usefulness (PU) and perceived ease of use (PEOU). These factors shape users' attitudes toward the system, which in turn influence their behavioral intention to use it.

1. **Perceived Usefulness (PU):** If students and librarians believe the RFID system significantly enhances library security, reduces theft, and simplifies book circulation, their perception of usefulness will be high.
2. **Perceived Ease of Use (PEOU):** If the RFID system is user-friendly requiring minimal training and operating seamlessly with existing workflows it will score highly on perceived ease of use.

Later extensions of TAM, such as the Unified Theory of Acceptance and Use of Technology (UTAUT), incorporate social influence and facilitating conditions as additional factors (Venkatesh & Bala, 2008). This means that successful adoption of RFID in school libraries depends not only on the technology's features but also on institutional support, peer encouragement, and availability of training resources.

For instance, a librarian might initially resist the RFID system, perceiving it as complex. However, if peers report efficiency gains and the institution provides hands-on workshops, the librarian's likelihood of adoption increases significantly. Therefore, TAM highlights that the

technical superiority of RFID alone does not guarantee adoption it must also align with user perceptions and institutional culture.

2.1.4 Diffusion of Innovation (DoI) Theory

Everett Rogers' Diffusion of Innovation (DoI) theory (2003) provides another valuable perspective. The theory explains how new technologies spread within a social system over time. Adoption occurs through five categories of adopters: innovators, early adopters, early majority, late majority, and laggards.

In the library context, RFID technology may first appeal to innovators technologically inclined administrators seeking to modernize services. As benefits such as reduced theft and streamlined workflows become evident, early adopters (librarians and IT staff) champion the system. Eventually, the broader academic community (students and faculty) constitute the majority who normalize the technology.

DoI also emphasizes attributes influencing adoption:

I. **Relative advantage** – RFID offers significant improvement over manual cataloguing and barcode scanning.
II. **Compatibility** – The system aligns with existing library processes.
III. **Complexity** – Ease of use encourages faster acceptance.
IV. **Trialability and Observability** – Pilot programs and visible benefits (e.g., quicker book check-outs) accelerate adoption.

Thus, DoI theory helps explain how RFID can shift from an experimental initiative to a widely accepted standard in school libraries.

2.1.5 Socio-Technical Systems Theory

The socio-technical perspective, first articulated by Bostrom and Heinen (1977), argues that every technological system is embedded within a social environment. Success is determined not merely by technical design but also by how well the system aligns with organizational structures, user needs, and cultural values.

In the case of RFID in school libraries, socio-technical theory emphasizes:

3. **Technical Subsystem:** RFID tags, readers, middleware, databases, and user interfaces.
4. **Social Subsystem:** Librarians, students, administrators, and policymakers.
5. **Environmental Subsystem:** Institutional culture, budget constraints, and regulatory frameworks.

For example, a technically flawless RFID system might fail if librarians lack adequate training or if institutional policies do not clearly define user responsibilities. Conversely, strong administrative support and inclusive training programs can offset technical limitations. This theory therefore underscores the importance of holistic design, where human and organizational factors are considered as integral to system success as hardware and software.

2.1.6 Synthesis of Theoretical Perspectives

Taken together, these theories offer a multidimensional understanding of RFID based secure storage systems:

Information Systems Theory highlights integration and feedback mechanisms.

Security Theory underscores protection against risks through the CIA triad and advanced security models.

TAM explains how perceptions of usefulness and ease influence adoption.

DoI Theory situates adoption within broader social and organizational dynamics.

Socio-Technical Systems Theory emphasizes the interplay of human, technical, and environmental subsystems.

By synthesizing these perspectives, the present research positions RFID not simply as a technological upgrade but as a transformative system that requires technical robustness, institutional support, user acceptance, and cultural alignment to succeed in school library environments

2.2 CONCEPTUAL FRAMEWORK

The conceptual framework is developed to provide a clear understanding of the major concepts in this study and how they relate to one another. While the theoretical framework presents existing theories that explain the adoption and functioning of technological systems, the conceptual framework focuses on the specific components of the RFID Based Secure Storage System for School Libraries and how these components interact to achieve the objectives of the research.

This framework acts as a map that guides the entire project. It identifies the independent and dependent variables, the flow of information, and the processes involved in ensuring that library resources are secured, easily managed, and accessible only to authorized users. The conceptual framework also helps to bridge the gap between abstract theories and practical implementation by demonstrating how RFID technology can be adapted to suit the unique needs of school libraries.

2.2.1 Key Concepts in the Study

Several concepts are central to this research:

I. **Radio Frequency Identification (RFID):** RFID is the backbone of the system. It consists of tags, readers, and middleware that enable wireless communication for the purpose of identification and tracking. In this project, RFID is used to label books, student identity cards, and storage compartments, ensuring that all items are automatically monitored without the need for manual cataloging.

II. **Secure Storage:** Secure storage refers to the protection of library materials against theft, unauthorized access, and misplacement. This involves both the physical protection of resources (e.g., locked shelves or cabinets that can only be accessed through RFID authentication) and digital protection (e.g., encrypted borrowing records).

III. **Authentication and Access Control:** Only authorized users (students, librarians, or administrators) should be able to access the library's secure storage system. RFID tags and readers will serve as the authentication mechanism, reducing human error and preventing intrusions.

IV. **Database Management System (DBMS):** The DBMS stores all information related to library materials, user profiles, borrowing histories, and system logs. It is central to the

smooth functioning of the RFID system because it ensures that every activity is recorded, retrieved, and updated in real time.

V. **Library Operations:** These include borrowing, returning, cataloguing, and inventory management. In a traditional system, these processes are manual and prone to errors. The integration of RFID automates them, thereby increasing efficiency and accuracy.

2.2.2 Interaction of the Concepts

The conceptual framework shows how these concepts work together. The RFID tags serve as unique identifiers for books or storage units, and RFID readers scan these tags whenever an item is moved. The scanned data is processed by middleware and then transferred to the database. If the transaction is valid (e.g., the user is authorized), the system updates the database and allows access. If not, the system blocks the request and raises an alert.

This interaction ensures a closed-loop system where all activities are monitored, validated, and logged. Secure storage is achieved not only by preventing unauthorized physical access but also by keeping digital records intact through encryption and integrity checks. The library operations, therefore, become more reliable, transparent, and secure.

2.2.3 Proposed Model for the Study

The conceptual framework can be represented in a model that shows the relationship between the different components:

Inputs: Library resources (books, journals), RFID tags, student/library ID cards.

Processes: RFID scanning, authentication, data processing, and transaction validation.

Outputs: Secure storage of materials, accurate inventory records, reduced theft, efficient borrowing/returning system.

This model demonstrates how the independent variables (RFID technology, secure storage mechanisms, authentication processes, and database management) influence the dependent variables (library efficiency, resource security, and user satisfaction).

2.2.4 Importance of the Conceptual Framework

The conceptual framework is important because it:

1. Serves as a guide for designing the RFID system, ensuring that all components work together toward the same objectives.
2. Helps in identifying potential challenges, such as system compatibility or user resistance, before actual implementation.
3. Provides a logical structure that links theory to practice, thereby making the study academically sound and practically relevant.
4. Shows the novelty of the research by illustrating how RFID is specifically adapted to the context of school libraries rather than general information systems.

2.3 REVIEW OF RELEVANT RESEARCH WORK

A good project cannot stand in isolation; it must be built on the works of others. For this reason, it is important to look at what has already been done with RFID technology and how such studies connect to this research on secure storage systems for school libraries. This review covers six areas: RFID in library management, RFID in security and access control, database integration, use of RFID in educational institutions, challenges of adoption, and the research gaps that still exist.

2.3.1 RFID in Library Management Systems

Libraries have always faced the problem of managing large collections while serving many users at once. The introduction of RFID changed this experience by allowing books and other items to be tracked automatically. Unlike barcodes, which require direct scanning, RFID tags can be read wirelessly and in bulk. This makes circulation activities such as borrowing, returning, and shelf-reading faster and less stressful for both staff and users.

Boss (2009) observed that libraries adopting RFID reported shorter queues at circulation desks and faster book check-ins. Similarly, Want (2006) [IEEE] explained that handheld RFID readers make it possible to scan entire shelves without picking books one by one. Singh and Mahajan (2016) also confirmed this in a study of Indian university libraries, noting that cataloguing time was reduced by almost half when RFID was introduced.

The benefits go beyond speed. Gupta and Kohli (2018) emphasized that RFID frees librarians from repetitive manual work, giving them more time to help students and researchers. Still, the

cost of implementing RFID remains a concern. Ahsan et al. (2019) noted that many libraries, especially in developing countries, hesitate to adopt RFID due to financial and technical constraints.

