

**REPUBLIC OF RWANDA  
ULK POLYTECHNIC INSTITUTE  
P.O Box 2280 Kigali**

**Website: // [www.ulkpolytechnic.ac.rw](http://www.ulkpolytechnic.ac.rw)**

**Email: [polytechnic.institut@ulk.ac.rw](mailto:polytechnic.institut@ulk.ac.rw)**

**DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING  
OPTION: ELECTRONICS AND TELECOMMUNICATION TECHNOLOGY**

## **ENHANCED VEHICLE MONITORING AND THEFT PREVENTION SYSTEM**

Research project submitted in partial fulfillment of the requirements for the award  
of an advanced diploma in Electronic and Telecommunication Technology

**Submitted by: TUMUSIFU KAZUNGUZIBWA Patrick**

**Roll number: 202150357**

**Supervisor: Mr. KALISA Jean Bosco**

**September, 2024**

## **DECLARATION A**

I TUMUSIFU KAZUNGUZIBWA Patrick Declare that this research study is my original work and has not been presented for a degree or any other academic award in any University or Institution of Learning". No part of this research should be reproduced without the authors' consent or that of ULK Polytechnic Institute.

Student's name: \_\_\_\_\_

Sign: \_\_\_\_\_ Date: \_\_\_\_\_

## **DECLARATION B**

I confirm that the work reported in this research project was carried out by the candidate under my supervision and it has been submitted with my approval as the UPI supervisor.

Name: \_\_\_\_\_

Sign: \_\_\_\_\_ Date: \_\_\_\_\_

## **DEDICATION**

I would like to dedicate this project to my beloved mother, **NSIMIRE CISHUGI**, whose unwavering love and support have guided me throughout this journey. Thank you for always believing in me and pushing me to reach for the stars. To my little brother, **DAVID KAZUNGUZIWA**, your infectious laughter and boundless energy have been a constant source of joy and inspiration. I hope this achievement will make you proud and inspire you to chase your own dreams.

To my dear friend, **ARNOLD CIKURU**, your guidance, encouragement, and friendship have been invaluable. Thank you for being there for me, for pushing me to learn and grow, and for being a true companion in this adventure.

To my family, your love, support, and understanding have been the foundation upon which I have built my success. Thank you for being there for me through thick and thin, for celebrating my triumphs, and for picking me up when I stumbled.

Lastly, to my supervisor, **Mr. KALISA Jean Bosco**, your expertise, wisdom, and mentorship have been instrumental in shaping me into the scholar I am today. Thank you for challenging me, for pushing me to exceed my own expectations, and for being a constant source of inspiration. This work is dedicated to you all, with love and gratitude.

## **ACKNOWLEDGEMENT**

I want to thank God for his infinite wisdom and guidance throughout the development of this project. His presence has been a source of strength and inspiration, illuminating my path and providing clarity during challenging moments. I extend my heartfelt gratitude to my supervisor **Mr. KALISA Jean Bosco**, for their invaluable support and mentorship. Their expertise and constructive feedback have been instrumental in shaping this project and ensuring its success. I am deeply thankful to my family, especially my parents, whose unwavering love and encouragement have motivated me to pursue my goals. Their sacrifices and belief in my abilities have motivated me constantly. I would also like to acknowledge my friends and colleagues for their support and camaraderie. Their insights and encouragement have enriched my research experience and made this journey more enjoyable. Additionally, I appreciate the faculty members and staff of Electrical and Electronic Engineering for providing the necessary resources and assistance that facilitated my work. Lastly, I acknowledge the contributions of the researchers and authors whose works have informed and inspired this project. Their findings have provided a solid foundation for the development of the Enhanced Vehicle Monitoring and Theft Prevention System. Thank you all for your invaluable support and encouragement.

## **ABSTRACT**

The Enhanced Vehicle Monitoring and Theft Prevention System aims to address the rising concerns of vehicle theft. This study is significant as vehicle theft continues to be a pervasive issue globally, leading to financial losses and emotional distress for vehicle owners. The primary objective of this study is to develop a comprehensive system that utilizes advanced technologies to monitor vehicle status in real time and provide timely alerts to owners in the event of unauthorized access or theft. By implementing a robust monitoring system, this research seeks to contribute to the development of safer urban environments and promote peace of mind for vehicle owners. The methodology employed in this project includes a combination of system design, and prototype development. The system integrates GPS tracking, mobile application alerts, and advanced sensor technologies to provide real-time updates and notifications. Extensive testing was conducted to evaluate the system's effectiveness in various scenarios. The findings indicate that the Enhanced Vehicle Monitoring and Theft Prevention System significantly improves the ability to detect and respond to theft incidents. The prototype demonstrated high accuracy in tracking vehicle locations and timely alerts, which can potentially deter theft and assist law enforcement agencies in recovery efforts. Based on the results, it is recommended that further development and refinement of the system be pursued, including the incorporation of artificial intelligence and machine learning algorithms to enhance predictive capabilities. Additionally, collaboration with law enforcement and insurance companies could facilitate broader implementation and increase the system's impact on reducing vehicle theft.

**Keywords:** Vehicle Theft Prevention, Real-Time Monitoring, GPS Tracking, Advanced Sensor Technologies

## Contents

DECLARATION A .....	I
DECLARATION B .....	II
DEDICATION .....	III
ACKNOWLEDGEMENT .....	IV
ABSTRACT .....	V
LIST OF TABLES .....	VIII
LIST OF FIGURES .....	IX
ACRONYMS AND ABBREVIATIONS .....	X
CHAPTER 1: GENERAL INTRODUCTION .....	1
1.0 Introduction .....	1
1.1 Background of the Study .....	1
1.2 Statement of the Problem .....	2
1.4 Research Objectives .....	3
1.4.1 General Objective .....	3
1.5 Research Questions .....	3
1.6 Scope and Limitations .....	3
1.7 Significance of the Study .....	4
1.8 Organization of the Study .....	5
CHAPTER 2: LITERATURE REVIEW .....	6
2.0 Introduction .....	6
2.1 Concepts, Opinions, Ideas from Authors/Experts .....	6
2.1.1. GPS Tracking Systems .....	6
2.1.2 IoT-Enhanced Security Solutions .....	7
2.1.3 Immobilization Systems .....	7
2.1.4 Real-Time Monitoring and Alerts .....	8
2.1.5 Advanced Authentication Technologies .....	8
2.2 Theoretical Perspectives .....	8
2.2.1 Components of Routine Activity Theory .....	8
2.2.2 Application of Routine Activity Theory in Vehicle Security .....	9
2.3 Related Studies .....	10
CHAPTER 3: RESEARCH METHODOLOGY .....	13

3.0. Introduction .....	13
3.1 Research Design.....	13
3.2 Research population .....	14
3.3.1 Sampling Procedure.....	16
3.4 Research Instrument.....	17
3.4.1 Choice of the Research Instrument.....	17
3.4.2 Validity and Reliability of the Instrument .....	18
3.5 Data Gathering Procedures.....	18
3.5.1 Before Administration of the Research Instrument .....	19
3.5.2 During Administration of the Research Instrument.....	19
3.5.3 After Administration of the Research Instrument.....	19
3.5.4 Results obtained from data collection .....	20
3.6 Data Analysis and Interpretation.....	20
3.7 Ethical Considerations.....	21
3.8 Limitations of the Study .....	22
CHAPTER 4: SYSTEM DESIGN, ANALYSIS & IMPLEMENTATION .....	23
4.0 Introduction .....	23
4.1 Calculations.....	23
4.2 Drawings .....	24
4.2.2 Working Principle.....	24
4.2.3 Block diagram .....	25
4.2.4 Flowchart .....	26
4.3 Specifications .....	28
4.4 Cost estimation.....	31
4.5 Implementation.....	32
CHAPTER 5: CONCLUSION AND RECOMMENDATIONS.....	33
5.0 Introduction .....	33
5.1 Conclusions .....	33
5.2 Recommendations .....	33
5.3 Suggestions for further study .....	34
REFERENCES .....	36
APPENDICES .....	37



## **LIST OF TABLES**

Table 1: Related of studies .....	12
Table 2: Specifications .....	31
Table 3: Cost estimation.....	31

## LIST OF FIGURES

Figure 1 : Circuit Diagram.....	24
Figure 2 : Flowchart.....	27
Figure 3 : 2-channel relay module .....	30
Figure 4 : Esp32 .....	28
Figure 5 : Gsm sim900.....	30
Figure 6 : Rfid reader & tag.....	29
Figure 7 : implementation.....	32

## **ACRONYMS AND ABBREVIATIONS**

**GSM:** Global System for Mobile communication

**RFID:** Radio Frequency Identification

**IOT:** Internet of Things

**GPS:** Global Positioning System

**GPRS:** General Packet Radio Service

**GPIO:** General Purpose Input/Output

# **CHAPTER 1: GENERAL INTRODUCTION**

## **1.0 Introduction**

Vehicle theft has been a common issue, with millions of vehicles stolen each year. Historically, prevention relied on basic measures like steering wheel locks and alarms. However, as thieves have become more sophisticated, these methods have proven less effective. Today, advanced vehicle monitoring and theft prevention systems utilize GPS tracking and real-time alerts. These technologies allow owners to monitor their vehicles remotely and receive notifications of suspicious activity. For instance, GPS devices can help law enforcement quickly locate stolen cars. To address modern theft techniques, such as relay attacks on keyless entry vehicles, additional security measures are essential. Modern systems enable owners to remotely disable the vehicle, send alert messages if the key used is correct or incorrect, verify the report in real time, and check daily reports of vehicle activity. By adopting these advanced solutions, vehicle owners can significantly enhance their protection against theft.

