**Integration of Contactless RFID-Based Student and Vehicle Access Control and Attendance Logging System for a Philippine State University**

A Bachelor’s Thesis Presented to the Faculty of IT

and Computer Education Unit

Leyte Normal University

Tacloban City

In Partial Fulfillment of the

Requirements for the Degree

Bachelor of Science in Information Technology

by:

Lingo, Ruby E.

Lopez, Victor Jose Francisco B.

Lotoc, Jef Lawrence H.

Pacala, Amabelle T.

APRIL 2024

Chapter 1

**Introduction**

In today's world, where information can easily travel between different places, it is crucial to have strong security measures in place. These measures aren't just important in one area—they are needed everywhere, no matter where you are in the world. This segment of discussion introduces the context of the research, emphasizing the international perspective and drawing insights from existing literature that stress the significance of embracing technological advancements. Wolff (2021) noted that as technology becomes increasingly complex and interconnected, it reshapes our world in profound and sometimes perplexing ways, prompting urgent questions about its direction and the tools needed to steer its development. From privacy concerns to state competition and the influence of big tech companies, navigating this technological landscape requires a refined understanding of the social, political, and economic dimensions of emerging technologies. In today's rapidly evolving technological environment, the need for innovative solutions in various sectors is becoming increasingly apparent.

This research is exploring the integration of RFID (Radio Frequency Identification) technology to transform its campus dynamics and elevate operational efficiency. While the school currently relies on traditional methods for various campus management tasks, such as attendance tracking and event management, the advent of RFID technology presents a promising opportunity for technological innovation and advancement.

The adoption of RFID technology in campus management aligns with global trends in educational institutions, where RFID is increasingly recognized for its transformative potential in improving productivity, efficiency, accuracy, safety, and convenience (Solanke, 2021). This shift towards RFID-based solutions reflects a growing recognition of the need for modernization and optimization of campus operations to meet the evolving needs of students, faculty, and staff.

Furthermore, international literature underscores the significant role of RFID technology in enhancing efficiency in various contexts such as logistics, supply chain management, Warehouse management and logistics, medical implants, road tolling, building access control, aviation security, luggage tracking at airports, libraries, etc. (Singh & Mahajan, 2014). By using RFID technology, this project aims to enhance campus security measures, and automation of attendance tracking in school events. Since while the potential benefits of RFID technology are evident, several gaps in its implementation in educational institutions need to be addressed. Firstly, RFID technology is not widely deployed in educational institutions, limiting improvements in attendance monitoring and campus security. Secondly, there is a lack of comprehensive RFID-based solutions tailored to the diverse needs of educational settings, including attendance tracking, access control, and student safety measures. Additionally, there's a need to integrate RFID technology with supplementary communication channels like SMS notifications and web-based apps to enhance stakeholder engagement, especially with parents and guardians. Finally, exploration of interdisciplinary collaboration and stakeholder engagement in developing RFID-based solutions for educational institutions is essential for successful implementation.

This chapter digs into the research landscape surrounding the integration of RFID solutions into campus operations, exploring how innovative RFID-based systems have been instrumental in elevating security measures and optimizing operational efficiency in various context globally. Through a comprehensive review of existing literature and best practices, this study aims to provide insights into the potential benefits and challenges of implementing RFID technolog, ultimately contributing to the advancement of campus management practices and the enhancement of the overall educational experience for students, faculty, and staff.

**Purpose and Description**

In this research initiative, researchers fall on a comprehensive exploration of RFID (Radio Frequency Identification) technology integration to optimize and modernize campus operations. With a focus on enhancing efficiency, safety, and parental engagement, this project aims to transform how the school will manage its daily activities and ensures a facilitated learning environment for its students.

One of the key objectives of this initiative is to gracefully administer processes through the automation of attendance tracking. By replacing traditional manual methods with RFID-enabled ID cards, Researchers seeks to accelerate the recording of student and staff attendance, reducing the time and effort required for record-keeping while minimizing errors. This transition promises not only greater accuracy in attendance records but also increased efficiency in administrative tasks, allowing faculty and staff to allocate more time to core educational activities.

The integration of RFID technology extends beyond administrative functions to surround campus security enhancement. Through RFID-enabled access control systems, this project aims to regulate entry to campus facilities more effectively, by that means strengthen campus security measures. By restricting access to authorized individuals and providing real-time monitoring capabilities, RFID technology empowers the school to safeguard its campus environment and protect the well-being of its community members.

Furthermore, this research initiative seeks to hold onto RFID technology for insurance students’ safety from the Integrated Laboratory School (ILS). By equipping students with RFID-enabled ID cards, parents will receive automated messages or notifications every time their children enter or exit the campus site. This real-time communication feature provides parents with peace of mind and enables them to stay informed about their children's whereabouts, enhancing parental involvement and student safety.

In addition to enhancing administrative efficiency, campus security, and parental engagement, the integration of RFID technology into event management systems represents a significant advancement in campus operations. Utilizing RFID technology for attendance tracking for events will optimize event organization, strengthen attendee management, and enhance overall event experiences. This innovative approach promises to simplify operational processes, reduce wait times, and ensure a smooth flow of activities during campus events, ultimately contributing to a more vibrant and engaging campus community.

Hence, the integration of RFID solutions into the university’s operations marks a bold step forward in the institution's commitment to innovation and excellence in education. By embracing advanced technology and review traditional practices, this project is assured to transform its campus dynamics, elevate operational efficiency, and create an enriched learning environment that nurtures the comprehensive development of its students. Through this research initiative, university’s dedication to advancing educational practices and promoting a culture of continuous improvement and innovation within its academic community maintains.

**Objective of the Study**

The objective of this research is to investigate, design, and implement a RFID-based access control and attendance logging system. The objectives are structured to ensure the development of an integrated, efficient, and secure system that addresses the diverse needs and challenges of campus operations. These objectives encompass both the core functionalities of the system and additional enhancements aimed at maximizing its effectiveness system and additional enhancements aimed at maximizing its effectiveness.

1. The primary objective of the study is to design, develop, and integrate RFID-based solutions for campus security, including attendance tracking for events, access control and student safety measures considering user preferences, efficiency, and security.
2. The study seeks to boost campus security measures by implementing RFID-based access control systems and real-time monitoring capabilities. This includes regulating entry to the campus, providing real-time campus entry tracking, and ensuring the safety of the university community.
3. Enhance parental engagement and student safety, particularly for students from the Integrated Laboratory School (ILS). This involves providing automated messages to parents whenever their children enter or exit the campus sites, showing parental involvement, and enhancing student safety.

By achieving these objectives, the study aims to provide a Philippine State University with an advanced RFID-based access control and attendance logging system that not only meets the essential operational requirements but also incorporates important enhancements for a more efficient, secure, and engaging campus environment.

**Scope and Limitations**

In scope, this research comprehensively explores the integration of RFID technology across the University's campus operations, surrounding access control, events’ attendance management, and student safety measures. The project aims to enhance efficiency by automating attendance tracking for school events through RFID-enabled ID cards, in that way reduces administrative burden and allows the academic organizations to focus on core event activities. Additionally, the project seeks to boost campus security measures through the implementation of RFID-based access control systems, regulating entry to campus facilities and providing real-time monitoring capabilities to ensure the safety of the university community. Furthermore, the integration of RFID technology aims to enhance parental engagement and student safety, particularly for students from the Integrated Laboratory School (ILS), by providing automated messages to parents whenever their children enter or exit the campus site.

In terms of limitations, several factors must be considered. Firstly, technological constraints may present challenges to the successful implementation of RFID technology, requiring adequate infrastructure. Financial considerations also play a significant role, as the integration of RFID technology may bring weighty advanced costs and ongoing maintenance fees. Training and adoption challenges may arise due to resistance to change or insufficient training among staff and stakeholders, impacting the effective utilization of RFID solutions. Privacy and data security concerns must be addressed to safeguard sensitive information collected through RFID technology and ensure compliance with relevant regulations. Lastly, integration complexity may present hurdles related to compatibility, transaction, and technical coordination, requiring careful planning and collaboration among departments and stakeholders. Despite these limitations, the proposed RFID integration project holds massive potential to enhance operational efficiency, security, and parental engagement covering the way for a more efficient and technologically advanced campus environment.

Chapter 2

This chapter discusses the literature, along with a review of related systems connected to our topic and the themes we've discovered. This chapter sets the background for the study and will aid in understanding the theoretical underpinnings and justification of conducting the study.

**Review of Related Literature and Systems**

**Related Literature**

Automatic Identification and Data Capture (AIDC) Technology

In our increasingly digital-centric world, accurate and timely data are essential for efficiency and success. According to the article by Woods (2024), Automatic Identification and Data Capture (AIDC) technology plays a vital role in achieving this by automatically identifying objects, collecting data about them, and entering that data directly into computer systems with little or no human intervention. This eliminates the need for manual data entry, which is a slow process prone to errors and can significantly hinder the automation process. AIDC technologies encompass a variety of methods, including radio frequency identification (RFID), barcoding, biometrics, electronic article surveillance (EAS), optical character recognition (OCR), and others (AIDC Technologies, n.d.). The technology utilized in this study is part of the diverse family of AIDC technologies, specifically Radio Frequency Identification (RFID) technology.

In contrast to traditional AIDC methods that require line-of-sight scanning, RFID utilizes radio waves for wireless identification. Tiny microchips, called RFID tags, are attached to objects. According to Manral (2022), these tags, which hold significantly more data compared to a barcode, can be read by scanners from a distance, even though non-metallic materials. This eliminates the need for precise positioning, making data capture faster, more reliable, and opening doors to exciting new possibilities. RFID technology offers several advantages that significantly enhance its utility across various applications (RFID Security and Privacy: A Research Survey, 2006). This makes it a vital component in the digital transformation of industries. Its ability to operate without the need for direct line-of-sight contact, combined with the ability to scan multiple items simultaneously, makes RFID an efficient and versatile solution for inventory management, asset tracking, and security systems.