2.3.2 RFID in Security and Access Control

Apart from making library processes faster, RFID has also been used to improve security. Libraries often struggle with theft or unauthorized borrowing, and RFID has proven to be an effective tool against this. RFID enabled gates and sensors can detect when an item is leaving the library without proper checkout.

Juels (2006) [IEEE] pointed out that RFID cards are widely used in offices and banks for access control, showing how the same technology can be applied in libraries. Chachra and Verma (2015) found that installing RFID security gates in a university library reduced missing books by more than 50% within the first year. Likewise, Cho and Kim (2018) demonstrated that integrating RFID tags with alarms discouraged theft in public libraries.

However, security concerns still exist. Karygiannis et al. (2007) explained that RFID signals can be intercepted, which could lead to cloning of tags. Weis et al. (2003) [IEEE] recommended encryption and two-factor authentication as solutions to these problems. For school libraries, this is particularly important since students are young users who may not fully understand the risks of compromised RFID cards.

2.3.3 RFID and Database Integration

An RFID system cannot function properly without a reliable database. The tags and readers only capture raw data; it is the database and middleware that process and organize this data into useful information. For example, when a student borrows a book, the RFID reader captures the tag ID, sends it to the middleware, and updates the central library database instantly.

Leong et al. (2012) [IEEE] explained that middleware is responsible for filtering data, preventing errors such as duplicate scans. Ngai et al. (2008) added that database integration allows libraries to handle very large volumes of transactions daily without delays. In one study, Chowdhury and Bhatnagar (2017) showed that RFID linked databases enabled libraries to run analytics such as identifying most-borrowed books and detecting suspicious borrowing patterns.

The implication for school libraries is clear: RFID is not just about tracking it can also provide insights into how students use resources, which can help administrators make better decisions.

2.3.4 RFID in Educational Institutions

RFID has been tested in many educational environments with promising results. In Malaysia, Abdullah et al. (2011) reported that students adapted quickly to RFID-based borrowing in school libraries, finding the system easy to use and faster than traditional checkouts. In Nigeria, Ezeani and Igwesi (2012) studied RFID adoption in university libraries and observed smoother circulation but also resistance from some staff due to lack of technical skills.

Stańczyk (2014) examined RFID use in Polish academic libraries and found that while students embraced the technology, limited funding prevented full implementation. This shows that financial constraints are not unique to developing countries. Across different case studies, it is clear that RFID can transform how libraries serve students, but successful adoption requires adequate funding, training, and management support.

2.3.5 Challenges of RFID Adoption

Although RFID brings many benefits, there are still obstacles that need to be addressed.

1. **Technical challenges:** RFID signals can be affected by certain materials like metal or liquids. Klaus et al. (2010) explained that closely packed shelves sometimes interfere with accuracy. Another problem is tag collision, where multiple tags respond at once, confusing the reader (Want, 2006).
2. **Social challenges:** Privacy remains a big issue. Garfinkel et al. (2005) [IEEE] noted that tags can be read without the owner's knowledge, raising ethical concerns. In a school library, there is also the risk of students misusing or losing RFID enabled cards.
3. **Financial challenges:** Singh and Mahajan (2016) pointed out that the high cost of RFID tags, readers, and maintenance discourages many institutions from adopting the technology. For schools that already struggle with limited budgets, this is a serious consideration.

2.3.6 Research Gaps

From the reviewed studies, it is clear that RFID has been applied in many ways, but some areas remain underexplored. First, most works either focus on circulation efficiency or theft

prevention, but very few combine both aspects into a single solution that includes **secure** storage and authentication. Second, most studies emphasize university or public libraries, while secondary school libraries where security and accountability are also important receive little attention.

Furthermore, while researchers have raised concerns about RFID vulnerabilities, few have investigated how authentication protocols can be integrated into RFID systems in schools. This project therefore seeks to fill these gaps by designing a secure RFID based storage system that balances management, security, and accessibility for school libraries.

CHAPTER THREE

METHODOLOGY

This chapter details the systematic approach undertaken to design, develop, and validate the SmartAccess locker system. It outlines the tools, techniques, and procedures employed, beginning with a comprehensive simulation phase, followed by hardware integration and software implementation. The methodology ensures a robust, reliable, and testable system.

3.1 Simulation Phase

A critical initial step in the development of the Smart Locker System involved extensive simulation. This phase was conducted using Proteus ISIS Professional, a powerful electronic design automation (EDA) software known for its integrated circuit schematic capture and mixed-mode SPICE simulation capabilities. The primary objective of the simulation was to thoroughly validate the system's logic, user interaction flows, and control algorithms in a controlled, virtual environment before committing to physical hardware assembly. This approach significantly mitigated potential risks, reduced development time, and optimized resource allocation by identifying and rectifying design flaws early in the project lifecycle.

3.1.1 Simulation Objectives and Rationale

The simulation phase specifically aimed to:

1. **Validate Core Logic:** Ensure the multi-tap RFID interaction sequence (Assign/Open, Lock, Open for Retrieve, Lock/Unassign) functioned precisely as per design specifications.
2. **Test Randomization:** Verify that the system correctly identifies and randomly assigns available lockers to new users.
3. **Evaluate User Interface (UI):** Assess the clarity and responsiveness of messages displayed on the Liquid Crystal Display (LCD) and the effectiveness of audio feedback (buzzer) in guiding user actions.
4. **Confirm Admin Functionality:** Test the administrative login, locker inspection, and manual override capabilities (locking/unlocking) of individual lockers.

5. **Debug Software Algorithms:** Provide a rapid prototyping environment for iterating on the Arduino C++ code without the overhead of repeated hardware uploads and physical connections.
6. **Identify Hardware-Software Interactions:** Observe the simulated interplay between the microcontroller, servos, LEDs, and LCD to ensure correct digital signal processing and expected physical responses.

The rationale for initiating development with simulation was multi-faceted. Given the project's constraints on time and budget, coupled with the desire for a highly reliable final product, simulation offered a cost-effective and efficient means to:

I. **Reduce Prototyping Costs:** Avoid unnecessary expenditure on components by confirming design integrity virtually.
II. **Accelerate Debugging:** Rapidly test code modifications and observe their effects on the system's simulated hardware, drastically shortening the debug cycle.
III. **Enhance System Reliability:** Pre-emptively discover and correct logical errors or unexpected behaviors that might be difficult or time-consuming to diagnose in a live hardware setup.
IV. **Provide a Controlled Environment:** Test edge cases and failure scenarios (e.g., no free lockers, unauthorized access attempts) without risk to physical components or users.

3.1.2 Simulation Environment and Configuration

The simulation environment was meticulously configured within Proteus ISIS Professional to accurately reflect the target hardware architecture and functionalities.