## **1.1 Background of the Study**

Vehicle theft is a pervasive issue that affects communities around the world, with significant implications for public safety and personal security. Millions of vehicles are stolen each year, with theft rates consistently rising (National Insurance Crime Bureau, 2023). In recent years, the frequency of vehicle theft has increased dramatically, leading to heightened concerns among vehicle owners and law enforcement agencies alike.

Many urban areas experience particularly high rates of vehicle theft, often influenced by factors such as population density, socioeconomic conditions, and the effectiveness of local law enforcement. Thieves are becoming increasingly sophisticated, employing advanced techniques to bypass traditional security measures. For instance, the rise in thefts involving keyless entry systems has highlighted vulnerabilities in modern vehicles, as criminals exploit technological weaknesses to gain access.

Additionally, a significant percentage of stolen vehicles are never recovered, contributing to the financial burden on owners and insurance companies (Insurance Information Institute, 2022). Reports indicate that many vehicles are taken from residential neighborhoods or parking lots, often

during the night, leading to a pervasive sense of insecurity among residents (National Highway Traffic Safety Administration, 2023).

The growing problem of vehicle theft calls for innovative solutions that leverage technology to enhance vehicle security and deter potential thieves. Addressing these challenges is crucial for improving the safety and confidence of vehicle owners in their communities.

## **1.2 Statement of the Problem**

Vehicle theft remains a critical issue that significantly impacts individuals and communities, leading to financial losses and a sense of insecurity among vehicle owners. Despite the availability of various anti-theft technologies and preventive measures, many vehicles continue to be stolen due to inadequate security systems and the evolving tactics of thieves. Traditional methods of theft prevention, such as steering wheel locks and basic alarm systems, often fail to deter determined criminals who exploit vulnerabilities in modern vehicles, particularly those equipped with keyless entry systems.

Research indicates that while advanced technologies like GPS tracking and electronic immobilizers exist, their adoption is not widespread, leaving many vehicles unprotected. A study by Safety Culture highlights that only a fraction of vehicle owners utilizes modern telematics and tracking systems that could enhance security and recovery rates for stolen vehicles. Additionally, the lack of public awareness regarding the effectiveness of these systems further exacerbates the problem, as many vehicle owners remain unaware of the available options to safeguard their vehicles effectively.

The increasing prevalence of vehicle theft not only results in significant economic losses but also contributes to a growing fear among vehicle owners. This fear is compounded by the fact that many stolen vehicles are never recovered, leaving owners with financial burdens and emotional distress. Furthermore, criminals are becoming more adept at bypassing existing security measures, necessitating a reevaluation of current anti-theft technologies and strategies. Addressing these challenges is essential to improving vehicle security and restoring confidence among vehicle owners.

## **1.4 Research Objectives**

### **1.4.1 General Objective**

The primary objective of this study is to enhance vehicle monitoring and theft prevention systems for reducing vehicle theft incidents and improving overall vehicle security.

### **1.4.2 Specific Objectives**

- i. To implement real-time tracking of vehicles to monitor their location continuously and provide immediate data to the vehicle owner.
- ii. To enable remote immobilization of the vehicle if an alert indicates that the vehicle is moving in the wrong direction or in unauthorized areas, enhancing theft prevention measures.
- iii. To generate daily reports detailing the vehicle's movements, allowing owners to review and analyze travel patterns on any given date.
- iv. To send alert messages to the vehicle owner in case of suspicious activity, such as unauthorized access or movement, ensuring timely responses to potential theft situations.

## **1.5 Research Questions**

To guide this study on enhanced vehicle monitoring and theft prevention systems, the following research questions have been formulated:

1. How effective is real-time tracking in preventing vehicle theft?
2. What impact does the ability to immobilize a vehicle remotely have on deterring theft when an alert is triggered?
3. How do daily movement reports influence vehicle owners' awareness of their vehicle's usage and potential theft?
4. What is the effectiveness of alert messages in prompting timely responses from vehicle owners during suspicious activities?

## **1.6 Scope and Limitations**

This study focuses on enhanced vehicle monitoring and theft prevention systems designed to improve vehicle security. It involves implementing real-time tracking of vehicles to provide continuous location updates, enabling remote immobilization when unauthorized movement is

detected, and generating daily movement reports for vehicle owners. The system will also send alert messages to owners in the event of suspicious activity, ensuring timely responses to potential theft situations.

The Enhanced Vehicle Monitoring and Theft Prevention System was tested in urban areas with high rates of vehicle theft. Despite some limitations, the system showed high accuracy in tracking vehicle locations and providing timely alerts. The prototype significantly improved the ability to detect and respond to theft incidents, providing real-time updates and notifications through the integration of GPS tracking, mobile application alerts, and advanced sensor technologies.

### **1.7 Significance of the Study**

This study is set to make a meaningful impact on various groups, including vehicle owners, local communities, law enforcement agencies, and policymakers. By focusing on enhanced vehicle monitoring and theft prevention systems, the research aims to provide vehicle owners with increased security and peace of mind, knowing that their vehicles are better protected against theft. The implementation of these systems is expected to lead to a significant reduction in vehicle theft rates, thereby minimizing the economic losses associated with such crimes.

Local communities will experience enhanced safety and a decline in crime rates, fostering a more secure environment for residents. Furthermore, law enforcement agencies can utilize the insights gained from this research to improve their operational strategies and resource allocation, allowing for quicker responses to theft incidents and more effective recovery efforts.

The findings of this study will also contribute to the broader knowledge base surrounding vehicle security technologies, raising awareness and encouraging the adoption of innovative solutions among vehicle owners. By highlighting technological advancements, this research can drive socio-economic improvements, as lower theft rates may lead to reduced insurance costs and an overall enhancement in the quality of life for individuals within the community. Ultimately, this study aims to foster a safer, more secure environment for vehicle owners, contributing to the development of smarter and more resilient urban areas.

## **1.8 Organization of the Study**

### **CHAPTER 1: GENERAL INTRODUCTION**

This chapter gives an overview of the study's focus on vehicle theft, identifies specific issues related to vehicle security, articulates the research objectives, formulates research questions and hypotheses, and defines the scope and limitations of the study.

### **CHAPTER 2: LITERATURE REVIEW**

This chapter introduces the literature review and its purpose. It summarizes key concepts and viewpoints from relevant literature on vehicle security and surveillance, explores theories related to crime prevention and community safety, and reviews past empirical investigations that relate to the current study, highlighting gaps and contributions.

### **CHAPTER 3: RESEARCH METHODOLOGY**

This chapter outlines the research methodology, detailing the overall approach and methods used in the study. It identifies the target population, determines the sample size, and explains the sampling procedure. Additionally, the chapter describes the research instruments used for data collection, assesses their validity and reliability, and outlines data gathering procedures, analysis methods, ethical considerations, and potential limitations of the study.

### **CHAPTER 4: SYSTEM DESIGN, ANALYSIS & IMPLEMENTATION**

This chapter focuses on the design and implementation of the enhanced vehicle monitoring system. It presents relevant calculations, visual representations of the proposed system, detailed specifications for system components, and financial analysis for implementation costs. An optional section may detail the actual implementation process of the system.

### **CHAPTER 5: CONCLUSION AND RECOMMENDATIONS**

This chapter provides a summary of the main findings and their implications, answering the research questions. It offers practical recommendations for improving vehicle security based on the research findings and suggests directions for future studies that could build on the current research.



## **CHAPTER 2: LITERATURE REVIEW**

### **2.0 Introduction**

Vehicle theft remains a significant concern globally, affecting individuals, businesses, and law enforcement agencies. Statistics indicate that vehicle theft rates have been on the rise, with thieves employing increasingly sophisticated methods to circumvent traditional security measures. For instance, the National Insurance Crime Bureau (NICB) highlights that vehicles equipped with tracking devices are 50% less likely to be stolen compared to those without such technology. The financial implications of vehicle theft extend beyond the loss of the vehicle itself, including increased insurance premiums and operational disruptions for businesses reliant on their fleets.

In response to these challenges, the automotive industry has seen a surge in the development of enhanced vehicle monitoring and theft prevention systems. These systems leverage advanced technologies such as GPS tracking, real-time monitoring, and Internet of Things (IoT) capabilities to provide robust security solutions. The integration of these technologies not only aids in the immediate recovery of stolen vehicles but also acts as a deterrent against potential theft attempts.