In their study, Suresh and Chakaravarthi (2022) highlight the revolutionary impact of RFID technology across various industries and applications. In retail, RFID enables automated inventory management, reducing stockouts and improving shelf availability. Retailers can track products throughout the supply chain, optimize inventory levels, and enhance the customer shopping experience. In manufacturing, it improves production processes and supply chain logistics. Manufacturers can track raw materials, monitor work-in-progress, and automate inventory management, leading to increased efficiency and cost savings. Bouhassoune et al. (2022) emphasize that in healthcare, RFID technology is pivotal for ensuring patient safety and operational efficiency. Hospitals and clinics leverage RFID tags to identify patients, track medical equipment, and manage medication inventory. Through the automation of data capture and inventory management processes, RFID facilitates the prevention of medication errors, optimization of asset utilization, and compliance with regulatory requirements. Casella et al. (2022) illustrate that logistics and transportation companies utilize RFID for real-time visibility into shipments and asset tracking, thereby reducing transit times and optimizing warehouse operations. Furthermore, RFID technology extends its applications to asset tracking and management, agriculture, event management, and various other domains. Companies spanning different industries employ RFID tags to track equipment, tools, and high-value assets, improve livestock and agriculture management, and streamline event operations. Its versatility, efficiency, and reliability make RFID a valuable tool for organizations seeking to improve processes, enhance visibility, and innovation.

RFID technology stands out as a highly suitable solution for addressing management and security needs across industries. With its ability to automate data capture, track objects remotely, and operate without the need for direct line-of-sight contact, RFID offers incomparable efficiency and reliability. It provides organizations with the tools to optimize operations, improve visibility, and ensure compliance, whether through optimizing inventory management, tracking assets, or enhancing security measures. By utilizing this technology, businesses can enhance their management processes, reduce costs, and strengthen security measures to meet the challenges of an increasingly digital world.

RFID Technology Across Industries

In the Philippines, the implementation of RFID technology in expressways is a significant example of how AIDC technology is being integrated into daily life to improve efficiency and convenience. Starting July, only one RFID tag will be required for the country's toll expressways, which currently require two different ones due to having two different operators (Garcia, 2024). This change aims to make tollway transactions cashless, thereby shortening queues at tollway plazas and enhancing the overall travel experience for motorists. The RFID implementation is a testament to the versatility and efficiency of RFID technology in addressing real-world challenges, such as traffic congestion and the need for streamlined payment processes. This initiative not only demonstrates the practical application of RFID technology in transportation but also highlights its potential to revolutionize other sectors by automating data capture and reducing the need for manual intervention.

Expanding beyond transportation, RFID technology has become a cornerstone in the clothing industry, with its widespread implementation transforming various facets of the sector, as mentioned by Guo and Luo (2024) in their recent studies. Particularly, major clothing store companies are embracing RFID to revolutionize their operations. By embedding RFID tags into garments, these companies can effortlessly track inventory movements throughout the supply chain, optimize logistics processes, and enhance retail operations. Real-time visibility into inventory levels enables better decision-making, minimizes stockouts, and improves overall efficiency. Moreover, RFID facilitates seamless checkout experiences, reduces waiting times, and empowers customers with interactive fitting rooms and authentication services, thus elevating the retail experience (Hooda & Devi, 2021). With its anti-counterfeiting capabilities, RFID offers an effective solution to combat fraudulent activities, safeguarding brand integrity and consumer trust. As RFID technology continues to evolve, its integration into the clothing industry underscores its pivotal role in shaping the future of retail and supply chain management, as outlined in the case studies of Industry 4.0 implementation in the textile sector (2023).

Moreover, the incorporation of RFID technology into student ID systems represents a significant advancement in educational institutions, providing a variety of benefits aimed at simplifying operations and beefing up campus security. By implanting RFID chips into student ID cards, schools can revolutionize the way attendance is tracked, replacing time-consuming manual methods with efficient, automated systems, as highlighted by studies on RFID technology in educational settings (Koppikar et al., 2019). This not only saves time for students and teachers but also ensures accurate attendance records for administrative purposes. Additionally, RFID-enabled ID cards beef up campus security by allowing precise monitoring of student movements and controlling access to restricted areas (Sihombing et al., 2019). With strategically placed RFID readers at entry points, schools can quickly identify and address potential security breaches, thereby creating a safer learning environment. Furthermore, these multi-purpose ID cards enhance various administrative tasks, such as library access, cafeteria purchases, and event registration, consolidating functions into a single card for improved operational efficiency and student convenience, as outlined in studies of Sathvik et al. (2021) on the integration of RFID technology in student ID systems. As educational institutions continue to embrace technological advancements, the integration of RFID technology into student ID systems plays a crucial role in modernizing campus operations and enhancing the overall educational experience, as predicted by future trends in this field (Markoska & Markoski, 2022).

Technological Innovations Revolutionizing Attendance Monitoring in Educational Institutions

Attendance monitoring systems represent a fundamental aspect of educational institutions, serving as a cornerstone for tracking student participation, ensuring accountability, and optimizing administrative processes. Traditional methods, reliant on manual paper-based systems or contact-based methods, often suffer from inefficiencies, inaccuracies, and limited real-time data analysis capabilities. However, the advent of technological innovations has paved the way for a new era in attendance monitoring, with recent studies showcasing the potential of RFID-based systems to revolutionize this essential aspect of educational administration.

The introduction of RFID-based Student Identification Card Attendance Monitoring Systems, as demonstrated by studies such as that by Bamidele et al. (2023), marks a significant advancement in attendance tracking methodologies. These systems leverage Radio Frequency Identification (RFID) technology in conjunction with programmable logic circuits, such as Arduino, to address the inherent limitations of traditional approaches. Each student and lecturer is equipped with an RFID card, which, upon proximity to an RFID reader, triggers the recording of attendance data, including the unique identifier (UID) and timestamp. By integrating real-time clock modules and secure digital (SD) card storage, these systems ensure not only automated attendance capture but also robust data backup and accessibility.

The adoption of RFID-based attendance monitoring systems offers a myriad of advantages over traditional methods. Firstly, the automation of attendance tracking processes eliminates the need for manual data entry, thereby reducing the likelihood of errors and discrepancies. Furthermore, the real-time nature of RFID technology enables instantaneous data capture, providing administrators with up-to-date attendance records for informed decision-making. Studies have also highlighted the role of RFID systems in enhancing security and accountability within educational institutions, as the unique identification codes associated with RFID cards help mitigate instances of proxy attendance or unauthorized access.

In addition to automated attendance capture, researchers have explored the integration of RFID technology with supplementary communication channels to enhance stakeholder engagement. Studies conducted by Antonio et al. (2019) and Nueva et al. (2024) showcase the utilization of Short Messaging Service (SMS) notifications and web-based applications to facilitate real-time communication between parents, teachers, and students. Through SMS notifications, parents receive instant updates regarding their child's attendance, fostering transparency and parental involvement in the educational process. Web-based applications further extend the utility of RFID systems by providing administrators with centralized platforms for attendance management, report generation, and data analysis.

The development and implementation of RFID-based attendance monitoring systems entail rigorous testing and stakeholder engagement processes. Researchers employ a combination of hardware setup, software development, and iterative testing methodologies to ensure the functionality, reliability, and user-friendliness of these systems. Stakeholder feedback, including input from students, teachers, and administrators, plays a pivotal role in refining system features and addressing usability concerns. By incorporating diverse perspectives and leveraging iterative design methodologies, researchers strive to develop RFID systems that seamlessly integrate into educational environments while meeting the diverse needs of stakeholders.

The evolution of RFID-based attendance monitoring systems is poised to have profound implications for educational institutions worldwide. Continued advancements in RFID technology, coupled with innovations in data analytics and artificial intelligence, hold the promise of further enhancing the efficiency, accuracy, and accessibility of attendance tracking processes. Moreover, the integration of RFID systems with emerging technologies such as biometrics and facial recognition presents exciting opportunities for augmenting security and personalization within educational settings. As educational institutions continue to embrace digital transformation initiatives, RFID-based attendance monitoring systems are likely to play an increasingly integral role in shaping the future of administrative processes and student engagement strategies.

In conclusion, technological innovations in attendance monitoring systems, particularly those leveraging RFID technology, represent a paradigm shift in educational administration. These systems not only streamline attendance tracking processes but also empower stakeholders with real-time data insights, enhanced communication channels, and improved security measures. By embracing RFID-based solutions and fostering interdisciplinary collaborations, educational institutions can unlock new avenues for optimizing administrative efficiency, enhancing student engagement, and driving positive educational outcomes in the digital age.

Enhancing Efficiency Through Automated Systems in Various Domains

The integration of automated systems across diverse domains represents a transformative approach to optimizing processes, improving efficiency, and enhancing user experiences. From automated parking management systems to risk management strategies in cultural institutions, recent studies emphasize the potential of technology-driven solutions to address complex challenges and streamline operations.

Automated systems have emerged as a cornerstone of modernization efforts across various domains, offering innovative solutions to longstanding challenges. Studies such as those by Dichoso et al. (2022) and Galora (2023) exemplify the diverse applications of automation, ranging from parking management to risk mitigation in cultural heritage institutions. By leveraging technologies such as Radio Frequency Identification (RFID), data analytics, and cloud computing, these systems enable seamless integration of processes, real-time data insights, and enhanced user experiences.

The implementation of RFID-based Automated Parking Management Systems, as explored by Dichoso et al. (2022), represents a paradigm shift in urban mobility solutions. These systems leverage RFID technology to streamline parking procedures, including entry and exit, payment processing, and slot location. By offering cashless, contactless, and paperless transactions, automated parking systems enhance convenience for users while optimizing parking space utilization and reducing traffic congestion. Moreover, the integration of real-time data analytics enables operators to monitor parking patterns, predict demand, and optimize resource allocation for improved service delivery.