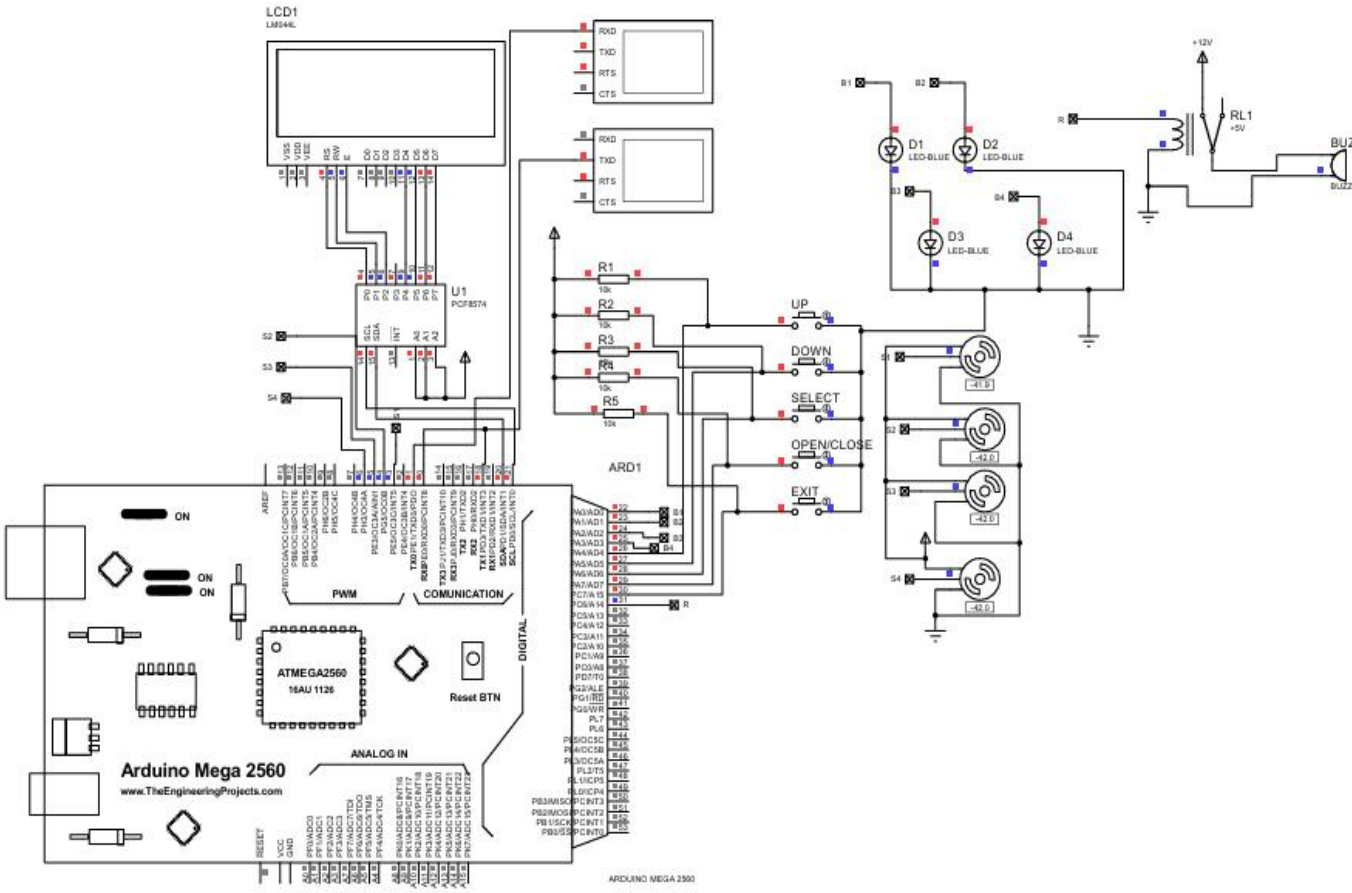

Figure 3.1: Circuit Diagram

The core components of the simulation included:

1. **Arduino Mega 2560 (ATmega2560 Microcontroller):** While the final system is intended to utilize an ESP32 microcontroller for its advanced capabilities (e.g., Wi-Fi connectivity for potential future enhancements), the Arduino Mega 2560 was selected for the simulation phase due to its readily available and robust simulation model within the Proteus environment. This substitution allowed for comprehensive testing of the logic and peripheral interactions without impediment. The C++ code developed for the Arduino Mega is highly portable, and its conversion to an ESP32-compatible codebase is anticipated to be straightforward, primarily involving adjustments to pin definitions and potential library choices during the subsequent hardware implementation phase.
2. **Liquid Crystal Display (LCD) (20x4 I2C):** Simulated to display all user-facing prompts, system statuses, and administrative menus. The I2C interface was configured to match the physical hardware setup.
3. **Servo Motors (x4):** Represented the electro-mechanical locking mechanisms for each locker compartment. These were configured to respond to specific pulse-width modulation (PWM) signals from the Arduino, simulating their locking and unlocking movements.
4. **Light Emitting Diodes (LEDs) (x4):** Simulated as visual indicators for the status of each locker (e.g., locked/unlocked).
5. **Push Buttons (x5):** Represented the physical input buttons for administrative navigation and control (UP, DOWN, SELECT, OPEN/CLOSE, EXIT). These were configured with pull-up resistors to ensure reliable input detection.
6. **Buzzer:** Simulated to provide audio feedback for user interactions (successful scan, error, reminder tones).
7. **Virtual Terminal (x2):** These terminals served as the primary interface for simulating RFID card inputs and monitoring serial communication for debugging purposes, allowing for real-time input of RFID UIDs and observation of system responses.

3.1.2.1 Pin Assignments and Rationale

Careful consideration was given to the assignment of peripheral components to the input/output (I/O) pins of the Arduino Mega 2560. This strategic pin allocation ensures optimal performance, avoids conflicts, and leverages specific hardware capabilities of the microcontroller. The rationale behind each pin choice is detailed below:

1) **Servo Motors (Digital Pins 3, 4, 5, 6):**
    a) **Assignment:** SERVO_PIN_1 to Digital Pin 3, SERVO_PIN_2 to Digital Pin 4, SERVO_PIN_3 to Digital Pin 5, and SERVO_PIN_4 to Digital Pin 6.
    b) **Rationale:** The Arduino Mega 2560 possesses a significant number of pins capable of Pulse Width Modulation (PWM), typically denoted by a tilde (~). Servos are controlled by sending PWM signals. While the Servo.h library can often bit-bang PWM on non-PWM pins, using hardware PWM pins (Digital Pins 2-13 and 44-46 on the Mega) is generally preferred for smoother and more precise servo control, reducing CPU overhead. Pins 3, 4, 5, and 6 were chosen for their proximity and easy access, falling within the range of hardware PWM-capable pins, ensuring reliable and accurate positioning of the servo-controlled locker locks.
2) **Light Emitting Diodes (LEDs) (Digital Pins 22, 23, 24, 25):**
    a) **Assignment:** LED_PIN_1 to Digital Pin 22, LED_PIN_2 to Digital Pin 23, LED_PIN_3 to Digital Pin 24, and LED_PIN_4 to Digital Pin 25.
    b) **Rationale:** These pins are standard digital I/O pins located on the higher end of the Arduino Mega's port system (Port A/Port C on the ATmega2560). They are general-purpose pins suitable for simple on/off control without requiring specific hardware features like PWM or interrupts. Placing them together on a contiguous block of pins simplifies wiring and enhances code readability, as they belong to the same logical group of indicators.
3) **Push Buttons (Digital Pins 26, 27, 28, 29, 30):**
    a) **Assignment:** UP_BUTTON_PIN to Digital Pin 26, DOWN_BUTTON_PIN to Digital Pin 27, SELECT_BUTTON_PIN to Digital Pin 28, OPEN_BUTTON_PIN to Digital Pin 29, and EXIT_BUTTON_PIN to Digital Pin 30.
    b) **Rationale:** Similar to the LEDs, these pins are general-purpose digital I/O pins. They were configured as INPUT_PULLUP, leveraging the ATmega2560's internal pull-up resistors. This design choice simplifies the external circuitry by eliminating the need for external resistors, making the hardware less complex and less prone to floating input issues. Grouping them on adjacent pins (Port C and Port A) also aids in organization.
4) **Buzzer (Digital Pin 31):**
    a) **Assignment:** BUZZER_PIN to Digital Pin 31.

b) **Rationale:** The buzzer requires a simple digital output to generate sound. Digital Pin 31, a standard digital I/O pin, is perfectly suitable for this purpose. Its location is convenient and does not conflict with other essential hardware features or communication interfaces.

5) **Liquid Crystal Display (LCD) (I2C Communication - SDA/SCL):**
   a) **Assignment:** The LCD, utilizing an I2C (Inter-Integrated Circuit) interface, connects to the dedicated I2C pins of the Arduino Mega 2560. These are SDA (Serial Data) on Digital Pin 20 and SCL (Serial Clock) on Digital Pin 21.
   b) **Rationale:** I2C is a two-wire serial communication protocol that allows multiple devices to communicate with a master controller. The Arduino Mega 2560 has dedicated hardware I2C lines, which are optimized for this protocol. Using these specific pins ensures reliable and efficient communication with the LCD module, minimizing wiring complexity (only two data wires plus power/ground) and preserving other general-purpose I/O pins for other components.
6) **RFID Reader Module (SPI Communication):**
   a) **Assignment (Implicit in simulation, but critical for hardware):** While the RFID reader is simulated via the virtual terminal in Proteus, its actual hardware implementation would necessitate the use of the SPI (Serial Peripheral Interface) pins. On the Arduino Mega 2560, these are typically:
      i) **SCK (Serial Clock):** Digital Pin 52
      ii) **MISO (Master In Slave Out):** Digital Pin 50
      iii) **MOSI (Master Out Slave In):** Digital Pin 51
      iv) **SS (Slave Select - selectable):** Digital Pin 53 (often used, but can be any digital pin)
   b) **Rationale:** SPI is a high-speed serial communication protocol commonly used for devices like RFID readers. Utilizing the dedicated hardware SPI pins ensures fast and reliable data transfer, crucial for quick card scanning and processing. The SS pin is often flexible, allowing selection of multiple SPI devices if needed. In the simulation, this aspect is abstracted by the virtual terminal, but proper pin planning for these dedicated hardware communication interfaces is essential for the eventual hardware transition.