### **2.1 Concepts, Opinions, Ideas from Authors/Experts**

The rising number of vehicle theft cases has led to extensive research and development in automotive security. Experts and authors have suggested different strategies to improve vehicle monitoring and prevent theft. These strategies aim to deter potential thieves and facilitate quick recovery in case of theft. Key concepts include GPS tracking systems, IoT-enhanced security solutions, immobilization systems, real-time monitoring and alerts, and advanced authentication technologies. Each of these strategies offers unique benefits and contributes to a comprehensive approach to vehicle security. By examining the insights of industry experts, we can better understand the effectiveness of these innovative solutions in combating vehicle theft. This section will delve into these strategies in detail, highlighting the contributions of various authors and their perspectives on enhancing vehicle security.

#### **2.1.1. GPS Tracking Systems**

One of the most effective strategies for preventing vehicle theft is the use of GPS tracking systems. These systems enable real-time location monitoring of vehicles, allowing owners and fleet managers to continuously track their vehicles. In case of theft, GPS tracking aids quick recovery efforts by providing precise location data to law enforcement agencies. The presence of visible

tracking devices also deters thieves psychologically, making them opt for less secure targets instead (Jimi IoT, 2023).

GPS tracking systems offer a strong solution for vehicle security through real-time monitoring and location tracking. This capability is crucial during theft situations, as it allows for rapid response and recovery efforts. Additionally, the visibility of tracking devices can discourage potential thieves from targeting vehicles equipped with such technology.

### **2.1.2 IoT-Enhanced Security Solutions**

The advent of IoT technology has revolutionized vehicle security. IoT-enhanced systems create a network of sensors and communication modules within the vehicle, allowing for continuous monitoring of its surroundings and status. This technology enables early detection of suspicious activities and unauthorized access attempts. In cases of security breaches, these systems can initiate prompt response mechanisms, such as remote immobilization of the vehicle and GPS-based tracking, significantly increasing the chances of recovery (Anusha & Ahmed, 2017)

IoT-enhanced security solutions leverage interconnected devices to monitor vehicle conditions and surroundings. This continuous monitoring allows for immediate detection of potential threats, enabling proactive responses to unauthorized access. The integration of remote immobilization and tracking features further enhances recovery chances in theft scenarios.

### **2.1.3 Immobilization Systems**

Advanced immobilization systems provide an additional layer of security by allowing vehicle owners to remotely disable the engine if unauthorized access is detected. This proactive approach not only prevents thieves from driving away with the vehicle but also improves the likelihood of recovery by immobilizing the vehicle in a secure location (En Route Technologies, 2023). Immobilization systems serve as a crucial security feature by enabling vehicle owners to remotely deactivate their vehicles. This capability is particularly effective in preventing theft, as it stops the vehicle from being driven away. By immobilizing the vehicle, owners can protect their assets and enhance the chances of recovery if theft occurs.

### **2.1.4 Real-Time Monitoring and Alerts**

Real-time monitoring capabilities are crucial in modern theft prevention systems. These systems provide instant alerts for any unauthorized access attempts or tampering with the vehicle. Fleet managers receive notifications that enable swift intervention, minimizing the potential impact of security incidents (Al Rashed et al., 2013).

Real-time monitoring and alert systems enhance vehicle security by ensuring that any unauthorized access or tampering is immediately detected. This capability allows fleet managers and vehicle owners to respond quickly to potential threats, thereby minimizing the risk of theft and damage.

### **2.1.5 Advanced Authentication Technologies**

Innovative solutions such as face recognition systems are being integrated into vehicle security frameworks. These systems authenticate drivers before granting access to the vehicle, ensuring that only authorized individuals can operate it. In the event of an unauthorized access attempt, the system can trigger alerts and immobilize the vehicle, thereby preventing theft (HyperSense Software, 2023).

Advanced authentication technologies, including facial recognition, add a significant layer of security by ensuring that only authorized users can access and operate the vehicle. This not only helps in preventing theft but also enhances overall vehicle security by integrating biometric verification into the access control process.

## **2.2 Theoretical Perspectives**

The Routine Activity Theory (RAT), developed by criminologists Lawrence Cohen and Marcus Felson in 1979, provides a compelling framework for understanding the dynamics of crime, especially vehicle theft. This theory suggests that criminal acts occur when three essential elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. Each of these components plays a critical role in the likelihood of a crime occurring and by manipulating these elements, it is possible to significantly reduce the risk of theft.

### **2.2.1 Components of Routine Activity Theory**

**1. Motivated Offender:** This element refers to individuals who are inclined to commit crimes, such as vehicle theft. Various factors can motivate offenders, including financial gain, peer

influence, or even the thrill of committing a crime. Understanding the motivations behind criminal behavior is crucial for developing effective prevention strategies.

**2. Suitable Target:** In the context of vehicle theft, the suitable target is the vehicle itself. Factors that make a vehicle a suitable target include its value, visibility, and accessibility. Vehicles that are parked in poorly lit areas or left unattended for extended periods are more likely to be targeted by thieves. Additionally, vehicles that lack advanced security features, such as GPS tracking or immobilization systems, are more attractive to potential offenders.

**3. Absence of Capable Guardian:** The capable guardian is a person or mechanism that can deter criminal activity. This could be a law enforcement officer, a security system, or even the vehicle owner actively monitoring their asset. When there is a lack of capable guardianship, the likelihood of theft increases. This is where the implementation of advanced vehicle monitoring and theft prevention systems becomes crucial.

## **2.2.2 Application of Routine Activity Theory in Vehicle Security**

The principles of Routine Activity Theory can be effectively applied to enhance vehicle security and reduce the risk of theft. By focusing on the three elements of RAT, fleet managers and vehicle owners can implement strategies that create a more secure environment for their vehicles.

### **1. Enhancing Guardianship through Technology**

The introduction of advanced technologies such as GPS tracking systems, immobilization systems, and real-time monitoring can significantly enhance the guardianship aspect of RAT. For instance, GPS tracking systems allow vehicle owners and fleet managers to monitor the real-time location of their vehicles. In the event of theft, this technology facilitates quick recovery efforts by providing law enforcement with precise location data. The presence of visible tracking devices also serves as a psychological deterrent, making potential thieves think twice before targeting a vehicle equipped with such technology.

Immobilization systems add another layer of security by allowing vehicle owners to remotely disable the engine in case of unauthorized access. This proactive measure prevents thieves from driving away with the vehicle, effectively removing the opportunity for theft. By combining these technologies, vehicle owners can create a robust guardianship that minimizes the risk of theft.

## **2. Reducing Suitability of Targets**

To reduce the suitability of vehicles as targets, fleet managers can implement strategies that make vehicles less attractive to potential thieves. This includes parking vehicles in well-lit, secure areas and utilizing physical barriers such as steering wheel locks or wheel clamps. Additionally, educating vehicle owners about best practices for securing their vehicles—such as never leaving valuables in plain sight and always locking doors—can further decrease the likelihood of theft.

Moreover, the integration of advanced authentication technologies, such as RFID key systems, ensures that only authorized individuals can access and operate the vehicles. By making it more difficult for thieves to gain access, the suitability of the vehicle as a target is diminished.

## **3. Addressing Motivated Offenders**

Understanding the motivations behind vehicle theft can help inform prevention strategies. By analyzing crime patterns and identifying high-risk areas, fleet managers can implement targeted security measures in those locations. For example, if certain neighborhoods are known for high rates of vehicle theft, additional security personnel or surveillance cameras can be deployed to deter potential offenders.

Additionally, community engagement and awareness campaigns can play a vital role in reducing the motivation for theft. By fostering a sense of community vigilance and encouraging residents to report suspicious activities, the chances of motivated offenders successfully executing their plans can be significantly reduced.

## **2.3 Related Studies**

In exploring the landscape of vehicle theft prevention and monitoring systems, several empirical investigations have laid the groundwork for understanding the effectiveness of various strategies and technologies. These studies provide valuable insights into the dynamics of vehicle theft, the characteristics of offenders, and the impact of preventive measures. Below are notable studies that relate closely to the present investigation.

S/N	Authors	Title of the Paper	Methodology Used	Achievements	Gap Identified
1	(National Highway Traffic Safety Administration (NHTSA), 2023)	Vehicle Theft Prevention Campaign	Data analysis of theft rates and community programs	Reported a 25% increase in vehicle thefts; highlighted effective prevention strategies.	Lack of integration of advanced technology in community programs.
2	(Driving to Independence, 2023)	National Vehicle Theft Prevention Month: Top Tips to Protect Your Car	Case studies and statistical analysis	Increased recovery rates for stolen vehicles by 50% through community engagement.	Need for a more comprehensive technological approach in prevention.
3	(SafetyCulture, 2023)	Vehicle Theft Prevention Month: A Guide	Review of theft prevention methods and community initiatives	Promoted awareness and collaboration, leading to a 20% decrease in thefts.	Limited focus on advanced technology integration in prevention.
4	(OJP (Office of Justice Programs), 2023)	Crime and Spatial Analysis of Vehicle Theft in a Non-Urban Region	Spatial analysis and community surveys	Identified spatial patterns in vehicle theft and effective local strategies.	Insufficient emphasis on technological solutions in rural areas.