In cultural institutions, the relocation of collections and preservation of heritage assets pose unique challenges that require meticulous planning and risk mitigation strategies. Galora's (2023) study investigates the motivations and strategies behind the relocation of collections in Filipiniana institutions, emphasizing the importance of risk management to safeguard valuable artifacts and institutional core motivations. By employing qualitative and quantitative methods, the study highlights the need for proactive risk assessment, stakeholder engagement, and contingency planning to mitigate potential threats and ensure the long-term preservation of cultural heritage.

The development and implementation of automated systems necessitate rigorous testing, iterative refinement, and stakeholder engagement to ensure effectiveness and acceptance. Researchers employ a combination of hardware prototyping, software development, and user testing methodologies to validate system functionalities and address usability concerns. Moreover, stakeholder engagement plays a pivotal role in identifying user requirements, gathering feedback, and fostering collaborative partnerships for successful deployment and adoption of automated solutions.

Looking ahead, the evolution of automated systems is certain to have far-reaching implications for various sectors, including transportation, healthcare, and environmental management. Continued advancements in sensor technology, artificial intelligence, and Internet of Things (IoT) offer unprecedented opportunities for innovation and optimization. By embracing automation, organizations can streamline operations, reduce costs, and enhance service quality, ultimately driving sustainable growth and societal progress in the digital age.

Automated systems represent a tool for transformation across diverse domains, offering novel solutions to complex challenges and unlocking new opportunities for efficiency and innovation. Whether in the field of urban mobility or cultural heritage preservation, the integration of automation holds the promise of improving user experiences, optimizing resource utilization, and fostering sustainable development. By embracing technological advancements and fostering collaboration between stakeholders, organizations can harness the power of automation to drive positive change and shape a more resilient and prosperous future for all.

**Related Systems**

Easytrip & Autosweep

A Radio Frequency Identification (RFID) system has revolutionized the way motorists traverse expressways in the Philippines. Found in condominiums, office buildings, and toll gates, RFID employs electromagnetic fields to automatically identify and track tags or stickers affixed to vehicles. In Luzon, two major RFID brands, Easytrip and Autosweep, dominate the expressway landscape, ensuring swift and seamless journeys for drivers.

Easytrip, managed by the Metro Pacific Tollways Corporation (MPTC), facilitates convenient travel on expressways such as CAVITEX, C5 Link, CALAX, NLEX, and SCTEX. Conversely, Autosweep, administered by the San Miguel Corporation (SMC), powers the toll collection systems on SLEX, SKYWAY, NAIAX, STARTOLL, TPLEX, and MCX. This division ensures that motorists can easily identify the appropriate RFID system for their chosen route.

As of November 2, 2020, cashless payment systems have become mandatory for drivers of Class 1, 2, and 3 vehicles. This transition eliminates toll booths designated for cash transactions, streamlining traffic flow and reducing congestion on expressways. While Easytrip and Autosweep previously allowed online sticker purchases, instances of improper installation have prompted the implementation of mandatory installation at designated sites. This measure ensures proper placement and functionality of RFID stickers, enhancing the efficiency of the cashless toll system.

RFID technology promises to significantly reduce travel time and enhance overall convenience for motorists in Luzon. With Easytrip and Autosweep emerging as the primary RFID service providers, drivers can expect smoother transactions and improved travel experiences on expressways. Even beyond the November 2nd deadline, installation services will remain readily available, ensuring that every driver can seamlessly transition to the cashless toll system without hassle.

FILIPAY & FILIPCOIN

RFID technology has seen widespread adoption for transportation systems in the Philippines. The article by Malapo (2021) sheds light on the transformative efforts undertaken by the Smart Electronics and Applications Institute (SEAI) to revolutionize the transportation sector in the Philippines, primarily through the introduction of two innovative systems: FILIPAY and FILIPCOIN.

FILIPAY stands out as a pioneering system in the Philippines' transportation landscape, introducing the Tap In/Tap Out automated fare collection system (AFCS). This system represents a significant leap forward in terms of convenience, efficiency, and security in fare payment mechanisms. By implementing a contactless payment system, FILIPAY streamlines the process for commuters, reducing queues, and minimizing the need for physical cash transactions. The Tap In/Tap Out feature enables passengers to simply tap their cards or devices upon entry and exit, automatically deducting the appropriate fare based on the distance traveled or other relevant factors.

Complementing FILIPAY is FILIPCOIN, a decentralized network aimed at revolutionizing fare payment systems further. FILIPCOIN leverages blockchain technology, specifically Ethereum and Binance Smart Chain, to facilitate secure and efficient transactions within the transportation ecosystem. The utilization of blockchain not only enhances the security and transparency of transactions but also promotes the widespread adoption of digital currencies for fare payments (Habib et al., 2022). The introduction of FILIPCOIN's native token, FCP (FILIPCOIN), serves as a catalyst for the transition towards digital currency trends in transportation fare payments globally. This decentralized approach not only enhances the efficiency of fare collection but also ensures greater resilience and reliability in the face of potential system failures or disruptions (Bieler et al., 2002). By utilizing blockchain technology, FILIPCOIN aims to decentralize the management of data, offering improved accessibility, reduced service failures, and lower transaction costs compared to centralized or distributed systems.

Similarly, in agriculture, Rayhana et al. (2021) discuss the adoption of emerging technologies in agriculture, particularly the shift towards "smart" agriculture practices. The paper highlights the aim of smart agriculture to automate various aspects of plant growing processes to enhance efficiency, yield, and crop quality while reducing labor requirements. Specifically, the study focuses on the application of Radio Frequency Identification (RFID) sensing technology in agriculture. The paper provides an introduction to RFID sensing technology and surveys its applications across four key areas of agriculture: plant growing environment, soil conditions, plant growth, and the quality of harvests. The aim is to identify the unique capabilities of RFID sensing technology in addressing agricultural challenges, as well as its limitations.

In the context of transportation infrastructure, Lindawati et al. (2020) present a Radio Frequency Identification (RFID)-based parking slot detection system designed to facilitate motorists in determining the availability of parking slots and locating empty slots within a parking lot. The system is particularly suitable for buildings with large, multi-storey parking spaces. Utilizing components such as Arduino Mega, photodiode sensor, RFID tag, and RFID reader, the system operates by notifying information about parking slots through a speaker after the driver uses an RFID card at the entrance portal of the parking lot. Through tests conducted, the study demonstrates that the RFID-based parking slot detection system effectively provides motorists with information regarding the availability and location of empty parking slots. RFID card at the entrance portal of the parking lot. Through tests conducted, the study demonstrates that the RFID-based parking slot detection system effectively provides motorists with information regarding the availability and location of empty parking slots.

Advancements in RFID Security: Integrating Cryptographic Protocols and Efficient Algorithms for IoT Systems

The intersection of Radio Frequency Identification (RFID) technology and advanced cryptographic protocols marks a significant stride in fortifying the security posture of Internet of Things (IoT) systems. These studies collectively highlight the multifaceted approach required to mitigate evolving security threats while ensuring the efficiency and practicality of RFID deployments. Origines et al. (2019) delve into the realm of lightweight authentication protocols, where they propose enhancements utilizing elliptic curve cryptography (ECC) and modified pseudorandom number generation (PRNG) algorithms. By leveraging epoch timestamps as seeds for PRNG, the study not only enhances security but also addresses efficiency concerns inherent in RFID systems. The integration of ECC not only bolsters security but also aligns with the trend towards lightweight cryptographic solutions suitable for resource-constrained IoT devices.

Harahap et al. (2023) expand on this foundation by introducing hybrid cryptographic algorithms tailored specifically for RFID data protection within IoT networks. Recognizing the dynamic nature of IoT environments characterized by high autonomous data capture rates and network connectivity, the study proposes a fusion of Advanced Encryption Standard (AES) and Elliptic-curve Diffie-Hellman (ECDH) keys. This hybrid approach not only enhances security but also reflects a pragmatic response to the interoperability demands of IoT ecosystems. By leveraging Python programming and Jupyter Notebook environments, the study demonstrates the feasibility of their approach while offering insights into potential implementation challenges and performance considerations.

Complementing these efforts, el Batouty et al. (2020) introduce a novel algorithmic framework aimed at bolstering RFID security through the design of a modified Substitution Box (S-Box) using chaotic maps. By harnessing chaotic dynamics, the proposed algorithm yields a key and plaintext-dependent S-Box, thereby enhancing the resistance against various cryptographic attacks. The meticulous evaluation of the proposed S-Box against state-of-the-art implementations underscores its efficacy in fortifying Advanced Encryption Standard (AES) encryption within RFID technology. Moreover, the study's focus on evaluating both security and performance metrics reflects a holistic approach essential for the practical deployment of cryptographic solutions in real-world IoT scenarios.

Efficiency emerges as a central theme in the discourse surrounding RFID security, particularly concerning the resource limitations inherent in RFID tags. Ali et al. (2021) tackle this challenge by proposing an RFID authentication scheme based on hyperelliptic curve Signcryption. By leveraging hyperelliptic curves, the study achieves a balance between security and efficiency, crucial for resource-limited RFID tags. Formal security analysis techniques, such as the Real-Or-Random (ROR) model and Automated Validation of Internet Security Protocols and Applications (AVISPA), validate the scheme's robustness against potential attacks while demonstrating significant efficiency gains compared to existing schemes based on Elliptic Curve Cryptography (ECC).

Similarly, Kumar et al. (2024) contribute to this discourse by designing a lightweight group authentication protocol tailored specifically for secure RFID systems. Through a comprehensive analysis of security vulnerabilities in existing RFID authentication schemes, the study proposes a novel protocol emphasizing stringent security, privacy, and cost-effectiveness. The protocol's design not only addresses existing vulnerabilities but also ensures compatibility with the resource constraints typical of RFID deployments. Formal security analysis coupled with performance evaluations offers compelling evidence of the protocol's superiority over existing schemes, positioning it as a promising solution for securing RFID systems in diverse IoT environments.