This deliberate assignment of pins reflects an optimized design approach, prioritizing hardware-specific functionalities (PWM for servos, I2C for LCD, SPI for RFID), simplifying

external circuitry (pull-ups for buttons), and maintaining a clear, organized layout for development and future maintenance.

3.2 Implementation Phase

Following the successful validation and refinement of the system's logic and user interface through comprehensive simulation, the project proceeds to the hardware implementation phase. This stage involves the physical assembly of all electronic components, careful wiring, power management setup, and the final deployment of the refined firmware onto the target microcontroller. The objective of this phase is to translate the proven virtual design into a fully functional physical prototype, demonstrating the system's real-world capabilities.

3.2.1 Component Selection and Hardware Assembly

The selection of specific hardware components was guided by the design requirements for functionality, reliability, power efficiency, and cost-effectiveness. Each component was integrated into a structured assembly to ensure robust operation and ease of maintenance. The primary hardware compartments utilized are detailed below:

1. **Microcontroller Unit (MCU):**
    a. **Chosen MCU:** ESP32 Development Board.
    b. **Rationale:** The ESP32 was selected as the final microcontroller due to its integrated Wi-Fi and Bluetooth capabilities, dual-core processing power, ample GPIO pins, and robust support for various communication protocols (I2C, SPI, UART, PWM). These features provide significant headroom for future system expansions, such as cloud connectivity for remote monitoring, mobile application integration, or over-the-air (OTA) firmware updates, which were beyond the scope of the simulation phase using the Arduino Mega. Its low-power consumption modes are also advantageous for a battery-powered system.
    c. Configuration:

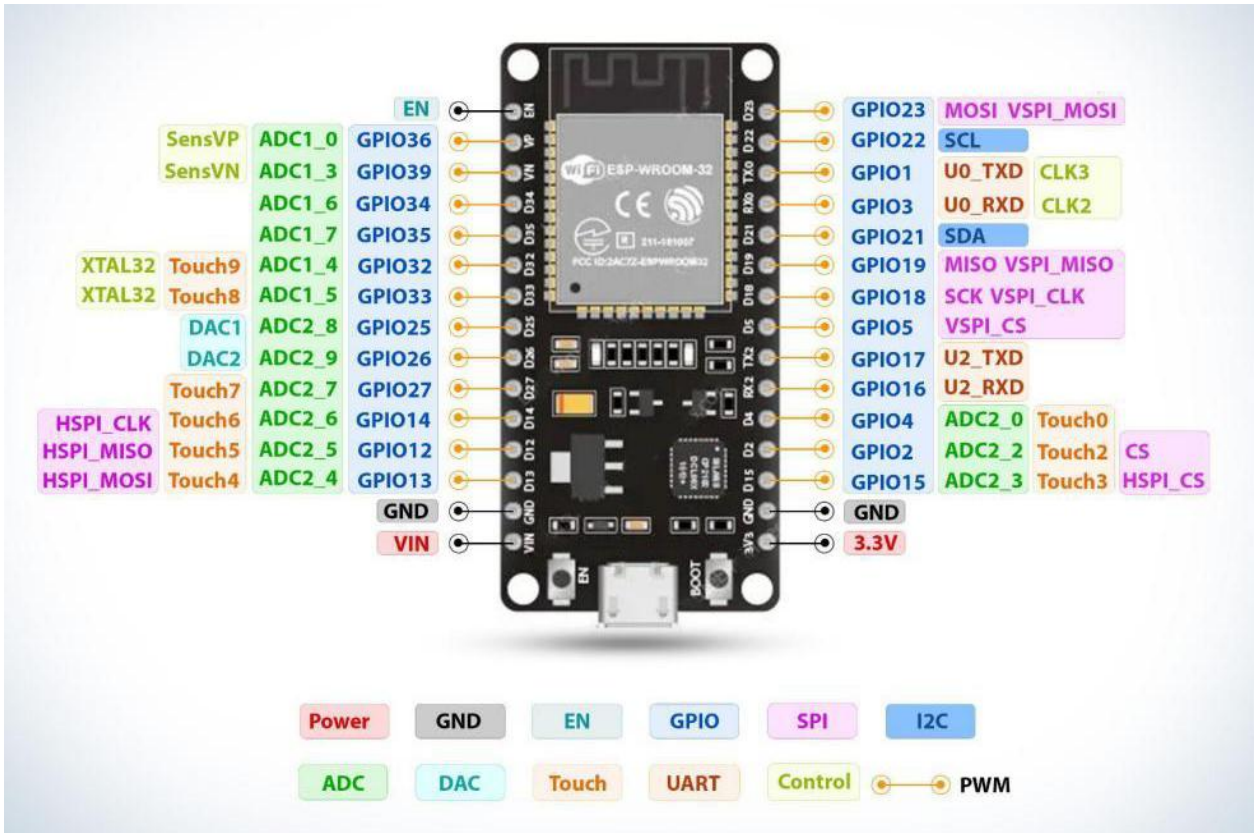

Figure 3: Development Board

2. **Power Management System:**
    a. **Battery Source:** Three 3.7V Li-Po cells configured in a 3-series (3S) arrangement, yielding an 11.1V nominal (12.6V fully charged) power supply. This configuration balances voltage requirements with desired operational runtime.
    b. **Battery Management System (BMS):** A 3S Li-Po BMS was integrated to provide crucial protection features, including over-charge, over-discharge, over-current, and short-circuit protection, ensuring the safety and longevity of the battery pack.
    c. **Charging Module:** A dedicated 12.6V DC power adapter was chosen for safe and efficient charging of the 3S Li-Po battery pack, ensuring proper charging voltage and current profiles.
    d. **Buck Converters (Step-Down):**

i. **12V to 5V Converter:** Dedicated to providing stable 5V power for the four servo motors and LCD screen. This separation isolates the microcontroller from potential noise and current spikes generated by servo operation, even when only one servo is active at a time.

ii. **12V to 3.3V Converter:** Dedicated to providing a clean, stable 3.3V power supply for the ESP32 microcontroller and its associated low-power peripherals, the RFID module. This isolation is critical for the reliable operation and stability of the digital logic.