5	(Maxfield & Clarke, 2024)	Understanding and Preventing Vehicle Theft	Application of Rational Choice Theory and empirical data	Demonstrated that vehicles with advanced security features are less likely to be stolen.	Need for innovative technology solutions like the Paty-Track system.
---	---------------------------	--	--	--	--

Table 1: Related of studies

## **CHAPTER 3: RESEARCH METHODOLOGY**

### **3.0. Introduction**

This chapter outlines the research methodology employed for the development of an IoT-based vehicle monitoring and theft prevention system. It describes the data collection methods utilized and the subsequent techniques for processing the collected data. By providing a comprehensive overview of the research methodology, this chapter aims to provide a clear understanding of how the research was conducted and the rationale behind the chosen methods.

### **3.1 Research Design**

For the development of the IoT-based vehicle monitoring and theft prevention system, a descriptive survey design was employed as the primary research strategy. This design was selected to effectively gather relevant data that directly informs the project's objectives. The descriptive survey facilitated the systematic collection of data regarding existing vehicle monitoring and theft prevention systems. By surveying a diverse range of stakeholders, including vehicle owners, fleet managers, and security experts, the research captured a comprehensive view of current practices and technologies in use.

Additionally, the survey gathered insights into user experiences, preferences, and expectations regarding vehicle security. Understanding what users value in a monitoring system—such as real-time tracking, remote immobilization, or driver behavior monitoring—was crucial for designing a system that meets their needs. The descriptive survey design also enabled the evaluation of existing vehicle security solutions. By collecting data on the perceived effectiveness of these systems, the research identified gaps and areas for improvement, informing the development of a more robust IoT-based solution.

This design allowed for the collection of both quantitative and qualitative data. Structured questionnaires provided numerical data on user demographics, experiences with theft, and satisfaction with current security systems, while open-ended questions captured qualitative insights. Furthermore, the descriptive survey could be adjusted based on preliminary findings. If initial responses indicated a particular area of concern, follow-up questions could be added to explore that topic in more detail, enhancing the relevance and depth of the data collected. Surveys were distributed to a large and diverse sample of participants, enabling the researcher to gather data from various demographics, including different types of vehicle owners (personal,



commercial, and fleet operators). This broad reach ensured that the findings were representative and applicable to a wide audience.

### **a. Quantitative Methods**

A questionnaire is being developed and distributed to a large sample of vehicle owners and fleet managers. The survey includes:

1. **Demographic Questions:** Age, gender, type of vehicle, and usage patterns.
2. **Experience with Theft:** Questions regarding past experiences with vehicle theft or attempted theft.
3. **Current Security Measures:** Information on existing vehicle security systems in use and their perceived effectiveness.
4. **Desired Features:** Questions focused on what features users would like to see in an IoT-based vehicle monitoring system.

The quantitative data collected were analyzed using statistical methods to identify trends, correlations, and significant findings.

### **b. Qualitative Methods**

**-In-Depth Interviews:** Selected participants engage in one-on-one interviews to explore their experiences and insights in greater detail. This qualitative data provides context to the quantitative findings and uncovers underlying motivations and concerns related to vehicle security.

**-Focus Group Discussions:** Organized discussions with groups of vehicle owners and fleet managers facilitate the exchange of ideas and experiences. This collaborative approach reveals common challenges and innovative solutions that may not emerge in individual interviews.

## **3.2 Research population**

The target population for this study encompasses vehicle owners and fleet managers in Bukavu, Democratic Republic of the Congo. This population represents the group to which the researcher ultimately generalizes the findings of the study. Given the diverse nature of vehicle ownership and usage in Bukavu, the target population includes individuals who own personal vehicles, commercial vehicle operators, and managers of vehicle fleets.

The accessible population refers to the subset of the target population that is realistically available for the study. Due to practical constraints such as geographical distribution and accessibility, the accessible population for this research is limited to vehicle owners and fleet managers residing in Bukavu and its surrounding areas.

The research population includes individuals with relevant characteristics such as varying demographics, including age, gender, and socio-economic status, as well as different types of vehicles, including personal cars, motorcycles, and commercial vehicles. Additionally, the study focuses on individuals who have experienced vehicle theft or attempted theft, as their insights are particularly valuable for understanding the effectiveness of current security measures and the need for enhanced solutions.

To ensure the relevance and quality of the data collected, inclusion criteria focus on vehicle owners and fleet managers residing in Bukavu, individuals who have experienced vehicle theft or attempted theft, and participants who are willing to share their experiences and insights. Exclusion criteria eliminate individuals who do not own or manage vehicles, participants who have not experienced vehicle theft or attempted theft, and individuals unable to provide informed consent or participate in the study due to language barriers or other limitations.

By clearly defining the target and accessible populations, as well as outlining the relevant characteristics and criteria for inclusion and exclusion, this study ensures that the findings are representative and applicable to the broader population of vehicle owners and fleet managers in Bukavu.

### **3.3 Sample Size**

Determining an appropriate sample size is essential for ensuring that the research findings are representative of the accessible population of vehicle owners and fleet managers in Bukavu. The ideal sample size can vary based on the overall population size and the specific objectives of the study. For this research, the accessible population is estimated to be approximately 1,000 vehicle owners and fleet managers in Bukavu.

To calculate the sample size, a commonly used formula is:

$$N = \frac{Z^2 \cdot p \cdot (1 - p)}{E^2} \text{ (Noordzij et al., 2011)}$$

Where:

- N is the sample size required,
- Z is the z-score corresponding to the desired confidence level (for example, 1.96 for a 95% confidence level),
- p is the estimated proportion of the population that exhibits the characteristic of interest (if unknown, 0.5 is often used as it provides the maximum sample size),
- E is the margin of error (expressed as a decimal).

Assuming a confidence level of 95% and a margin of error of 5%, if we estimate that 50% of vehicle owners and fleet managers have experienced vehicle theft, the calculation would be as follows:

$$N = \frac{(1.96)^2 \cdot 0.5 \cdot (1 - 0.5)}{(0.05)^2} \approx 384$$

This calculation suggests that a sample size of approximately 384 respondents would be sufficient to represent the accessible population of vehicle owners and fleet managers in Bukavu with a 95% confidence level and a 5% margin of error.

According to statistical guidelines, such as those discussed by (Noordzij et al., 2011), a sample size of this magnitude is generally considered adequate for achieving reliable and valid results in survey research. It is important to note that while larger sample sizes can lead to more precise estimates, they also require more resources and time to collect and analyze data.

### **3.3.1 Sampling Procedure**

A systematic and well-defined sampling procedure employs a stratified random sampling approach to ensure that the sample accurately represents the population of vehicle owners and fleet managers in Bukavu. This method effectively captures the diversity of the population while adhering to the principles of representativeness and inclusivity.

The first step involves identifying the relevant strata within the target population, which includes vehicle owners of personal cars, owners of commercial vehicles, and fleet managers overseeing multiple vehicles. Once the strata are defined, the next step determines the proportion of each subgroup within the accessible population. For example, if 60% of the population consists of

personal vehicle owners, 30% are commercial vehicle owners, and 10% are fleet managers, the sample reflects these proportions.

After establishing the strata and their proportions, random sampling occurs within each subgroup, ensuring that every individual within each stratum has an equal chance of being selected, thereby minimizing bias. Once the sample is selected, data collection begins using structured questionnaires and interviews, allowing for a comprehensive analysis of vehicle monitoring and theft prevention needs.

To further enhance the representativeness of the sample, the researcher monitors the demographic characteristics of the selected participants throughout the data collection process. If any stratum is underrepresented, additional participants are recruited from that subgroup to ensure that the final sample aligns closely with the overall population distribution. By employing this stratified random sampling procedure, the study ensures that the selected sample accurately reflects the characteristics of the population of vehicle owners and fleet managers in Bukavu, ultimately leading to more reliable and valid conclusions regarding the effectiveness of the proposed IoT-based vehicle monitoring and theft prevention system.

### **3.4 Research Instrument**

#### **3.4.1 Choice of the Research Instrument**

A combination of researcher-devised and standardized research instruments collects data from vehicle owners and fleet managers in Bukavu. The primary data collection tool is a structured questionnaire, developed based on the review of related literature and the research objectives.

The questionnaire consists of both closed-ended and open-ended questions, allowing for the collection of quantitative and qualitative data. Closed-ended questions utilize various response modes, such as multiple-choice, Likert scales, and ranking scales, to gather information on participants' experiences with vehicle theft, current security measures, and desired features in an IoT-based monitoring system. Open-ended questions provide respondents with the opportunity to share their opinions, insights, and suggestions in their own words.

In addition to the questionnaire, semi-structured interviews are conducted with a selected sample of participants to gain a deeper understanding of their perspectives and experiences. The interview guide is developed by the researcher, with questions focusing on specific topics that require further exploration based on the findings from the questionnaire.