Moreover, cryptographic algorithm advancements play a pivotal role in augmenting the security of IoT systems, as demonstrated by De Leon et al. (2019). Their work on enhancing the Tiny Encryption Algorithm (TEA) exemplifies the iterative refinement required to mitigate evolving cyber threats effectively. Through meticulous modifications to TEA's key scheduling and round function, the study achieves improved security properties essential for safeguarding IoT devices against sophisticated attacks. The rigorous evaluation of the modified TEA against standard cryptographic benchmarks underscores its efficacy in fortifying data security for IoT deployments, reaffirming the critical role of cryptographic primitives in IoT security architectures.

These studies collectively underscore the dynamic and interdisciplinary nature of securing IoT systems, particularly in the context of RFID technology. By integrating advancements in cryptographic protocols, algorithmic frameworks, and security analysis techniques, researchers strive to strike a delicate balance between security, efficiency, and practicality essential for realizing the full potential of IoT deployments in diverse application domains.

Chapter 3

This chapter discusses the manual processes of the current system and the processes involved in the proposed system, along with the software, hardware, and peopleware requirements of the proposed system.

**Technical Background**

**Current System**

In one of the Philippine State Universities, security measures heavily rely on manual processes. Student ID verification is sometimes done with security personnel checking students' IDs. Parents of ILS students remain uninformed about their children's whereabouts, as there is no automated notification system in place. Additionally, the manual inspection of vehicles entering the campus causes delays and inefficiencies. During school events, the complex process of recording attendance with pen and paper leads to long lines and potential inaccuracies.

**Proposed System**

The proposed system provides a comprehensive solution by introducing a long-range RFID scanner at the university entrance to automate student ID verification. This technology will ensure accurate identification and an efficient entry process. Moreover, automated text notifications will be implemented to alert parents of ILS students about their children's arrivals and departures. By embedding RFID stickers in vehicles, the system will provide the security personnel with real-time vehicle details on a monitor screen, enhancing security and efficiency. Furthermore, event attendance recording will be automated using a long-range RFID scanner at the gym entrance, eliminating manual processes, and reducing waiting times.

Software Requirements

|  |  |  |
| --- | --- | --- |
| **Name** | **Features** | **Purpose** |
| Visual Studio Code | * Visual Studio provides a unified platform for developers to create, debug, and deploy applications efficiently. * Supports a wide range of programming languages, allowing developers to choose the most suitable language for their needs. * Visual Studio offers version control integration and collaboration features, facilitating teamwork among developers. * Visual Studio supports a  wide range of extensions, enhances functionality and integrates with various tools and services. * Visual Studio supports cross-platform development, this enables the development of applications that run on different platforms, fostering flexibility. * Visual Studio features debugging tools for identifying and resolving code issues during development. * Visual Studio has a comprehensive IDE for various projects and provides a comprehensive integrated development environment for different project types, including web, mobile, and cloud applications. | Visual Studio serves as an adaptable and unified development environment, making the coding and collaboration processes for developers working on different  projects. |
| Laravel Framework | * Powerful tools for building web applications. * Modular packaging system with dependency manager. * Built-in support for authentication and authorization. * Powerful ORM system. | Laravel Framework aims to simplify the development process by maximizing developer productivity and maintaining code quality and scalability. |
| PHP | * Server-side scripting language. * Server-side scripting language. * Wide ecosystem of libraries and frameworks. * Adaptable and embeddable into HTML. | PHP is widely used for developing dynamic websites and web applications, enabling developers to create interactive and feature-rich online platforms across various industries. |
| CSS | * Style sheet language for document formatting. * Control over layout, colors, fonts, etc. * Separation of content and presentation. | Its role in web development is defining the visual presentation of web pages, enhancing the user experience, and enabling the creation of modern and responsive websites. |
| Twilio API | * Cloud communications platform * Integration of messaging, voice, and video capabilities * Advanced features like number provisioning and call recording | Twilio API simplifies the integration of communication functionality into applications, allowing developers to easily add features such as SMS notifications, voice calls, and two-factor authentication to their projects. |
| Hostinger | * Hostinger provides support for relational databases, allowing users to organize and manage data efficiently through structured tables. * Hostinger's database hosting is designed to scale, accommodating growing datasets and increasing demands, making it suitable for dynamic applications. * Hostinger's performance optimization Implements caching, indexing, and query optimization to enhance database performance, ensuring efficient handling of data and complex queries. * Hostinger incorporates various security features, including user authentication, access control, and encryption, to protect sensitive data stored in the database. | Hostinger's database hosting service aims to provide a strong and flexible solution for users to store, manage, and secure their data. It ensures optimal performance and reliability for applications relying on databases. |
| Laragon | * Portable, isolated, and fast development environment * Supports PHP, Node.js, Python, and other web technologies * Lightweight alternative to traditional development stacks | Laragon aims to simplify the local development process by providing developers with a lightweight and feature-rich environment that is easy to set up and use, enhancing productivity and creativity in the development workflow. |
| Readersoft | * Readersoft supports customization of RFID reader output, allowing users to choose an output format to their specific requirements. * Users can configure output to be in hexadecimal, decimal, or other formats supported by the RFID reader. * Readersoft enables users to specify the length of output, adjusting the number of characters transmitted per read. * The software offers flexibility in output settings, allowing users to define delimiters and formatting options for seamless integration with existing systems. | Readersoft enhances the usability of RFID readers by providing a customizable solution for managing output formats. It enables users to adapt RFID reader output to suit their application needs, ensuring compatibility and efficiency in data processing and integration. |

**Table1.** *Proposed System Software Requirements*

Hardware Requirements

|  |  |  |
| --- | --- | --- |
| **Name** | **Features** | **Purpose** |
| Desktop Computer/Laptop | The minimum hardware requirements for the desktop computer or laptop using the system:   * Processor: 10th generation of an Intel Core i3 or above. * RAM: At least 4 GB of RAM. * Storage: SSD or HDD with at least 500 GB capacity. * Operating System: A 64- bit version of Windows 10. | Running the system on a desktop computer/laptop and utilizing its features. |
| UHF Long Range RFID Reader | * Frequency: A reading frequency of 902 - 928MHz * Reading Distance: A reading range of 1-8 meters. | Detecting Student ID’s and RFID embedded vehicles. |
| UHF RFID Cards | * Frequency: A frequency of 860-960MHz | Student ID cards will be in high frequency so that it will be readable by the UHF readers. |
| UHF RFID Sticker | * Frequency: A frequency of 860-960MHz | Attached to registered vehicles for identification and access control. |

**Table 2.** *Proposed System Hardware Requirements*

Peopleware

*Students*

* The students are primary end-users of the system. They interact with it by scanning their student IDs for entry, exit, and attendance purposes. They are responsible for adhering to the system's rules and procedures.

*Guardians*

* The guardians, typically parents or legal guardians of ILS students, play a secondary role in the system. They may receive automated notifications regarding their children's entry and exit from the campus, providing them with real-time information about their children's whereabouts.

*Vehicle Owners*

* Registered vehicle owners who frequently access the campus will benefit from the system's RFID vehicle identification feature. They can expect smoother entry processes with automated vehicle checks, contributing to enhanced campus security and efficiency.

*Security Personnel*

* The security personnel are essential operators of the system, responsible for monitoring and managing campus entry points. They utilize the system to verify student IDs, inspect vehicles (if necessary), and ensure campus security protocols are followed.

*Organization Officers*

* Organization officers representing different campus organizations may have specific access privileges within the system. They can use the system to track attendance at organization or university wide events that is held at the gymnasium.

*Admin*

* The Administrator oversees the entire system. They have full access and control over system functionalities, including managing user accounts, configuring system settings, and ensuring system integrity and security.

Network Plan

In our network plan, we will be using one computer along with three long-range RFID readers, one placed at the entrance of the university where it would record all student logs, one will be at the vehicle entrance to record all vehicle logs, then another one placed at the entrance of the gymnasium to record student attendance for events.

There will be one account for each university organization so they can have access to create an event attendance sheet for their respective organization, they would need to use a phone or a computer connected to the university’s network to access the site.

For the hosting service, we will be using Hostinger for its support with relational databases and scalable hosting solutions, ensuring efficient data management and long-term feasibility for the application. Hostinger's emphasis on performance optimization and security aligns with a smooth user experience and protecting sensitive data

A computer and mobile devices

Description automatically generated with medium confidence

**Figure 1.** *Proposed System Network Diagram*

Chapter 4

This chapter discusses the methods employed in the development of the system. Specifically, it discusses the requirements analysis and the system design. Providing a deep understanding of the procedures involved in development and the study of the system.

**Methodology**

This research design adopts a quantitative approach, allowing researcher to systematically collect and analyze data from a larger number of individuals. This methodology enables us to summarize key characteristics across different groups or explore relationships within the phenomenon under investigation with statistical rigor and precision.

The sampling technique that will be utilized is stratified random sampling. The selection of stratified random sampling as the sampling technique for this research is driven by its capacity to effectively address the heterogeneity present within the target population. Given that populations often consist of diverse subgroups with distinct characteristics, stratified random sampling allows researchers to partition the population into homogeneous strata based on these attributes. By doing so, researchers ensure that each subgroup is adequately represented in the sample, thus enhancing the precision and accuracy of our estimates. This approach enables researchers to obtain a more comprehensive understanding of the population by capturing variability across different segments.

The target population for this study surrounds individuals associated with the university campus, including students, guardians, vehicle owners, security personnel, and organization officers. To ensure a comprehensive understanding of the system's effectiveness and user satisfaction, the population has been stratified into distinct groups based on their roles and interactions with the campus system. This stratification acknowledges the diverse responsibilities and requirements of each subgroup within the campus community.

Students, as primary end-users of the system, are responsible for utilizing it for entry, exit, and event attendance tracking purposes. Guardians, in a secondary role, will receive automated messages regarding their children's entry and exit from the campus, providing them with real-time information about their whereabouts. Registered vehicle owners, another subgroup, benefit from the system's RFID vehicle identification feature, which modernizes entry processes and contributes to enhanced campus security and efficiency.