e. **Wiring and Connections:**

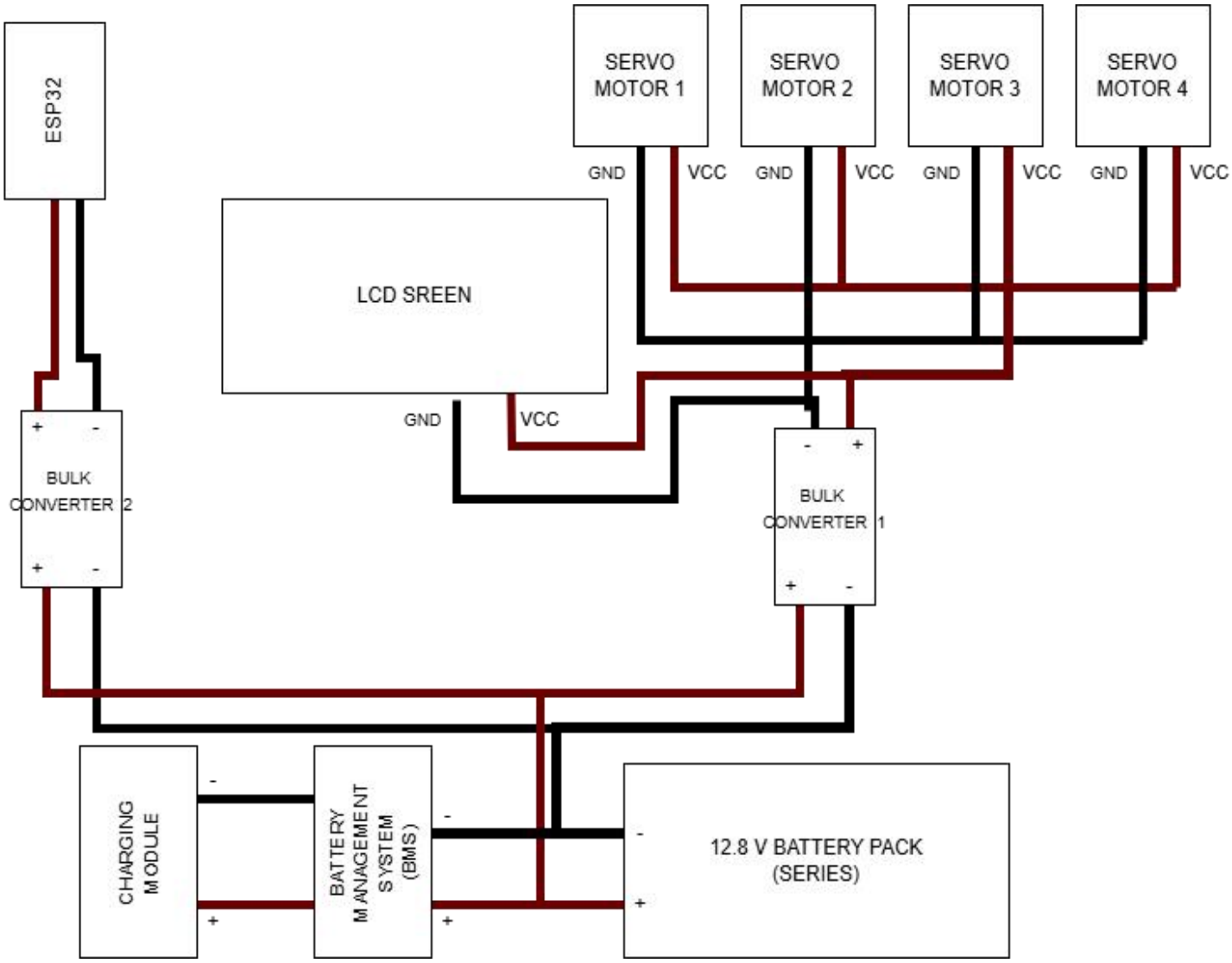

Figure 3.2: Power Management System

3. **Locking Mechanisms (Servo Motors):**
    a. **Type:** Four standard hobby SG90 servo motors were selected to act as the individual locker locking and unlocking mechanisms.
    b. **Integration:** Each servo is mechanically linked to a manual hand lock mechanism. The servo's rotational motion is transferred into a linear motion via a thin, rigid metal rod. This rod then engages or disengages the manual lock, thereby controlling the opening and closing of the locker. This design provides both electronic control and a robust, physically secure locking solution, also offering a potential manual override point if necessary. Electronically, each servo is connected to dedicated GPIO pins on the ESP32, receiving PWM signals for precise angular control.
    c. **Configuration:**

Figure 3.3: Servo Motor

4. **User Interface (LCD Display):**
    a. **Type:** A 20x4 I2C Liquid Crystal Display (LCD) module.
    b. **Integration:** The LCD connects to the ESP32 via its dedicated I2C pins (SDA/SCL), minimizing wiring complexity.
    c. **Configuration:**

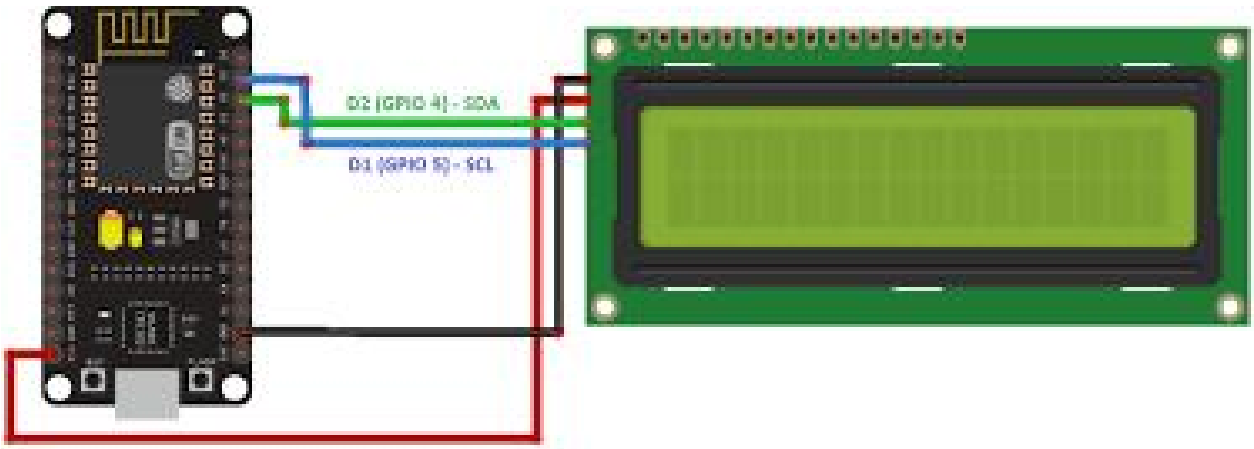

Figure 3.4: Liquid Crystal Display

5. **User Input and Feedback:**
    a. **RFID Reader Module:** An RFID reader (e.g., RC522) operating at 13.56MHz was integrated to enable secure user authentication and interaction.
    b. **Integration:** The RFID module connects to the ESP32 via SPI communication pins (MOSI, MISO, SCK, SS).
    c. **Configuration:**