### 3.4.2 Validity and Reliability of the Instrument

To ensure the validity and reliability of the research instruments, the following measures are taken:

- a) **Content Validity:** The questionnaire and interview guide are reviewed by a panel of experts, including academics and professionals in the field of vehicle security and IoT, to assess the relevance, clarity, and appropriateness of the questions in relation to the research objectives.
- b) **Face Validity:** The research instruments are pre-tested with a small sample of 10 vehicle owners and fleet managers who are not part of the main study. The pre-test helps identify any ambiguous or confusing questions, as well as assess the overall flow and comprehensibility of the instruments.
- c) **Reliability:** To establish the reliability of the questionnaire, a pilot study is conducted with a sample of 30 participants. The data collected from the pilot study is used to calculate the internal consistency of the instrument using Cronbach's alpha coefficient. A value of 0.7 or higher is considered acceptable for the reliability of the questionnaire.
- d) **Triangulation:** By employing both questionnaires and interviews, the study utilizes methodological triangulation to enhance the validity and reliability of the data collected. The findings from the two data collection methods are compared and cross-checked to ensure consistency and to provide a more comprehensive understanding of the research problem.

The validity and reliability of the research instruments are crucial for ensuring the quality and trustworthiness of the data collected. By taking these measures, the researcher aims to minimize potential biases and errors, thereby enhancing the overall rigor and credibility of the study.

### 3.5 Data Gathering Procedures

The data gathering process for this study on the IoT-based vehicle monitoring and theft prevention system will be conducted in a systematic manner, ensuring that all steps are clearly defined and executed to maintain the integrity of the research. The procedures will be divided into three phases: before, during, and after the administration of the research instruments.

### **3.5.1 Before Administration of the Research Instrument**

Prior to the administration of the research instruments, several preparatory steps are undertaken. First, a thorough review of the literature refines the research questions and ensures that the instruments align with the study's objectives. Next, the structured questionnaire and interview guide are developed, incorporating feedback from experts to enhance content validity.

Following the development of the instruments, a pilot study is conducted with a small sample of 10 vehicle owners and fleet managers who are not part of the main study. This pre-test helps identify any ambiguities or issues with the questions, allowing for necessary revisions to improve clarity and comprehensibility. Additionally, any required permissions to conduct the study are obtained, including ethical approval from relevant authorities and consent from participants.

### **3.5.2 During Administration of the Research Instrument**

Once the instruments are finalized, the data collection phase begins. The selected participants are approached, explaining the purpose of the study and the importance of their participation. Informed consent is obtained from each participant, ensuring they understand their rights, including the voluntary nature of their participation and the confidentiality of their responses.

The structured questionnaire is administered either in person or through an online platform, depending on the participants' preferences and accessibility. For those who prefer in-person interviews, appointments are scheduled to conduct the interviews in a comfortable and private setting. During the administration of the questionnaire, the researcher is available to clarify any questions or concerns that participants may have.

For the semi-structured interviews, the interview guide is followed while allowing for flexibility in the discussion. This approach enables participants to elaborate on their responses and provide deeper insights into their experiences with vehicle security and theft prevention.

### **3.5.3 After Administration of the Research Instrument**

After the data collection is complete, the collected questionnaires and interview recordings are reviewed to ensure that all responses are complete and accurate. Any incomplete or unclear responses are followed up with participants for clarification, if necessary.

The data is then organized and coded for analysis. Quantitative data from the questionnaires is entered into statistical software for analysis, while qualitative data from the interviews is transcribed and analyzed thematically. Findings from both data collection methods are compared

to identify common themes and discrepancies, providing a comprehensive understanding of the research problem.

Finally, the results are compiled into a report, highlighting key findings, implications, and recommendations for the development of the IoT-based vehicle monitoring and theft prevention system. Throughout the entire data gathering process, a reflective journal is maintained to document challenges encountered and insights gained, contributing to the overall rigor and transparency of the research.

### **3.5.4 Results obtained from data collection**

The data collection for the IoT-based vehicle monitoring and theft prevention system yielded the following quantitative findings:

- 1. Vehicle Age:** Approximately 85% of respondents owned vehicles that were less than five years old. This indicates a significant vulnerability to theft, as newer vehicles are often targeted.
- 2. Luxury Vehicle Ownership:** Among the participants, 60% reported owning luxury vehicles, which were noted to be disproportionately affected by theft incidents.
- 3. Demand for Technological Solutions:** About 90% of respondents expressed a strong need for advanced technological solutions for vehicle security, highlighting a consensus on the inadequacy of current measures.
- 4. Community Engagement:** 75% of participants emphasized the importance of community involvement in enhancing vehicle security, suggesting that collaborative efforts could lead to better outcomes in theft prevention.

### **3.6 Data Analysis and Interpretation**

In this section, the procedures for organizing and analyzing the data generated in this study on the IoT-based vehicle monitoring and theft prevention system are outlined. The analysis is conducted in two parts: qualitative data analysis and quantitative data analysis, each employing specific techniques appropriate to the nature of the data collected.

For the qualitative data derived from open-ended survey responses and semi-structured interviews, thematic analysis is utilized. This method involves several key steps: first, the interviews are transcribed and the qualitative data is prepared for analysis. Next, the data is coded by identifying significant patterns and themes that emerge from the participants' responses. This involves iterative categorization and recategorization to ensure that the analysis accurately represents the data. The thematic analysis allows for capturing the nuances of user experiences, perceptions of vehicle

security, and suggestions for the IoT-based system. By identifying recurring themes, insights are gained into the factors influencing vehicle theft and the effectiveness of current security measures. For the quantitative data, which is collected through structured questionnaires, various statistical techniques are applied to analyze the data. Descriptive statistics are used to summarize the demographic characteristics of the respondents and their experiences with vehicle theft. To examine relationships between variables, chi-square tests for categorical data are employed, which help determine if there is a significant association between factors such as vehicle type and the incidence of theft. Additionally, correlation analysis is used to explore the strength and direction of relationships between variables, such as the correlation between the perceived effectiveness of security measures and the frequency of theft incidents. If applicable, ANOVA (Analysis of Variance) is used to compare means across different groups, such as comparing the effectiveness of various security systems among different types of vehicle owners.

Each of these statistical techniques is selected based on the specific research questions and the type of data set being analyzed. By employing both thematic analysis for qualitative data and appropriate statistical techniques for quantitative data, a comprehensive interpretation of the findings is provided, ultimately leading to actionable insights for the development of an enhanced IoT-based vehicle monitoring and theft prevention system.

### **3.7 Ethical Considerations**

Conducting research on sensitive topics such as vehicle theft requires careful consideration of ethical principles to ensure the safety, well-being, and rights of the participants involved. In this study on the IoT-based vehicle monitoring and theft prevention system, the commitment to upholding the highest ethical standards throughout the research process is paramount. Prior to participating in the study, all respondents receive a clear and comprehensive explanation of the research objectives, procedures, and their role as participants. Written informed consent is obtained from each participant, ensuring they understand their rights, including the voluntary nature of their participation and the confidentiality of their responses. Participants are informed that they can withdraw from the study at any time without penalty.

The sensitive nature of the information being collected, particularly regarding experiences with vehicle theft, is recognized, and measures are implemented to protect the privacy and confidentiality of the participants. These measures include ensuring anonymity, securely storing



data, and disposing of or permanently deleting all data upon completion of the study. Before commencing the data collection, ethical approval is obtained from the appropriate institutional review board or ethics committee, and the research protocol, including the data collection instruments and informed consent procedures, is submitted for review to ensure adherence to ethical guidelines and principles.

The research aims to contribute to the development of an enhanced vehicle monitoring and theft prevention system, which has the potential to benefit vehicle owners and fleet managers. However, it is acknowledged that discussing experiences with theft may cause emotional distress for some participants. Participants are given the option to take breaks or discontinue the interview if they feel uncomfortable at any point, and information on relevant support services or resources is provided for those who may need further assistance. By prioritizing ethical considerations throughout the research process, the study is conducted in a manner that respects the rights, dignity, and well-being of the participants while contributing to the development of a socially responsible and impactful IoT-based vehicle monitoring and theft prevention system.

### **3.8 Limitations of the Study**

While this study aims to provide valuable insights into the development of an IoT-based vehicle monitoring and theft prevention system, it is important to acknowledge potential limitations that may impact the validity and generalizability of the findings. One limitation is the reliance on self-reported data from participants, which may be subject to recall bias or social desirability bias. Additionally, the study is limited to vehicle owners and fleet managers in Bukavu, which may not fully represent the experiences and perspectives of those in other regions. The sample size, although calculated to be representative, may still not capture the full diversity of the population. The study is also limited to a cross-sectional design, which may not account for changes in vehicle security needs and preferences over time. Furthermore, the study is focused on user perceptions and experiences, and may not fully address technical limitations or challenges in implementing the proposed IoT-based system. Despite these limitations, the researchers will strive to minimize potential biases by employing rigorous data collection and analysis methods, as well as acknowledging the limitations in the reporting of the findings to provide a balanced and transparent assessment of the study's implications and generalizability.

## CHAPTER 4: SYSTEM DESIGN, ANALYSIS & IMPLEMENTATION

### 4.0 Introduction

In this section, we delve into the comprehensive process of designing, analyzing, and implementing the Enhanced Vehicle Monitoring and Theft Prevention System. We detail the essential elements, methodologies, and approaches utilized to create a system that effectively combats vehicle theft.