Security personnel play a crucial role as operators of the system, responsible for monitoring and managing campus entry points. They utilize the system to verify student IDs, inspect vehicles if necessary, and ensure campus security protocols are followed.

The choice of stratification is justified by the distinct roles and responsibilities of each subgroup within the campus ecosystem. By stratifying the population, the study aims to conduct targeted analysis and organize system improvements to meet the specific needs of each group. The sampling process involves determining sample sizes for each stratum based on their relative importance and representation within the population. Samples are then randomly selected within each stratum to ensure unbiased representation, with the number of samples proportional to the size of each subgroup. This approach ensures that the study captures the perspectives and experiences of all user groups within campus community, facilitating a comprehensive analysis of system usage and user satisfaction.

For the calculation of sample size, researchers will determine the percentage of population they need to be the research respondents. The proportion of the total population that each stratum represents will be calculated by dividing the size of each stratum by the total size of the population. Once the proportions are there, the total sample size wished to collect will be multiplied by the proportion of each stratum to determine how many individuals is needed to sample from each stratum.

For data collection, survey questionnaires will be employed as the primary instrument. A structured questionnaire will be meticulously designed, consisting a closed-ended question to capture relevant information from the respondents. To ensure a representative sample, a stratified random sampling technique is implemented, stratifying the population into distinct groups based on factors. Survey questionnaires will then be disseminated to the samples within each stratum. Clear instructions will be provided to respondents, emphasizing the significance of providing accurate and honest responses. Additionally, a specific collection period will be established to maintain consistency and timeliness throughout the data collection process. These measures collectively aim to facilitate strong data collection while ensuring the integrity and reliability of the information that will be gathered.

For data analysis, researchers will use descriptive statistics. As noted by Kaliyadan & Kulkarni (2019), without making any deductions based on probability theory, descriptive statistics provide an overview of the sample under investigation.

**Requirement Analysis**

|  |  |
| --- | --- |
| Performance Requirements | * Response Time: The system should have low response times when processing access requests or logging attendance to ensure quick and efficient operation, especially during peak usage periods. * Scalability: The system should be able to handle a large number of users and vehicles simultaneously without experiencing performance degradation, as the university may have a significant student population and vehicle traffic. * Reliability: The system should be highly reliable, with minimal downtime or system failures, to ensure continuous access control and attendance logging functionality. * Accuracy: The system should accurately identify and log student and vehicle access, as well as attendance records, to maintain data integrity and ensure accurate reporting. * Security: The system should have robust security measures in place to prevent unauthorized access or tampering with attendance records, safeguarding the integrity and privacy of student and vehicle data. * Interoperability: The system should be compatible with various RFID tags and readers, ensuring interoperability with different types of student and vehicle identification technologies. * Auditability: The system should provide audit trails and logs of access control activities and attendance records, enabling administrators to track system usage and investigate any discrepancies. * User Experience: The system should offer a user-friendly interface for both students and administrators, making it easy to access campus facilities and view attendance information. * Maintenance: The system should require minimal maintenance and support efforts, with automated monitoring and alerting mechanisms to detect and address any performance issues promptly. |
| Safety Requirements | * Electrical Safety: All electronic components and devices, including scanners, must comply with safety standards to prevent electrical hazards. Proper insulation, grounding, and circuit protection mechanisms should be implemented to mitigate the risk of electric shock or fire hazards. * Physical Safety: The contact-based scanner and contactless RFID scanner should be securely installed and positioned to prevent physical harm to users. Sharp edges or protruding parts should be adequately covered or shielded to prevent accidental injuries. * Data Protection: Safeguards must be in place to protect sensitive user data stored in the system's database. Encryption techniques should be employed to secure data transmission and storage, ensuring that personal information, such as user IDs and transaction records, remains confidential and protected from unauthorized access or tampering. * System Reliability: The system should undergo rigorous testing and quality assurance processes to ensure its reliability and stability. Regular maintenance checks and inspections should be conducted to identify and address any potential safety concerns or malfunctions promptly. * Emergency Procedures: Clear and documented emergency shutdown procedures should be established to guide users and administrators in case of system malfunction, security breaches, or other unforeseen incidents. These procedures should include steps for safely powering down the system and addressing any immediate safety risks. * Compliance with Regulations: The system design and operation must comply with relevant safety regulations and industry standards governing the use of RFID technology in library environments. This includes adherence to standards set by regulatory bodies such as OSHA (Occupational Safety and Health Administration) and FCC (Federal Communications Commission). * User Training and Awareness: Adequate training programs should be provided to library staff and users to ensure their understanding of safety protocols and proper use of the system. Users should be informed about potential safety hazards and instructed on how to respond in case of emergencies or system malfunctions. |
| Security Requirements | * Access Control: The system must enforce strict access control measures to prevent unauthorized access to sensitive information and system functionalities. User authentication mechanisms, such as username/password authentication and role-based access control, should be implemented to ensure that only authorized individuals can access specific features or data within the system. * Data Encryption: All communication channels and data storage facilities must employ encryption techniques to protect data integrity and confidentiality. This includes encrypting user credentials, transaction records, and other sensitive information to prevent unauthorized interception or tampering. * Audit Trails: The system should maintain detailed audit trails of user activities, including login attempts, data modifications, and system configurations. These audit logs serve as a security measure to monitor for suspicious behavior or unauthorized access and facilitate forensic analysis in case of security incidents. * Physical Security: Physical access to system components, such as servers and databases, should be restricted to authorized personnel only. Adequate physical security measures, such as access controls, surveillance cameras, and intrusion detection systems, should be implemented to prevent unauthorized entry or tampering with hardware devices. * Incident Response: The system should have predefined incident response procedures in place to address security breaches, data breaches, or other security incidents promptly. These procedures should include steps for containment, investigation, remediation, and communication with affected parties, as well as compliance with regulatory reporting requirements. * Vulnerability Management: Regular security assessments and vulnerability scans should be conducted to identify and mitigate potential security weaknesses in the system. Patch management processes should be implemented to ensure that software vulnerabilities are promptly addressed with security updates or patches. * Privacy Compliance: The system must comply with applicable privacy regulations and laws governing the collection, storage, and processing of personal data. User consent should be obtained for data collection and processing activities, and appropriate measures should be taken to safeguard user privacy rights. |

**Table 3.** *System Requirement Analysis*

**System Design**

System Development Life Cycle

Agile methodologies, characterized by their iterative nature and emphasis on continuous delivery, are particularly suitable for this project. Unlike traditional models, Agile frameworks promote adaptive planning, allowing for changes in requirements and priorities throughout the development process. Each iteration delivers potentially shippable increments of the product, ensuring a steady pace of development and alignment with evolving stakeholder needs. Agile's focus on collaboration, feedback, and incremental improvement aligns well with the dynamic nature of this project and its need for continuous refinement.

A diagram of a process

Description automatically generated

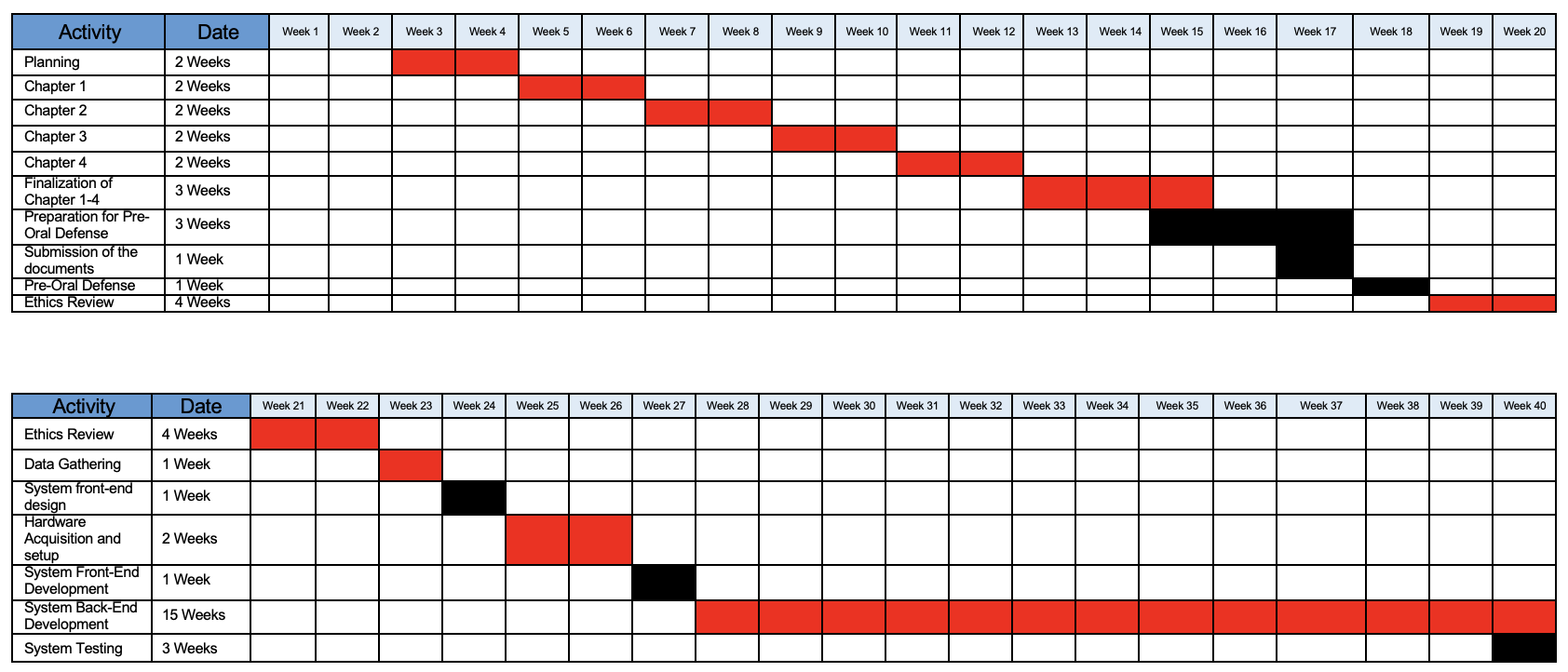
**Figure 2.** *SDLC Model - Agile*

Planning Phase

* + Define and refine the overall objectives of the RFID-Based access control and event attendance tracking for the campus based on evolving needs and feedback.
  + Identify key stakeholders and ensure ongoing communication and collaboration throughout the project.
  + Maintain a dynamic list of high-level system requirements and constraints, prioritized based on immediate needs and feedback from users and stakeholders.
  + Establish a flexible project timeline, breaking down work into smaller tasks or user stories that can be pulled into the workflow as capacity allows.