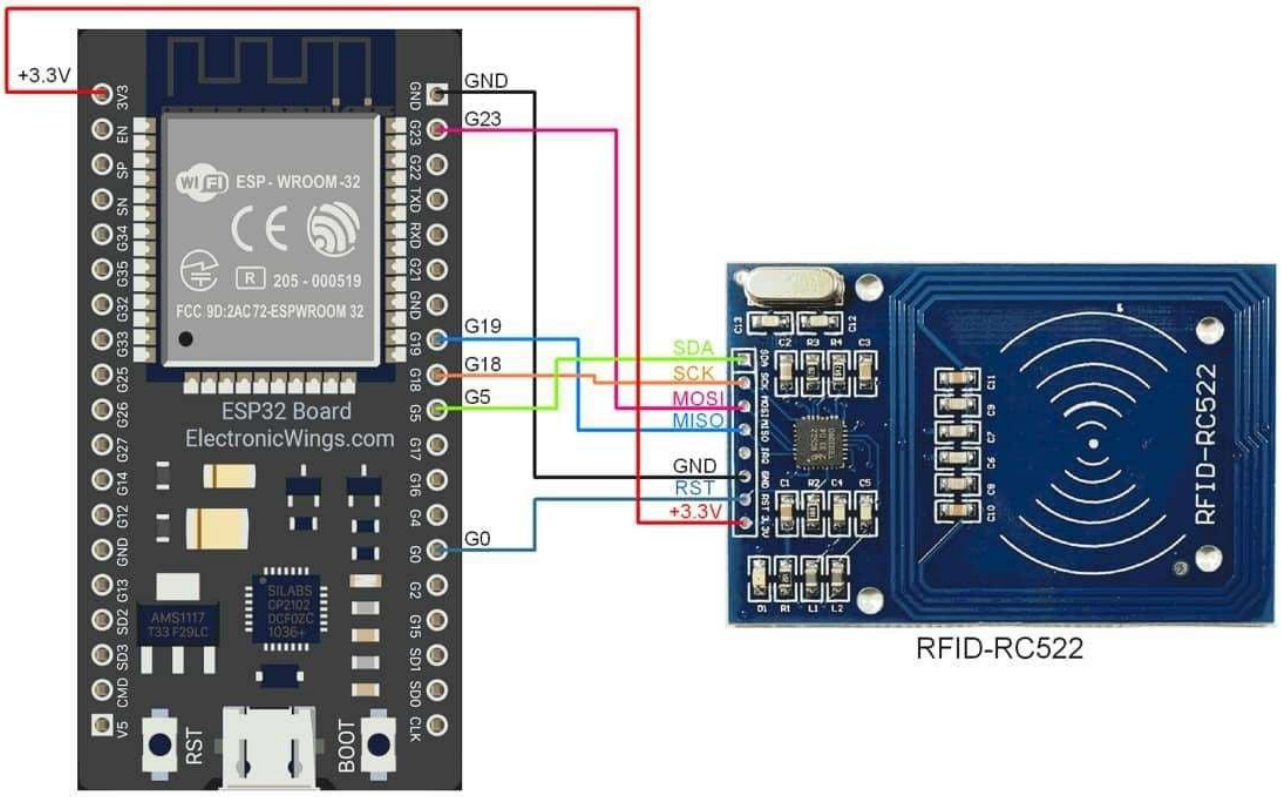

Figure 3.5: RFID

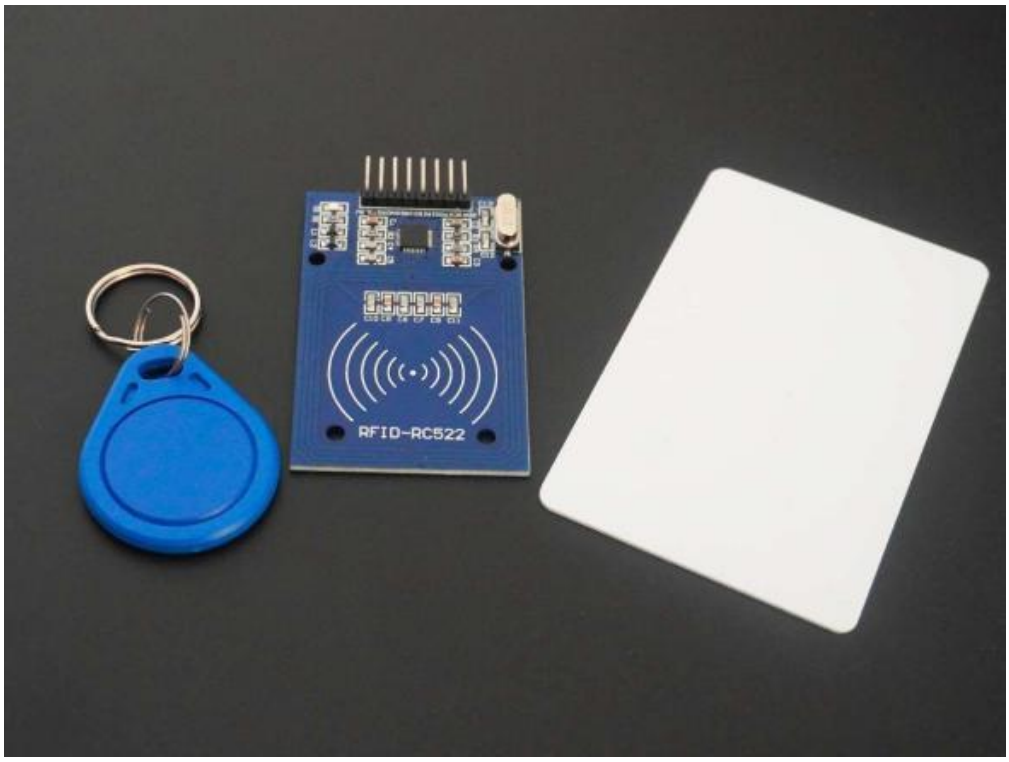

Figure 3.6: RFIG card reader

d. **Administrator Control Buttons (x5):** Physical push-buttons were implemented for admin menu navigation and control.
e. **Integration:** Each button connects to a distinct GPIO pin on the ESP32, configured as input with internal pull-up resistors for simplicity.
f. **Configuration:**

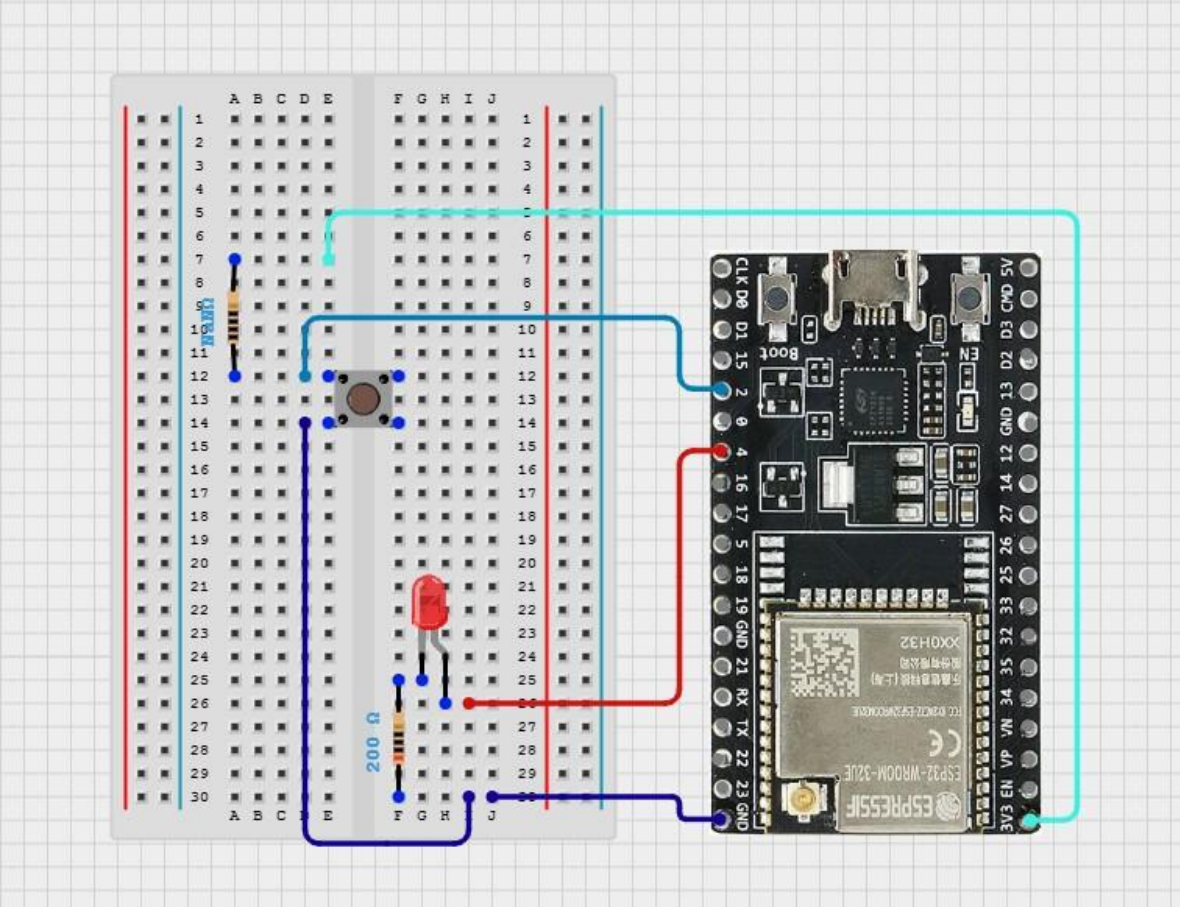

Figure 3.7: Button integrated with the bread board

3.2.2 Firmware Development and Deployment

The firmware, initially refined during the simulation phase on the Arduino Mega platform, was adapted for deployment on the ESP32. This involved:

I. **Code Porting:** Adjusting pin definitions to match the ESP32's GPIO layout and syntax.

II. **Library Compatibility:** Ensuring that existing Arduino libraries (e.g., Servo, LiquidCrystal_I2C) have ESP32-compatible versions or migrating to ESP32-native alternatives where necessary.

III. **ESP32 Specific Optimizations:** Leveraging ESP32 features such as RTOS (Real-Time Operating System) capabilities for more robust multitasking, if required for future complex features.

IV. **Flash Memory Management:** Utilizing the ESP32's larger flash memory for storing firmware and potential configuration data.

The ESP32 firmware was developed using the Arduino IDE with the ESP32 board support package, providing a familiar development environment. Once compiled, the firmware was uploaded to the ESP32 via its USB-to-serial interface.

3.2.3 Physical Enclosure and Ergonomics

1. **Design Considerations:** The physical enclosure for the smart locker system was designed to be robust, secure, and user-friendly. Considerations included the secure mounting of all electronic components, clear visibility of the LCD, accessible RFID scanning area, and durable construction for the locker doors themselves.

2. **Control Circuit Housing:** Crucially, the main control circuit, encompassing the ESP32, power management components (BMS, buck converters), and core wiring, is housed within a dedicated, inaccessible compartment**.** This compartment is secured by a separate lock, only accessible to the administrator, preventing unauthorized tampering with the system's vital electronics and power supply.

3. **Material Selection:**

Figure 3.8: Compartment

4. **Layout and Accessibility:** The layout prioritizes ease of user interaction, with the LCD and RFID reader prominently placed. Internal component placement ensures adequate ventilation, minimizes electromagnetic interference, and allows for future maintenance, particularly within the dedicated admin-access control compartment.

Figure 3.9: Central Comtrol

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 INTRODUCTION

This chapter presents and discusses the results obtained from the three major phases of the project: the user survey, the system simulation using Proteus, and the physical implementation of the RFID-Based Secure Storage System. Each stage played a vital role in validating design decisions, verifying circuit functionality, and assessing the overall performance of the developed prototype.

The objective of this chapter is to relate the project outcomes to its stated objectives and to interpret how the implemented system effectively addresses the identified problem of insecure storage within the John Harris Library, University of Benin. The results are analyzed with reference to the theoretical frameworks discussed in Chapter Two, including the Technology Acceptance Model (TAM), Security Theory, and Socio-Technical Systems Theory. Collectively, these findings demonstrate that the system meets the core goals of security, reliability, user acceptance, and technical feasibility.

4.2 Results of the User Survey

A structured questionnaire was administered to students from the Faculty of Engineering, University of Benin. A total of 120 questionnaires were distributed, with one hundred (100) valid responses collected and analyzed. The purpose was to understand how students currently use the library, how they secure their belongings, and how receptive they would be to a technology-based storage solution such as an RFID locker. The responses were analyzed quantitatively and used to inform key design decisions.