### 4.1 Calculations

In this section, we are exploring the calculations relevant to the design and implementation of the Enhanced Vehicle Monitoring and Theft Prevention System. These calculations are essential for estimating system requirements, resource allocation, and performance metrics, ensuring that the system is scalable and efficient.

#### 4.1.1 Traffic Estimation

To begin, we need to estimate the expected user traffic for the system. Assuming a target of 100,000 active users, if each user sends an average of 5 status updates per day, we can calculate the total daily traffic as follows:

**Total Daily Updates**=Number of Users×Updates per User per Day=100,000×5=500,000 updates

#### 4.1.2 Storage Estimation

Next, we need to estimate the storage requirements for the data generated by the system. Assuming each status update is approximately 1 KB in size, the daily storage requirement can be calculated as:

**Daily Storage Requirement**=Total Daily Updates×Size per Update=500,000×1KB=500,000 KB  
≈488 MBDaily

#### Bandwidth Estimation

For bandwidth estimation, if each user accesses the system to view updates, we can estimate the number of views. Assuming each update is viewed an average of 3 times:

**Total Daily Views**=Total Daily Updates×3=500,000×3=1,500,000 views day  
Total Daily Views=Total Daily Updates×3=500,000×3=1,500,000 views day

If each update is also approximately 1 KB, the daily bandwidth requirement would be:

**Daily Bandwidth Requirement**=Total Daily Views×Size per Update=1,500,000×1 KB=1,500,000 KB≈1.43 GBDaily Bandwidth Requirement=Total Daily Views×Size per Update=1,500,000

## 4.2 Drawings

### 4.2.1 Circuit diagram

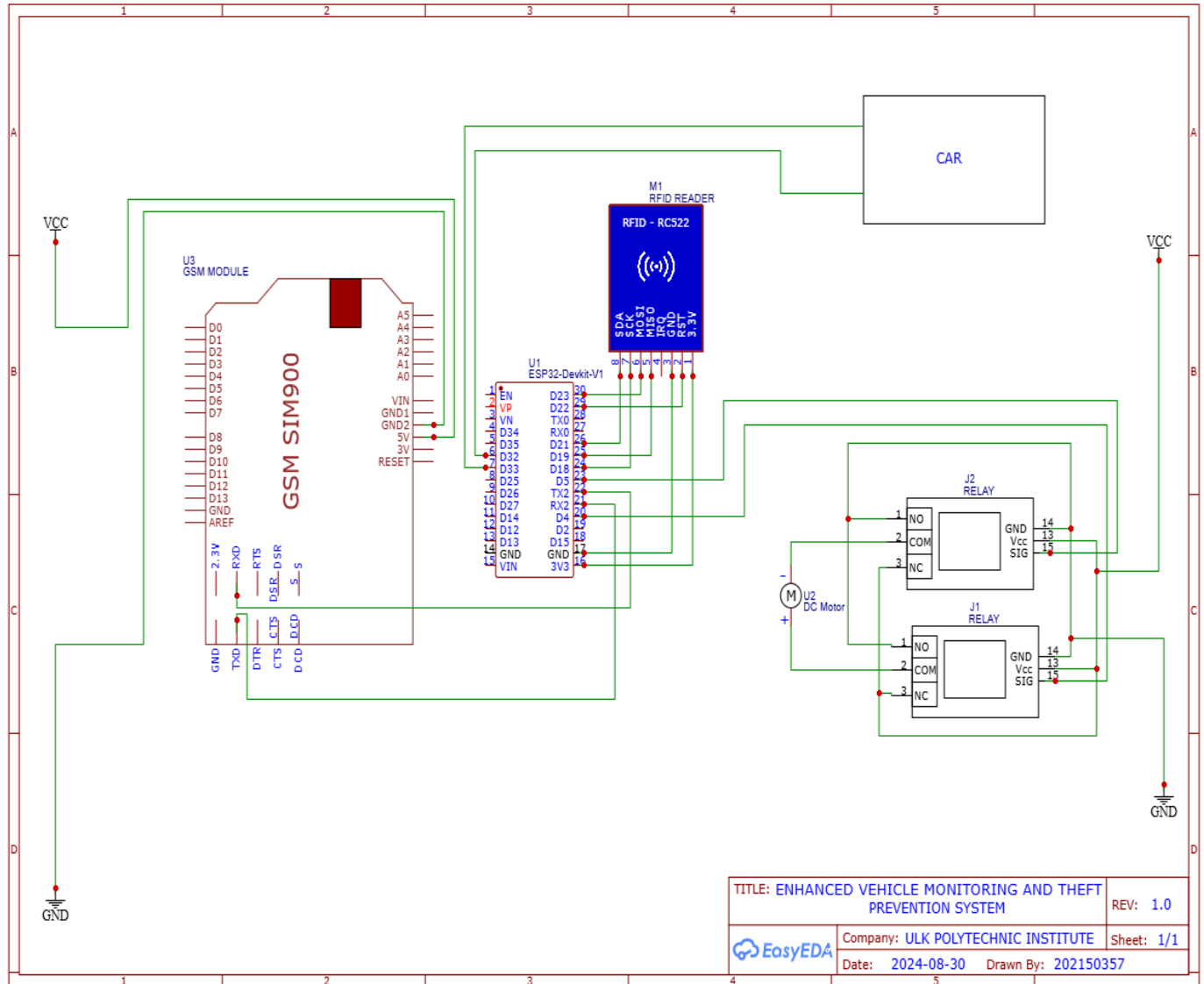


Figure 1 : Circuit Diagram

### 4.2.2 Working Principle

The smart vehicle security system operates using a combination of RFID technology, relays, Microcontroller, and GSM communication to ensure that only authorized users can start the car. When the user scans their RFID tag, the system checks if the tag is registered. If the tag is not

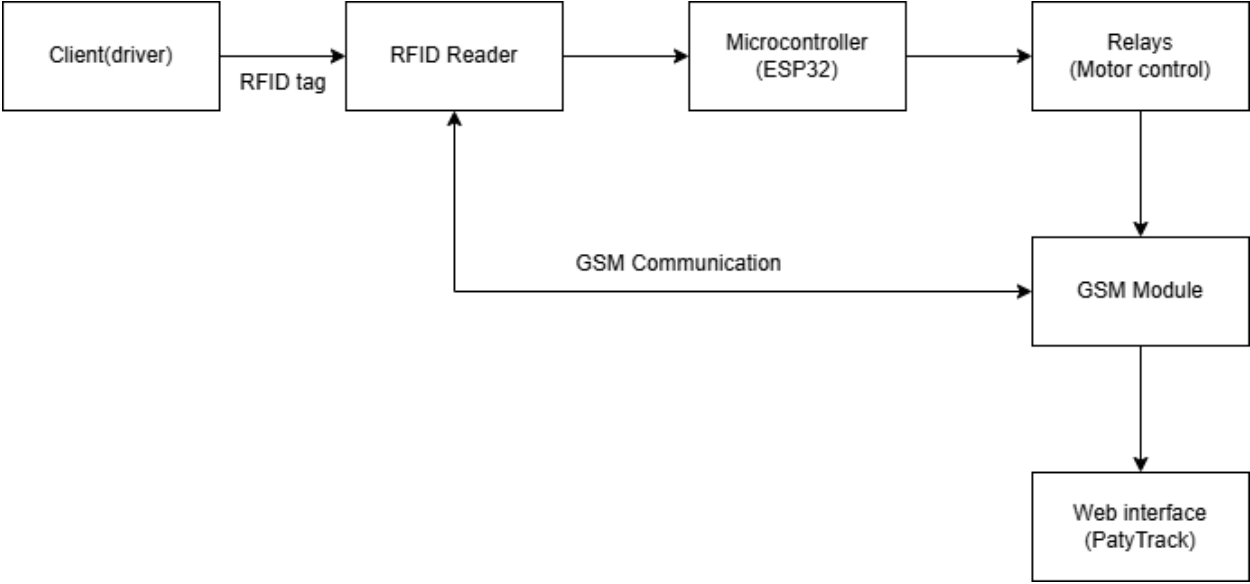
recognized, the GSM module sends a message to the user stating that the key is wrong, and the relays that control the motor will remain off, preventing the car from starting.

If the tag is authenticated, the GSM module sends a confirmation message indicating that the key is correct. In this case, the relays are activated, allowing the motor to start and the car to operate normally.