Gantt Chart

The chart below is a Gantt chart that serves as a map showing when tasks happen. It helps researchers see what needs to be done and when. This helps use the time and resources well, so researchers can make good decisions and keep things moving forward smoothly.



**Figure 3.** *Proposed System Gantt Chart (Week 1-40)*

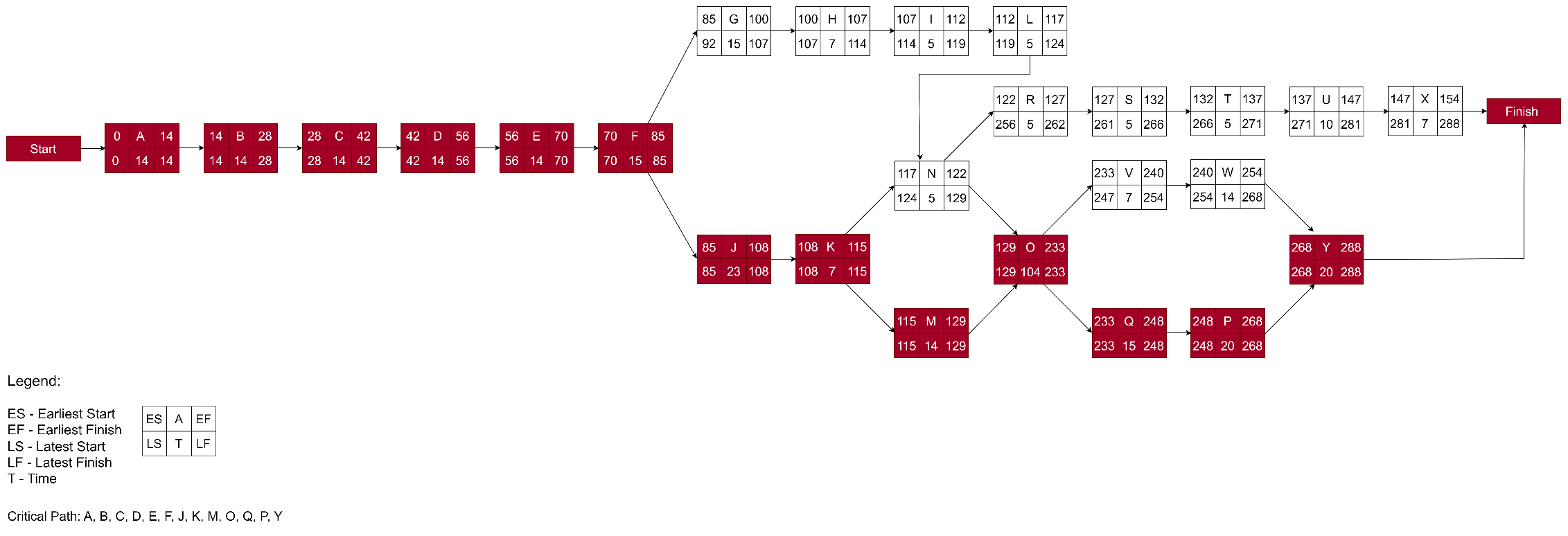
A red square on a white grid

Description automatically generated with medium confidence

**Figure 4.** *Proposed System Gantt Chart (Week 41-55)*

PERT Chart

The PERT chart is the big picture of researchers' tasks and how they connect. It helps researchers see which tasks are most important and how long they might take. This helps plan the work and deal with any problems that might come up along the way.



**Figure 5.** *Proposed System Pert Chart*

Activity List

This research's activity list is a detailed plan of everything that needed to be done. It tells what each person needs to do and when, then helps researchers work together and make sure everybody are all doing their part to reach the research objectives.



**Table 4.** *Proposed System Activity List*

Analysis Phase

* + Gather and refine detailed requirements by analyzing the existing manual processes and incorporating ongoing feedback from stakeholders and users.
  + Identify and prioritize specific functionalities and features required for the RFID-Based access control and event attendance tracking system.
  + Conduct ongoing feasibility analyses to ensure the proposed system remains viable and aligns with the evolving needs of the library environment.

Design Phase

* + Design and refine the architecture and user interface of the system based on emerging requirements.
  + Design and refine the architecture and user interface of the system based on emerging requirements.

Coding Phase

* + Develop and refine the system in iterations, focusing on delivering small, valuable increments of functionality that can be deployed as soon as they are ready.
  + Implement RFID technologies incrementally, prioritizing features based on user and stakeholder feedback.
  + Code functionalities related to event attendance tracking and access control for cars and students, ensuring each piece of functionality adds value to the system.

Testing Phase

* + Execute unit tests for each component, focusing on the smallest units of functionality such as individual functions or methods.
  + Conduct system-wide end-to-end testing, such as event attendance tracking and access control for the students.
  + Develop a UAT test plan that outlines the strategy for verifying the system against the project requirements. Conduct UAT sessions with real-world user roles and scenarios and document the test results, including any issues or defects found.
  + Re-test the system to ensure that the fixes have resolved the issues and that no new issues have been introduced
  + Continuously iterate on the system based on feedback and performance data, adjusting as necessary to improve the system's functionality and user experience.

Deployment Phase

* + Deploy the developed system incrementally to the campus, prioritizing features and updates based on user needs and stakeholder feedback.
  + Conduct ongoing testing and gather user feedback throughout the deployment process, addressing any issues or concerns as they arise.
  + Iterate on the deployed system based on feedback and performance data, continuously improving, and refining the system over time to better meet the needs of users.

|  |  |  |
| --- | --- | --- |
| **Test Plan** | **Security Plan** | **Maintenance Plan** |
| * Develop test cases for each functionality. * Conduct unit testing, integration testing, and system testing at each development phase. * Ensure proper validation of RFID scanning. | * Implement encryption for RFID data. * Regularly monitor and update the security system to address vulnerabilities. * Conduct penetration testing to identify and fix potential security issues. | * Schedule regular maintenance for RFID scanners and alert systems. * Update the system to accommodate any changes in library policies or requirements. * Provide training to library staff on system maintenance. |

**Table 5.** *Proposed System Deployment Plan*

Context Free Diagram

The context diagram is used to define the boundaries and context of the system that must be modeled (Context Diagrams, n.d.). It was emphasized that it shows what is inside and outside the system and how it is related to these outside entities. The following comprehensive context-free diagram of the proposed book security system illustrates the innovative integration of contactless and contact-based RFID technologies to enhance the security measures for the library's reading materials.

A diagram of a library security system

Description automatically generated

**Figure 6.** *Proposed System Context Free Diagram*

Data Flow Diagram

In this section, researchers present a comprehensive data flow diagram illustrating the proposed book security system the library, which integrates contactless and contact-based RFID technologies to enhance the security and efficiency of book borrowing, return, and access monitoring processes. Data-flow diagrams, or DFDs, represent a user-friendly perspective of the system - the way data moves through the system and the processes involved in handling it (“Introduction to Data-flow Diagrams,” n.d.).

A diagram of a structure

Description automatically generated with medium confidence

**Figure 7.** *Proposed System Data Flow Diagram (Organization)*

A diagram of a structure

Description automatically generated with medium confidence

**Figure 8.** *Proposed System Data Flow Diagram (Vehicles)*

A diagram of a structure

Description automatically generated with medium confidence

**Figure 9.** *Proposed System Data Flow Diagram (Students)*

Entity Relationship Diagram

An Entity Relationship Diagram (ERD) visually depicts the division of a system's subject domain into entities, comprising edges to signify relationships and nodes to denote various entity types.

A diagram of a company

Description automatically generated with medium confidence

**Figure 10.** *Proposed System Entity Relationship Diagram*

Database Normalization

According to the study of Singh, et.al (2020), Data normalization is one of the pre-processing approaches where the data is either scaled or transformed to make an equal contribution of each feature. It includes discretization of data, removing outliers and noise from the data, integration of data from various sources, dealing with incomplete data and transformation of data to comparable dynamic ranges.