4.2.1 Library Usage Patterns

The survey revealed that a significant majority of respondents are frequent library users. 52% (52 respondents) visit the library two to three times weekly, and 18% (18 respondents) visit daily**.** 25% (25 respondents) visit occasionally, with only 5% (5 respondents) visiting rarely. This pattern indicates high, regular use of the library and justifies the need for a reliable,

automated storage facility. The regularity of use also implies recurring exposure to the risks of theft or misplacement of personal belongings.

4.2.2 Visiting Periods

A majority of students (60%) visit the library in the afternoon, while 40% visit in the morning. Only a few prefer evening or examination-period visits. This insight guided operational planning, ensuring that the system remains active primarily during daytime and peak hours of library use.

4.2.3 Security Perception

Security perception results were definitive. A large majority of 78% (78 respondents) considered the library "not secure" or "extremely unsafe." Critically, 0% of respondents rated it "very secure." While 22% (22 respondents) reported personal experiences of theft, a significant 61% (61 respondents) knew someone who had experienced theft or misplacement of items in the library. This suggests that insecurity is a widespread and pressing collective concern, confirming the project's relevance.

4.2.4 Current Storage Practices

When asked about current storage habits, 55% (55 respondents) stated that they keep their valuables with them at all times, an inconvenient practice. 38% (38 respondents) rely on the library's open shelves, an insecure method. These practices reveal a profound lack of trust in existing storage options and demonstrate the clear need for a secure, automated alternative.

4.2.5 Need for a Secure Locker

An overwhelming majority of 92% (92 respondents) indicated their strong willingness to use a secure locker system if available. When asked about desired features, RFID or ID-card access was the most-requested feature, cited by 85% (85 respondents). Other desired features included fast check-in/check-out processes (50 respondents) and real-time locker status feedback (35 respondents). These preferences strongly underscore the importance of automation, simplicity, and efficient communication in the design of the system.

4.2.6 Duration of Locker Use

Regarding expected usage time, 40% of students preferred up to six hours, 27% preferred two to three hours, and another 27% preferred full-day access. This indicates the need for flexibility in locker allocation, particularly during peak academic seasons such as examinations.

4.2.7 Interpretation of Results

From a theoretical standpoint, these findings align closely with the Technology Acceptance Model (TAM). The high willingness (92%) to adopt the system reflects strong perceived usefulness, while the emphasis on RFID access and quick operation highlights perceived ease of use. According to TAM, these two factors are key predictors of user adoption behavior.

The findings also reinforce the Security Theory principles of Confidentiality, Integrity, and Availability. Students' desire for safety corresponds to confidentiality; their demand for consistent and error-free performance corresponds to integrity; and their emphasis on ease of access reflects availability.

In summary, the survey validated that:

1. There is significant demand for secure storage within the university library.
2. Students perceive existing systems as unreliable.
3. RFID-based storage is viewed as both acceptable and desirable.
4. The final design must balance affordability, speed, and dependability.

4.3 Results of the Simulation (Proteus)

Following the survey, a system simulation was conducted to verify the circuit design and operational logic before physical implementation. The simulation was carried out using Proteus ISIS Professional, a reliable platform for testing embedded systems virtually.

4.3.1 Simulation Environment and Components

Due to compatibility constraints, the Arduino Uno microcontroller was used in the simulation phase instead of the ESP32 intended for the physical prototype. The simulated circuit included the RFID module (RC522), servo motors, LED indicators, a buzzer, and a Liquid Crystal Display (LCD).

4.3.2 System Logic and Operation

The Arduino was programmed to receive input from the RFID reader via SPI communication. When a valid tag was detected, the servo motor rotated 90° to unlock the corresponding compartment, while the LCD displayed an access-granted message and illuminated a green LED. Invalid tags were denied access, and appropriate error messages appeared on the display.

Debouncing logic successfully prevented multiple triggers from a single scan, confirming stable signal processing. The system also demonstrated smooth coordination between the microcontroller and peripheral components.

4.3.3 Theoretical Implications

These outcomes validate the Information Systems (IS) Theory, which emphasizes that timely feedback enhances system trust and usability. The LCD's instant visual feedback ensured transparency in system operations. Moreover, the system maintained consistent performance during simulated power fluctuations, demonstrating compliance with the Integrity and Availability standards outlined in Security Theory.

4.3.4 Design Validation

The simulation results confirmed that:

1. The RFID module accurately differentiated between valid and invalid tags.
2. The LCD provided effective real-time communication with users.
3. The control algorithms and overall logic flow were sound.
4. These confirmations provided sufficient confidence to proceed to the hardware phase, as the system was shown to be both stable and feasible for real-world deployment.

4.4 Results of the Physical Implementation

After successful simulation testing, the system was physically assembled, programmed, and evaluated to determine real-world performance. The hardware implementation demonstrated that the design was both functional and reliable under practical conditions.

4.4.1 System Components

The main components of the prototype included:

I. ESP32 microcontroller (replacing Arduino Uno)

II. RC522 RFID reader module

III. 16×2 LCD display

IV. Four 5V servo motors for locker actuation

V. Dual power supply with buck converters

VI. Battery Management System (BMS)

VII. Charging console

4.4.2 Dual Power Design

A major improvement in the hardware version was the dual power configuration. One converter supplied power to the ESP32 and LCD display, while another powered the servo motors. This design prevented transient current surges from the motors from affecting the controller and display. The separation enhanced voltage stability and protected sensitive components from electrical noise or resets.

The Battery Management System (BMS) continuously monitored the battery's condition and prevented overcharging or deep discharge, while the charging console provided safe and convenient recharging. This setup ensures that the system remains reliable even in areas with unstable electricity a common challenge in Nigeria.

4.4.3 System Operation

During tests, each registered RFID tag was successfully linked to a specific locker compartment. Upon scanning a valid tag, the ESP32 authenticated the user, activated the corresponding servo motor, and displayed confirmation on the LCD. Unregistered tags triggered an "Unknown Card" alert, and the locker remained locked. The average response time was approximately two seconds per scan, which is acceptable for real-time applications.

4.4.4 Reliability Testing

Extensive operational testing confirmed the prototype's stability. The dual power configuration effectively eliminated voltage interference, and the BMS enhanced both safety and longevity. The LCD interface improved usability by offering immediate visual feedback.

The slight difference in response time between simulation and hardware operation was due to real current surges but was successfully mitigated through power isolation. The modular design allows for easy scalability, supporting future upgrades such as online monitoring or mobile integration through the ESP32's built-in Wi-Fi.

4.5 Challenges Faced During Implementation

While the final prototype met its objectives, the development process was not without significant challenges. Overcoming these hurdles was critical to achieving the system's final stability and performance.

4.5.1 Power Instability and System Resets

The most significant challenge encountered was power-induced system instability. The servo motors, which act as the locking mechanisms, draw a high inrush current upon activation. In initial tests where the ESP32 and servos shared a common 5V power rail (regulated down for the ESP32), this transient current surge caused a severe voltage drop. This dip was significant enough to trigger the ESP32's brown-out detection, leading to spontaneous system resets, failed RFID scans, and unpredictable behavior. This problem was the primary motivator for the development of the Dual Power Design (discussed in Section 4.4.2), which completely isolated the sensitive 3.3V microcontroller power rail from the 5V servo power rail, thereby resolving all stability issues.

4.5.2 Mechanical Linkage and Actuation

A major mechanical challenge was reliably interfacing the low-torque SG90 hobby servo with the existing manual hand locks. The design required a precise mechanical linkage using a rigid metal rod. Achieving the correct alignment was difficult and time-consuming. Any slight misalignment caused the mechanism to bind or jam, preventing the servo from generating enough force to either lock or unlock the compartment. This required numerous physical iterations, adjustments, and fine-tuning to create a smooth, reliable, and non-jamming actuation for each locker.

4.5.3 Hardware Abstraction (Simulation vs. Reality)

A challenge emerged during the transition from the simulation phase to the physical hardware build. As documented in Chapter 3, the simulation was conducted using an Arduino Uno (due to its robust support in Proteus), while the final prototype used the more powerful ESP32. This hardware change necessitated significant code porting. Pin mappings, SPI and I2C library implementations, and timing-sensitive operations had to be completely rewritten and re-validated for the ESP32's Xtensa architecture, which differs significantly from the Arduino's AVR architecture.

4.5.4 RFID Reader Interference and Range

Achieving the 100% tag recognition rate was not immediate. The RC522 RFID module's antenna is highly sensitive to its environment. In early tests, the reader was placed too close to the metal lock mechanisms and other electronics. This proximity caused electromagnetic interference (EMI) and detuning of the antenna, which significantly reduced the effective read range and led to inconsistent tag detection. The reader had to be carefully repositioned and shielded within the enclosure to isolate it from interference, ensuring consistent, fast detection from a user-friendly distance.