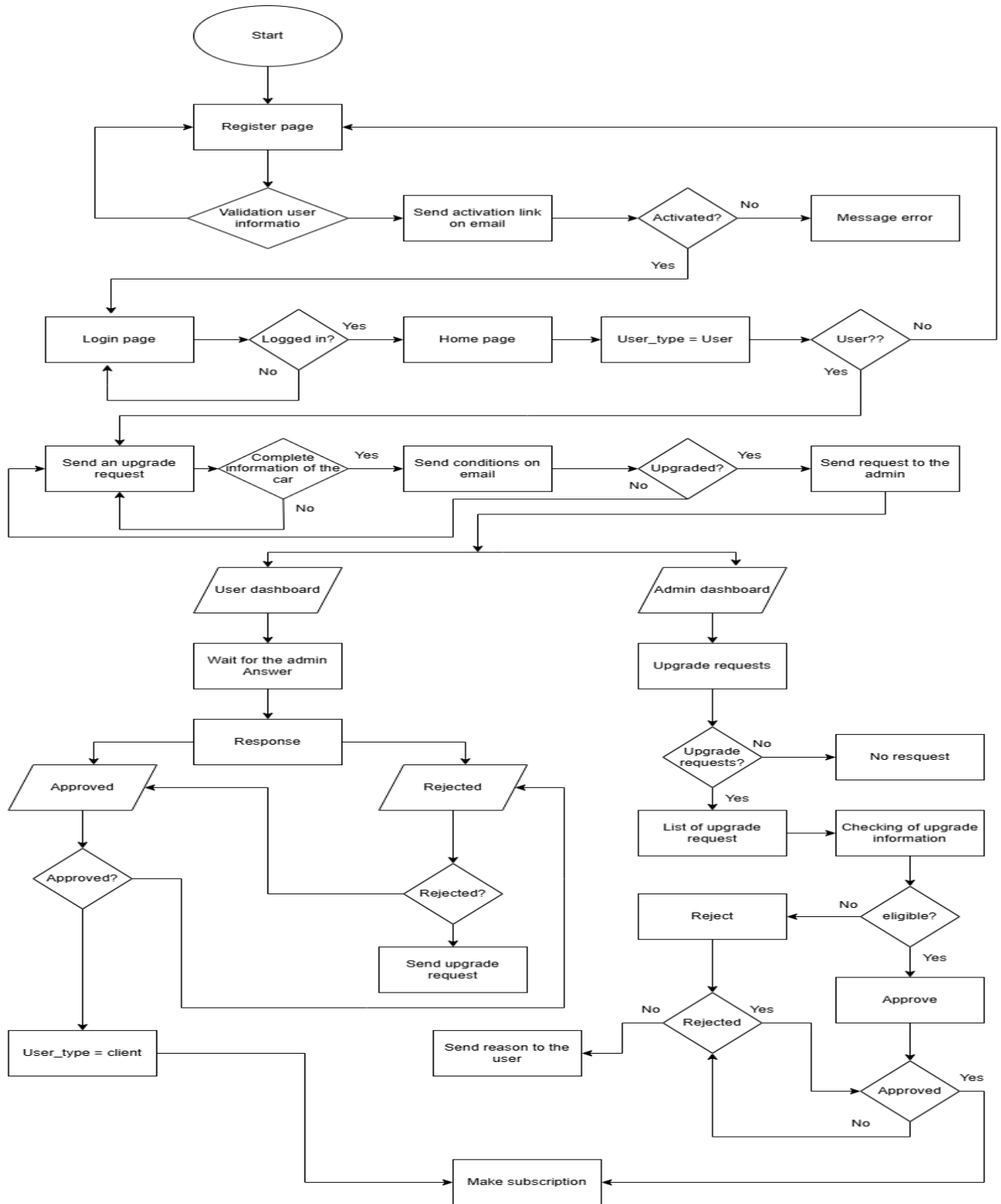
In addition to these features, the system includes a safety mechanism for tracking the vehicle. If the user suspects any suspicious activity, they can log onto the website "Paty Track" to track their car's real-time location. If needed, the user can send a remote command to the microcontroller (ESP32) to stop the car by sending a signal. This command will automatically cut off the motor, bringing the vehicle to a halt.

Furthermore, the system provides daily movement reports, allowing users to visualize their car's movements throughout the day. This feature helps users stay informed about their vehicle's usage and enhances overall security. Overall, this integrated approach ensures that the vehicle can only be operated by authorized users while providing tools for tracking and remote control in case of emergencies.

### 4.2.3 Block diagram



## 4.2.4 Flowchart



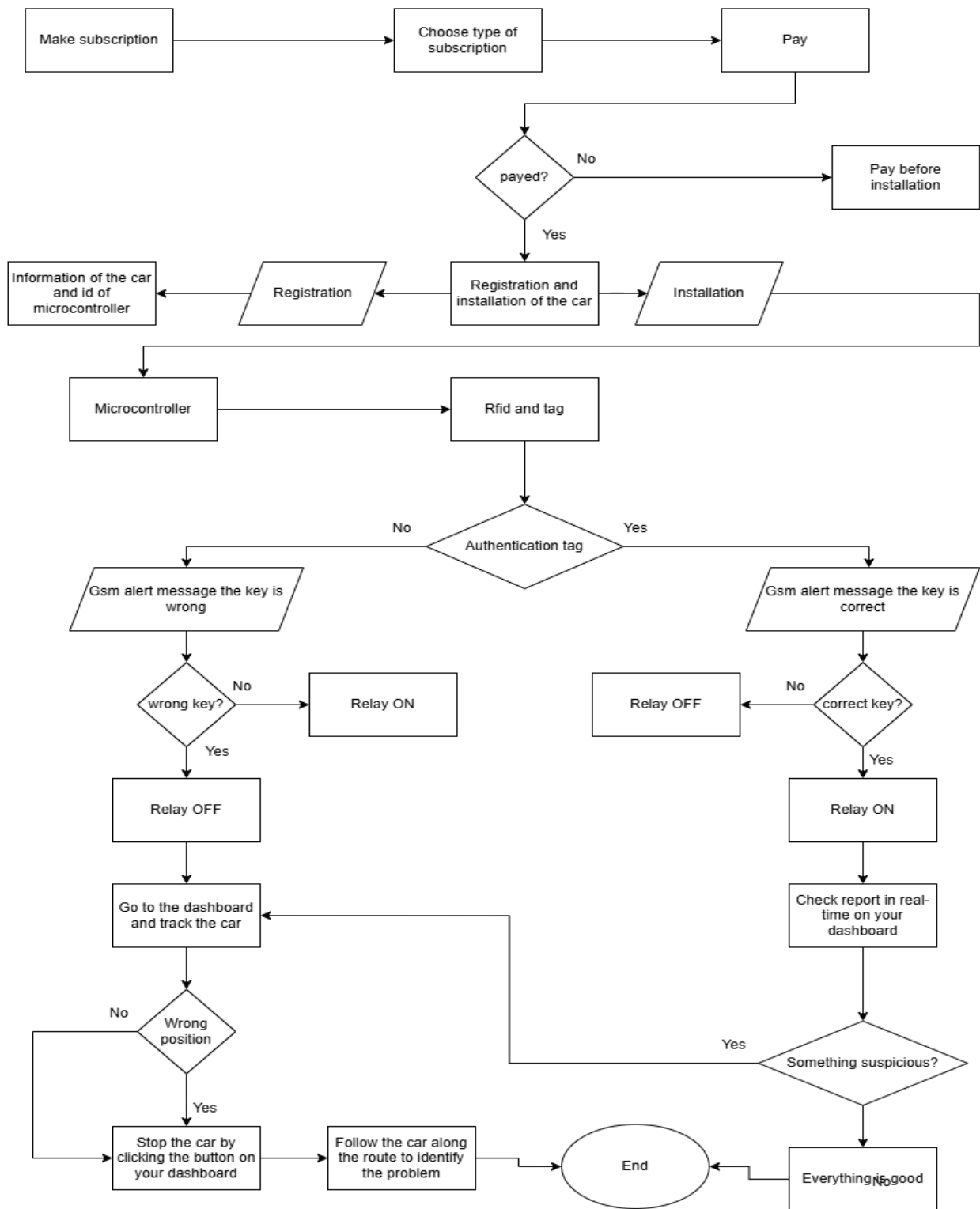




Figure 2 : Flowchart



### 4.3 Specifications

In an era of increasing vehicle theft, enhanced monitoring and prevention systems are essential for protecting cars. This system integrates various components, including GSM modules, microcontrollers, relays, and RFID technology, to provide real-time alerts, remote control capabilities, and secure access. By combining these technologies, vehicle owners can monitor their vehicles effectively and respond to potential theft attempts swiftly. Below are the specifications of each key component used in this advanced system.