Users Table:

The user’s table is in 3rd Normal form, with username, email, password, and user type as non-key attributes that are fully dependent on the id primary key. This table meets the criteria for 3NF, as there are no transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| id | INT | Primary Key(PK) |
| username | VARCHAR |  |
| email | VARCHAR |  |
| password | VARCHAR |  |
| user\_type | VARCHAR |  |

**Table 6.** *Users Table*

Students Table:

The students table stores information about the students, including student\_id, name, course, year\_level, and academic\_status if he is a graduate, undergraduate or ILS student, all of which are fully dependent on the student\_rfid\_uid primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| student\_rfid\_uid | BIGINT | Primary Key(PK) |
| student\_id | BIGINT |  |
| name | VARCHAR |  |
| course | VARCHAR |  |
| year\_level | VARCHAR |  |
| academic\_status | VARCHAR |  |

**Table 7.** *Students Table*

Car Owners Table:

The carowners table stores information about the car owners, including owner\_id, name, contact\_number, plate\_number, vehicle\_type, vehicle\_color, all of which are fully dependent on the owner\_id primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| owner\_id | INT | Primary Key(PK) |
| name | VARCHAR |  |
| contact\_number | BIGINT |  |
| plate\_number | VARCHAR |  |
| vehicle\_type | VARCHAR |  |
| vehicle\_color | VARCHAR |  |

**Table 8.** *Car Owners Table*

Guardians Table:

The guardians table stores information about the guardian of the student with the student\_rfid\_uid as foreign key referencing the student in the students table to link who is the guardian of the student including the name and contact\_number. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| guardian\_id | INT | Primary key(PK) |
| name | VARCHAR |  |
| student\_rfid\_uid | BIGINT | Foreign Key(FK) |
| contact\_number | BIGINT |  |

**Table 9.** *Guardians Table*

Events Table:

The event table stores information about the events, including event\_id, event\_name, event\_date, event\_start and event\_end, with reader\_id as the foreign key referencing the reader\_id in the rfidreaders table all of which are fully dependent on the event\_id primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| event\_id | INT | Primary Key(PK) |
| reader\_id | INT | Foreign Key(FK) |
| event\_name | VARCHAR |  |
| event\_date | DATE |  |
| event\_start | TIMESTAMP |  |
| event\_end | TIMESTAMP |  |

**Table 10.** *Events Table*

Rfidreaders Table:

The rfidreaders table stores information about RFID readers, including reader\_id, location\_name and mac\_address, all of which are fully dependent on the event\_id primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| reader\_id | INT | Primary Key(PK) |
| location\_name | VARCHAR |  |
| mac\_address | VARCHAR |  |

**Table 11.** *Rfidreaders Table*

Studentlogrecords Table:

The studentlogrecords table stores information about the student logs when entering the university, including log\_id, time\_in and time\_out, with rfid\_uid as the foreign key referencing the rfid\_uid in the students table and reader\_id referencing the reader\_id in the rfidreaders table, all of which are fully dependent on the log\_id primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| log\_id | INT | Primary Key(PK) |
| rfid\_uid | BIGINT | Foreign Key(FK) |
| reader\_id | INT | Foreign Key(FK) |
| time\_in | TIMESTAMP |  |
| time\_out | TIMESTAMP |  |

**Table 12.** *Studentlogrecords Table*

Carlogrecords Table:

The carlogrecords table stores information about the car logs when entering the university, including log\_id, time\_in and time\_out, with owner\_uid as the foreign key referencing the owner\_uid in the carowners table all of which are fully dependent on the log\_id primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| log\_id | INT | Primary Key(PK) |
| owner\_uid | BIGINT | Foreign Key(FK) |
| time\_in | TIMESTAMP |  |
| time\_out | TIMESTAMP |  |

**Table 13.** *Carlogrecords Table*

Eventlogrecords Table:

The eventlogrecords table stores information about the event logs, including log\_id, time\_in and time\_out, with event\_id as the foreign key referencing the event\_id in the events table and rfid\_uid referencing the rfid\_uid in the students table all of which are fully dependent on the log\_id primary key. This table is in 3NF due to the absence of transitive dependencies among its non-key attributes.

|  |  |  |
| --- | --- | --- |
| **Column** | **Data Type** | **Constraints** |
| log\_id | INT | Primary Key(PK) |
| event\_id | INT | Foreign Key(FK) |
| rfid\_uid | BIGINT | Foreign Key(FK) |
| time\_in | TIMESTAMP |  |
| time\_out | TIMESTAMP |  |

**Table 14.** *Eventlogrecords Table*

Use-Case Diagram

A use case diagram is an overview of the interactions between a system and its users can be found in a UML use case diagram (Educative, n.d.). The easy-to-understand use case diagram will highlight the key interactions and functionalities of the system with the users, making it accessible for readers of all backgrounds.

A diagram of a person's identification

Description automatically generated

**Figure 11.** *Proposed System Use-Case Diagram*

**Description of the Prototype**

The prototype for the integration of contactless RFID-based student and vehicle access control and attendance logging system for a Philippine State University comprises a comprehensive arrangement of hardware components specially made to enhance campus operations. According to the University of Massachusetts Amherst's Information Technology department, recommended and minimum computer configurations for students are designed to ensure compatibility and optimal performance in the UMass Amherst computing environment (UMass Amherst IT, 2024). The specifications include a 10th generation Intel Core i3 processor or higher, a minimum of 4 GB of RAM, and either a Solid-State Drive (SSD) or Hard Disk Drive (HDD) with a capacity of at least 500 GB, all running on a 64-bit version of Windows 10. This setup guarantees the smooth operation of the system software and database management, critical for effective campus management.

RFID technology forms the backbone of the access control and attendance logging system. UHF RFID stickers operating within the frequency range of 860-960MHz are attached to student ID cards for precise identification and tracking. UHF RFID readers with a reading frequency range of 915-928MHz and a maximum reading distance of 180mm will be strategically placed across campus entry points to scan student ID cards, facilitating access control and recording attendance.

In addition to student access control and attendance logging, the system integrates UHF RFID stickers attached to registered vehicles within the campus. These stickers, operating within the same frequency range as student ID cards, enable identification and tracking of vehicles, enhancing campus security and traffic management. To further boost campus security, a UHF Long Range RFID reader with a reading frequency range of 902-928MHz and a maximum reading range of 10 meters will be deployed at strategic locations. This reader scans for RFID tags embedded within vehicles, ensuring authorized access and enhancing overall campus safety and efficiency.

This comprehensive hardware setup ensures the efficient integration of contactless RFID-based student and vehicle access control and attendance logging system, addressing the unique operational needs of a Philippine State University. By surrounding access control, attendance logging, and vehicle tracking functionalities, the prototype aims to smoothen campus operations and enhance overall campus safety and efficiency.

**Implementation Plan**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module** | **Specific Objective/s** | **Hardware Requirements** | **Software Requirements** | **Duration** | **Person Involved** | **Estimated Budget** | **Risk Assessment and Mitigation** | **Evaluation and Monitoring** |
| Project Scope Definition | Define project objectives, deliverables, timelines, and budget constraints. | None | None | 1 week | Project Manager, Stakeholders | ₱0 | Scope creep, Lack of stakeholder engagement | Regular progress meetings, Stakeholder feedback |
| Requirements Analysis | Gather and analyze functional and non-functional requirements to ensure the system meets university needs. | RFID readers, Tags | Requirements gathering tools | 2 weeks | Project Manager | ₱0 | Incomplete or inaccurate requirements | Requirement validation, Stakeholder review |
| System Design | Design system architecture, database schema, user interface, and technical components based on requirements. | Server, RFID readers, Tags, Networking equipment | Design tools  Development IDE | 3 weeks | System Architect, Developers | ₱16,000 | Incompatible hardware or software | Design review, Prototyping |
| Hardware Procurement and Setup | Procure necessary hardware components and set up infrastructure, including installation and configuration. | RFID readers, Tags, Server, Networking equipment | None | 2 weeks | IT Technician | ₱0 | Delays in procurement or installation | Procurement tracking, Installation testing |
| Software Development | Develop application software for access control, attendance logging, and other required functionalities. | Server, RFID readers, Tags | Programming languages | 6 weeks | Software Developers, QA Analysts | ₱0 | Software bugs or errors | Code review, Testing |
| Testing and Quality Assurance | Conduct comprehensive testing (unit, integration, system, user acceptance) to ensure system functionality and performance. | RFID readers, Tags, Server | Testing tools | 4 weeks | QA Analysts, Developers | ₱0 | Undetected defects or performance issues | Test coverage analysis, User acceptance testing |
| Training and Documentation | Provide user and administrator training and document system functionality, configuration, and maintenance procedures. | RFID readers, Tags | Documentation tools | 2 weeks | Trainers, Technical Writers | ₱0 | Inadequate training or documentation | Training feedback, Documentation review |
| Pilot Deployment and Evaluation | Deploy system in a pilot environment, gather feedback, and make necessary adjustments or improvements. | RFID readers, Tags, Server, Networking equipment | None | 4 weeks | Project Manager, IT Technician | ₱0 | Pilot environment issues (e.g., hardware failure) | User feedback, Pilot evaluation |
| Full-Scale Deployment | Deploy system across entire campus or designated areas, finalize configurations, conduct final testing, and transition to full-scale operation. | RFID readers, Tags, Server, Networking equipment | None | 8 weeks | Project Manager, IT Team | ₱0 | Disruption to campus operations | Rollout plan, Post-deployment support |
| Maintenance and Support | Provide ongoing maintenance, troubleshooting, updates, patches, and user support to ensure system functionality and efficiency. | RFID readers, Tags, Server, Networking equipment | Maintenance tools (e.g., monitoring software) | Ongoing | IT Support Team | ₱0 | Downtime due to maintenance activities | Regular maintenance schedule, User support channels |

**Table 15.** *Proposed Implementation Plan*

**Ethical Considerations**

Informed Consent

Informed consent is a foundational principle in the implementation of the RFID-Based Student and Vehicle Access Control and Attendance Logging System. It entails ensuring that all individuals whose data is collected or utilized within the system fully understand the purpose, functionalities, and potential implications of the technology. Users must be provided with transparent information about how their data will be used, stored, and protected. Before participating in any data collection processes or utilizing the system's services, individuals should be given the opportunity to provide explicit consent based on their understanding of the associated risks and benefits. Informed consent empowers users to make autonomous decisions regarding their involvement with the RFID-based system and promotes respect for their privacy and autonomy rights.

Privacy and Confidentiality

Supporting privacy and confidentiality is of great importance in implementing the RFID-Based Student and Vehicle Access Control and Attendance Logging System. All data collected, including the university population information, must be securely stored and accessed only for its intended purpose. Measures should be in place to safeguard individuals' privacy rights and ensure that their confidential information is not exposed or misused. Access to sensitive data should be restricted to authorized personnel, and encryption techniques should be utilized to protect data during transmission and storage.

Autonomy Respect

Respecting the autonomy of users involves providing transparent information about the RFID-based system and allowing individuals to make informed choices regarding their participation. Users should be informed about the purpose and functionalities of the system, as well as any options available for choosing not to participate on certain data collection processes. Respecting autonomy also requires obtaining direct consent from users before collecting or using their personal data for any purpose beyond what is necessary for university’s security.