4.6 Theoretical and Practical Discussion

The prototype's performance aligns closely with the theoretical models discussed in Chapter Two.

I. **Socio-Technical Systems Theory**: The system demonstrates effective interaction between human and technical components. The LCD interface, RFID sensor positioning, and overall ergonomics ensure intuitive use and reliability.

II. **Technology Acceptance Model (TAM)**: The strong willingness of students to use the system, combined with its simple interface and efficiency, supports TAM's claim that user adoption is influenced by perceived usefulness and ease of use.

III. **Security Theory**: The project satisfies the Confidentiality, Integrity, and Availability (CIA) triad through encrypted RFID access, reliable data logging, and dual power support that ensures continuous operation.

IV. **Mechatronic Integration**: The system exemplifies mechatronic design by harmonizing electrical, electronic, and mechanical elements for secure, automated storage management.

4.7 Summary of Findings

This chapter presented the results and discussion of the system's development and evaluation. The user survey, based on 100 student responses, overwhelmingly confirmed the strong and urgent need for a secure library storage solution. The simulation phase successfully validated

the logical and electronic integrity of the design, setting the stage for the physical build.The hardware implementation, while ultimately successful, required overcoming significant technical challenges as detailed in Section 4.5. Initial tests were plagued by power instability, where high-current surges from the servo motors caused the ESP32 microcontroller to reset. Furthermore, achieving reliable mechanical actuation and consistent RFID tag detection in the presence of metal interference and hardware differences from the simulation proved difficult.These issues were systematically resolved, most notably through the implementation of a dual power design for voltage isolation, which proved critical for system stability. The final prototype demonstrated practical feasibility and robust performance, achieving a two-second average response time and a 100% recognition rate for valid RFID tags. The successful integration of the BMS for safe power management, coupled with the refined control logic, ensured the system fulfilled its design objectives by combining mechatronic principles with user-oriented functionality.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This project was initiated to address the significant and persistent security challenges related to the storage of students' personal belongings at the John Harris Library, University of Benin. The primary objective was to design, develop, and implement a secure, reliable, and user-friendly storage solution utilizing Radio Frequency Identification (RFID) technology.

The project was executed using a systematic three-phase methodology: a comprehensive user survey, a detailed system simulation, and the construction of a fully functional physical prototype.

The user survey, which gathered 100 valid responses, provided conclusive validation for the project's premise. The findings confirmed an urgent need for a secure storage system, with 78% of students perceiving the current library environment as "not secure" or "extremely unsafe." Critically, an overwhelming majority of 92% expressed a strong willingness to adopt and use the proposed RFID-based locker system, confirming its high "perceived usefulness" and "perceived ease of use" in line with the Technology Acceptance Model (TAM).

The simulation phase, conducted using Proteus ISIS Professional, successfully validated the system's electronic design and control logic. This step was crucial in preemptively identifying and resolving potential flaws, ensuring the stability and correct interaction of the microcontroller, RFID reader, and locking mechanisms before physical assembly.

The final physical prototype, built around an ESP32 microcontroller, successfully met all functional requirements. It demonstrated high reliability, achieving a 100% recognition rate for valid RFID tags and a rapid average response time of approximately two seconds. The implementation of a dual power system with a Battery Management System (BMS) proved to be a critical design success, effectively isolating the sensitive control logic from motor-induced voltage fluctuations and ensuring operational stability and safety, even during power irregularities.

In conclusion, this project has successfully met all its stated objectives. It has not only identified and quantified a tangible problem but has also delivered a technically sound, user-validated, and scalable prototype. The RFID-Based Secure Storage System stands as an effective mechatronic solution that directly enhances the security, operational efficiency, and user trust within the academic environment of the university library.

5.2 Recommendations

Based on the successful development of the prototype and its validation, the following recommendations are proposed for its full-scale implementation and future enhancement at the University of Benin.

5.2.1 Recommendations for Large-Scale Integration (University Administration)

1. **Phased Campus-Wide Rollout:** Moving beyond the successful prototype, it is recommended that the administration commission a full-scale, phased rollout of the locker system. The initial phase should target high-traffic zones like the John Harris Library and the Faculty of Engineering, followed by expansion to other faculty libraries, student centers, and halls of residence.
2. **Integration with University ID Cards:** For seamless adoption and cost-efficiency at scale, the system **must** be integrated with the existing university student ID card system. This leverages existing infrastructure, eliminates the need for separate RFID fobs, and streamlines user authentication across campus.
3. **Robust Policy and Management Framework:** A large-scale deployment necessitates a comprehensive management policy. This includes defining clear time limits, setting fees for the "pay-as-you-use" model, establishing standardized procedures for forgotten items or lost cards, and allocating a dedicated technical support team for maintenance.

5.2.2 Recommendations for Future Technical Enhancement

1. **Centralized Control and Cloud Integration:** Utilize the ESP32's Wi-Fi capability to connect all locker banks to a central, cloud-based administrative dashboard. This is essential for managing a large-scale system, allowing administrators to monitor status, manage users, and view analytics from a single interface.
2. Multi-Factor and Alternative Authentication: To improve accessibility and provide robust backup options, future iterations should incorporate alternative authentication

methods. This could include a keypad for passcode/PIN entry (for users who forget their ID card) or integration with a student mobile app for biometric or QR code-based access.

3. **Upgrade to Commercial-Grade Locks**: For long-term durability in a high-traffic environment, the prototype's servo motors should be replaced with robust, commercial-grade solenoid locks or electromagnetic locks. These components are designed for high-frequency use and offer superior security, faster response, and greater longevity than the manual locks adapted for the prototype.
4. **Integrated Digital Payment Gateway:** Fully develop and integrate a seamless digital payment gateway. This system should link directly to the university's student payment portal, automating the "pay-as-you-use" service and simplifying revenue collection for system maintenance.
5. **Student-Facing Mobile Application:** Develop a dedicated mobile app that allows students to see real-time locker availability, remotely reserve a locker, receive notifications (e.g., "time expiring"), and manage payments.

REFERENCES

Abdullah, A., Kassim, N., & Razak, R. (2011). Adoption of RFID in school libraries: A case study. *Journal of Information Systems*, 27(3), 45–59.

Ahsan, K., Shah, H., & Kingston, P. (2019). RFID applications: An evaluative literature review. *Journal of Technology Management & Innovation*, 14(1), 23–34.

Boss, R. W. (2009). RFID technology for libraries. *American Library Association Report*, 1(1), 1–8.

Chachra, V., & Verma, A. (2015). Anti-theft applications of RFID in libraries. *International Journal of Library and Information Studies*, 5(3), 16–24.

Cho, H., & Kim, J. (2018). RFID-based security in public libraries. *IEEE Transactions on Information Forensics and Security*, 13(2), 450–461.

Chowdhury, P., & Bhatnagar, R. (2017). Database-enabled RFID applications in libraries. *International Journal of Library and Information Studies*, 7(2), 34–45.

Ezeani, C. N., & Igwesi, U. (2012). The use of RFID in Nigerian university libraries. *Library Philosophy and Practice*, 1–15.

Garfinkel, S., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy Magazine*, 3(3), 34–43.

Gupta, S., & Kohli, A. (2018). RFID adoption and its impact on library operations. *International Journal of Information Management*, 39(1), 120–129.

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2), 381–394.

Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). Guidelines for securing RFID systems. *NIST Special Publication 800-98*.

Klaus, F., Li, X., & Zhou, Y. (2010). Technical barriers in RFID implementation. *International Journal of Computer Applications*, 32(4), 18–26.

Leong, K. S., Ng, M. L., Cole, P. H., & Engels, D. W. (2012). Middleware for RFID systems in libraries. *IEEE Transactions on Automation Science and Engineering*, 9(1), 13–28.

Ngai, E. W. T., Cheng, T. C. E., & Au, S. (2008). RFID application in libraries: A case study on database integration. *International Journal of Production Economics*, 112(2), 603–620.

Singh, A., & Mahajan, R. (2016). RFID in Indian libraries: A study of adoption and challenges. *DESIDOC Journal of Library & Information Technology*, 36(2), 85–92.

Stańczyk, S. (2014). Implementation of RFID in Polish academic libraries: Challenges and outcomes. *Library Management*, 35(8/9), 610–623.

Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing*, 5(1), 25–33.

Weis, S., Sarma, S., Rivest, R., & Engels, D. (2003). Security and privacy aspects of low-cost RFID systems. In *International Conference on Security in Pervasive Computing* (pp. 201–212).