Beneficence and Non-maleficence

The implementation of the RFID-Based Student and Vehicle Access Control and Attendance Logging System should prioritize the well-being of users. It should aim to enhance campus operations without causing harm or discomfort to individuals. Steps should be taken to minimize any potential negative impacts on users' experiences within the university, and measures should be in place to address any unpleasant effects that may arise as a result of the system's implementation. Additionally, the system should be regularly evaluated to ensure that it continues to serve its intended purpose without causing harm.

Use of Deception

Deception should be avoided in all aspects of implementing and communicating the RFID-Based Student and Vehicle Access Control and Attendance Logging System. Users should be provided with accurate and transparent information about the system, including its purpose, functionalities, and potential implications. Any attempts to deceive or mislead users about the system's capabilities or intentions threaten trust and may result in ethical concerns. Transparency and honesty in communication are essential to maintain integrity and sustain ethical standards throughout the implementation process.

Conflict of Interest

It is essential to identify and address any potential conflicts of interest that may arise during the implementation of the RFID-based system. Decisions should be made based on the best interests of the university and its users rather than personal or organizational gain. Transparency and accountability are crucial in reducing conflicts of interest, and measures should be in place to ensure that decision-making processes are fair, unbiased, and free from inappropriate influence.

Data Manipulation

Integrity in data collection, storage, and analysis processes is vital to maintaining ethical standards in the implementation of the RFID-Based Student and Vehicle Access Control and Attendance Logging System. Data should be accurately recorded and interpreted without manipulation or bias. Any attempts to manipulate data threaten the reliability and validity of the system's outcomes and may lead to ethical concerns. Transparency in data handling and sticking to established protocols for data management are essential to sustain integrity and trustworthiness.

Intellectual Property

Respecting intellectual property rights is crucial when developing and implementing the RFID-based system. Proper permissions and acknowledgments should be obtained for any use of existing technologies, methodologies, or literature. Unauthorized use or reproduction of intellectual property may violate upon the rights of others and result in ethical and legal consequences. Respecting intellectual property ensures fairness in the development and utilization of the RFID-based system.

Cultural Sensitivity

Cultural differences and sensitivities should be considered throughout the implementation of the RFID-Based Student and Vehicle Access Control and Attendance Logging System. The technology and its associated processes should be designed and implemented in a manner that is respectful and inclusive of diverse perspectives and backgrounds. Cultural sensitivities may impact how users perceive and interact with the system, and efforts should be made to accommodate varying cultural norms and preferences. By prioritizing cultural sensitivity, the system can better serve the needs of all users and promote inclusivity and equity.

Continuing Monitoring and Reflection

Continuous monitoring and reflection are essential aspects of maintaining ethical conduct throughout the implementation of the RFID-Based Student and Vehicle Access Control and Attendance Logging System. Regular evaluations should be conducted to assess the system's impact on users and identify any ethical concerns that may arise. Reflection on the ethical implications of system implementation allows for ongoing adjustments and improvements to ensure that ethical principles are verified. By actively monitoring and reflecting on the system's performance, ethical considerations can be addressed actively, promoting accountability and integrity in campus operations.

**References**

Acasamoso, D., Jr, Avila, E., & Vargas, S. (2021). Development And Acceptability of

a Student Daily Attendance Monitoring System. Conference: 2021 IEEE 13th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM). <https://doi.org/10.1109/HNICEM54116.2021.973196>

Ali, U., Idris, M. Y. I., Ayub, M. N., Ullah, I., Ihsan, A., Nandy, T., Yahuza,

M., & Khan, N. (2021). RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption. IEEE Journals & Magazine | IEEE Xplore. <https://doi.org/10.1109/ACCESS.2021.3069429>

Awotunde, J. B., Sur, S. N., Aderinto, M. T., & Gaber, T. (2023). RFID-Based Student

Identification Card Attendance Monitoring System. In Lecture notes in electrical engineering (pp. 31–41). <https://doi.org/10.1007/978-981-99-1983-3_4>

Batouty, A. S. E., Farag, H. H., Mokhtar, A., El-Badawy, E. A., & Aly, M. H. (2020).

Improvement of radio frequency identification security using new hybrid Advanced Encryption Standard Substitution box by Chaotic Maps. Electronics, 9(7), 1168. <https://doi.org/10.3390/electronics9071168>

Biag, C. a. C. (2021). Electronic Cartero Machine (ECM): an RFID-Based One-Way

SMS-Sending kiosk. Animo Repository. <https://animorepository.dlsu.edu.ph/conf_shsrescon/2021/paper_csr/3/>

Canlas, J. R., Punsalang, K. K., Galura, E., Herrera, L., & Medina, J. R. (Eds.). (2022).

Re:SCN: A Web–based Report Management System with RFID–Based Vehicle Monitoring for Villa Belen. Proceedings of the International Conference on Industrial Engineering and Operations Management. <https://ieomsociety.org/proceedings/2022istanbul/381.pdf>

Context diagrams. (n.d.-d).

https://www.cs.uct.ac.za/mit\_notes/software/htmls/ch06s06.html

Corpuz, B. S. G. F. T. (2023). Development of a Class Attendance Monitoring System

Using Barcode with SMS Notification. sifisheriessciences.com. <https://doi.org/10.17762/sfs.v10i1S.717>

De Leon, R., Sison, A. M., & Medina, R. (2019). A modified tiny encryption algorithm

using key rotation to enhance data security for internet of things. IEEE Conference Publication | IEEE Xplore. <https://doi.org/10.1109/ICOIACT46704.2019.8938456>

Dichoso, W. L., Gonzaga, M., Erlano, S., Guevarra, K., Lasam, S. G., & Ronquillo, N.

L. (2022). IMPLEMENTATION OF RFID-BASED AUTOMATED PARKING MANAGEMENT SYSTEM: A FEASIBILITY STUDY. Barometer, 7(2), 119–129. <https://doi.org/10.35261/barometer.v7i2.6764>

D. Antonio, M. C., P. Alicaway, L., & N. Lardizabal, E. (2019). CAMS: CVCITC

ATTENDANCE MONITORING SYSTEM. Journal of Technology, Business Education and Interdisciplinary Studies, 2. <https://cvcitc.edu.ph/wp-content/uploads/2021/10/1-CAMS-CVCITC-ATTENDANCE-MONITORING-SYSTEM-1.pdf>

Educative. (n.d.-b). What are database schemas? 5 minute guide with examples.

<https://www.educative.io/blog/what-are-database-schemas-examples>

Galora, H. M. S. C. (2023). Safeguarding Filipiniana materials: recognizing and

prioritizing risks in transporting, moving or relocating library, archives, and museum collections. University Library at a New Stage of Social Communications Development, 8, 62–78. <https://doi.org/10.15802/unilib/2023_293480>

Kumar, S., Banka, H., & Kaushik, B. N. (2024). Lightweight group authentication

Protocol for secure RFID system. Multimedia Tools and Applications. <https://doi.org/10.1007/s11042-024-19013-1>

Maulidzart, A. V. T., Harahap, R. K., Sukowati, A. I., Nur’ainingsih, D., & Widyastuti,

W. (2023). The hybrid cryptographic algorithms for secure RFID data protection in the internet of things. Jurnal ELTIKOM : Jurnal Teknik Elektro, Teknologi Informasi Dan Komputer, 7(2), 160–169. <https://doi.org/10.31961/eltikom.v7i2.860>

Nueva, C. H., Tapic, F. M. J., Pineda, I. T., Melendrez, J. K. T., Jimena, P. C., &

Alquiza, R. J. (2022). RFID-Based Student Attendance Monitoring System with SMS Notification Using Arduino for Bestlink College of the Philippines: Vol.3, No.1A. <https://www.ojs.aaresearchindex.com/index.php/aasgbcpjmra/article/view/12810>

Origines, D., Sison, A. M., & Medina, R. P. (2019). A Secured RFID Lightweight

Authentication Protocol based on Elliptic Curve Cryptography using modified PRNG Algorithm. ICCBD 2019: Proceedings of the 2nd International Conference on Computing and Big Data. <https://doi.org/10.1145/3366650.3366664>

Raguro, M. C. F., Lagman, A. C., & Juanatas, R. (2021). Technology Management

Framework for Smart University System in the Philippines. ICIT ’21: Proceedings of the 2021 9th International Conference on Information Technology: IoT and Smart City. <https://doi.org/10.1145/3512576.3512642>

Singh, N., & Mahajan, P. (2014). RFID and it’s use in libraries: a literature review.

ResearchGate. <https://www.researchgate.net/publication/272575963_RFID_and_It%27s_Use_in_Libraries_A_Literature_Review>

Solanke, D. (2021a). RFID TECHNOLOGY IN LIBRARIES. International Journal of

Research(IJR), 8(12), 90–97. <https://www.researchgate.net/publication/356986252_RFID_TECHNOLOGY_IN_LIBRARIES>

Sunico, R. J. A., Argana, E. S., & Dumale, M. M. (2020). Development and Evaluation

of Automated Gate Pass System. International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 8846–8850. <https://doi.org/10.30534/ijatcse/2020/279952020>

UMASS Amherst Information Technology | UMASS Amherst. (2024).

<https://www.umass.edu/it/>

Wolff, J. (2021). How is technology changing the world, and how should the world

change technology? Global Perspectives, 2(1). <https://doi.org/10.1525/gp.2021.27353>

Non, J. D. A., Flores, K. M. C., Otadoy, C. S. K., Rodas, J., Tabaco, J. F., ̃Nera, J. D.

C., & Macapagal, A. J. (2020). Classroom Attendance Monitoring System Using Radio Frequency Identification with Web Application. Research Briefs on Information & Communication Technology Evolution, 6, 108–128. <https://doi.org/10.56801/rebicte.v6i.110>