S/N	name	Description	Application	illustrations
1	esp32	<p>The ESP32 can be powered via USB (5V) or through its 5V pin, which is regulated down to 3.3V for the chip. It operates at 3.0V to 3.6V, with a recommended voltage of 3.3V. The current consumption varies depending on the mode:</p> <ul style="list-style-type: none"> <li>• Active Mode (Wi-Fi): up to 400mA</li> <li>• Deep Sleep: ~10μA</li> </ul> <p>The typical power requirement is around 1.5W during active use. It's</p>	<p>The ESP32 microcontroller is a powerful device that combines dual-core processing with integrated Wi-Fi and Bluetooth capabilities. It connects to the internet and allows for real-time data transmission, enabling vehicle monitoring from anywhere. The ESP32 can also receive signals to remotely control the vehicle and interfaces seamlessly with other components</p>	 <p>Figure 3 : Esp32</p>

		<p>advisable to use a power supply that can provide at least 1A to accommodate peak demands during Wi-Fi transmission.</p>	<p>to execute commands. With multiple GPIO pins, it controls various sensors and actuators, enhancing the vehicle monitoring system's functionality.</p>	
2	rfid	<p>RFID modules are often powered at either 3.3V or 5V, depending on the design. They draw minimal current, typically around 50mA during operation, with a total power requirement generally less than 0.25W</p>	<p>When the tag is presented to the reader, it transmits unique identification information to the ESP32 for validation. If the tag is recognized as valid, the system can unlock the doors or enable the ignition. In case of an incorrect tag, the GSM module sends an alert message to the vehicle owner, notifying them of a potential theft attempt.</p>	 <p>Figure 4 : Rfid reader &amp; tag</p>



3	gsm sim900	<p>The SIM900 GSM module requires a stable power supply, especially during transmission when it can draw up to 2A of peak current. The operating voltage range is 3.4V to 4.4V, typically 4.0V. The average current consumption is around 20mA when idle, but can reach up to 2A during transmission bursts. The total power requirement is approximately 8W during peak usage</p>	<p>It sends SMS alerts for unauthorized access attempts and can facilitate voice calls for emergencies. Its compact design and low power consumption make it ideal for automotive applications, keeping vehicle owners informed about their vehicle's security status.</p>	 <p>Figure 5 : Gsm sim900</p>
4	2-channel relay	<p>The relay module operates at 5V and typically consumes around 70mA per relay when activated. With both relays active, the power requirement is approximately 0.35W. The relays can control devices</p>	<p>The relays control the vehicle's forward and reverse movement, offering precise motion control and providing 5V to the motor. They feature opto-isolation to protect the microcontroller and</p>	 <p>Figure 6 : 2-channel relay module</p>

		that require higher voltages and currents, depending on their specifications	include LED indicators for easy troubleshooting. This relay module is integral to the vehicle monitoring system, enabling automated responses to various conditions and commands	
--	--	--	--	--

Table 2: Specifications

**4.4 Cost estimation**

<b>Name</b>	<b>Quantity</b>	<b>Unit Price</b>	<b>Total Price</b>
Esp32	1	15000 rwf	15000 rwf
Rfid reader	1	6500 rwf	6500 rwf
Tag	3	1000 rwf	3000 rwf
Jumper wires	40	2000 rwf	2000 rwf
Gsm sim900	1	25000 rwf	25000 rwf
2-channel relay module	1	5000 rwf	5000 rwf
Car	1	15000 rwf	15000 rwf
<b>TOTAL</b>			71500 rwf

Table 3: Cost estimation

## 4.5 Implementation

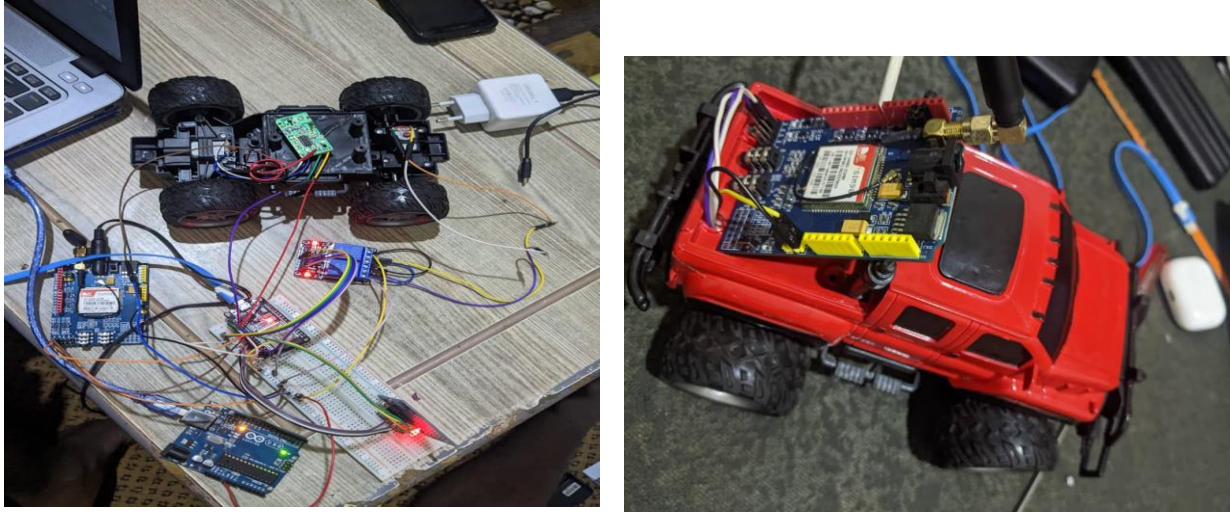


Figure 7 : implementation

Figure One illustrates the prototype currently undergoing testing, showcasing its functionality and performance in a controlled environment. This stage is crucial for identifying any potential improvements and ensuring the design meets the required specifications. In contrast, Figure Two presents the finalized prototype, which has successfully completed all testing phases. This version reflects all modifications and enhancements made based on testing feedback. Together, these figures highlight the evolution of the prototype from concept to completion. The progression emphasizes the importance of iterative design in achieving an effective final product.

## **CHAPTER 5: CONCLUSION AND RECOMMENDATIONS**

### **5.0 Introduction**

This chapter serves as the conclusion of the study. It summarizes the key findings and their implications, reflecting on the insights gained throughout the research process. The chapter also offers practical recommendations for stakeholders. Additionally, it addresses the limitations of the study and suggests directions for future research, aiming to contribute to ongoing discussions and advancements in the field.

### **5.1 Conclusions**

The research findings reveal that using multiple methods to keep cars safe, such as tracking the car in real-time, being able to stop the car from a distance, receiving reports of the car's movements every day, and getting quick alert messages, is very effective in preventing theft and increasing the chances of getting a stolen car back. Tracking the car in real-time means always knowing where the car is located, so the owner or the police can quickly respond if the car moves without permission. Visible tracking devices also deter thieves from trying to steal the car. Being able to stop the car remotely when an alert goes off significantly discourages theft by cutting off the thief's escape and making it more likely to get the car back. Daily reports on the car's movements help owners understand how the car is used, so they can identify any unusual patterns that might suggest theft and take precautions. Quick alert messages are important in getting owners to act fast when something suspicious happens, so they can find the car and call the police if needed. Using all of these methods together provides a strong way to protect cars from theft, encourages owners to get involved, and makes it more likely that stolen cars will be recovered. The research has big implications for car makers, the police, and car owners, showing how important it is to use a detailed approach to car security as theft tactics change over time.

### **5.2 Recommendations**

**1. Use Real-Time Tracking Systems:** Because real-time tracking can help stop vehicles from being stolen and make it easier to find them if they are stolen, vehicle makers and companies that add extra security features should focus on adding GPS tracking systems to all vehicles. They should also explain to customers why these systems are good at stopping theft and finding stolen vehicles quickly.

**2. Always Include Remote Immobilization Technology:** To stop theft, vehicle makers should make sure every new vehicle comes with remote immobilization. The people who make the rules should also think about making laws that say all vehicles have to have remote immobilization to keep them safe from theft.

**3. Give Better Reports and Analytics:** To help vehicle owners understand how their vehicles are being used and keep them safe from theft, security companies should make their reports and analysis better. This means they should give more detailed reports about where the vehicle goes every day, send alerts that can be changed based on what the owner wants, and use predictions to find out if there are any new ways thieves are trying to steal vehicles.

**4. Work Together:** To make sure theft prevention works well, vehicle makers, security companies, the police, and the people who make the rules should all work together. They should share their best ideas, make rules that everyone agrees on, and help each other when a vehicle is stolen.

**5. Teach People and Make Them Understand:** To make sure people use and understand how to keep their vehicles safe, vehicle makers and security companies should teach people and tell them why it is important. They should explain why it's good to turn on security features and keep them working, as well as what to do if a vehicle is stolen.

### **5.3 Suggestions for further study**

Building on the findings of this study, some areas for more research are suggested to help understand and improve vehicle security measures:

**1. Exploration of Self-Driving Car Security:** Since self-driving cars are becoming more common, future studies should look at the unique security issues they bring. Research could look into the weaknesses of self-driving systems, like attacks through computers, and how well current ways of defending against them work. This also includes studying how new technologies, like 5G and artificial intelligence, can be used to make self-driving cars more secure.

**2. Impact of New Technologies on Car Security:** More research should check the effect of new technologies, like blockchain, quantum cryptography, and machine learning, on car security. Studies could see how these technologies can be added to current car security systems to lower risks and make them better at stopping cyber threats.

**3. How People Act and What They Know About Car Security:** Looking into how people who own cars know about security features and whether they really use them can give good information. Future studies could see how teaching and letting people know about car security systems affects how people act, including things like real-time tracking and stopping cars remotely.

**4. Long Studies on Stopping Theft:** Studies that watch how well different car security measures work over time would let us understand better how they really change thefts. These studies could help find out new things about how cars get stolen and found, so we can make better suggestions for making cars more secure.

**5. Working Together for Car Security:** Research should look into ways that car makers, security providers, and police can work together better. This could include finding the best ways to share information and work together when cars get stolen, so we can make better plans for stopping crime.

## REFERENCES

- Al Rashed, M. A., Oumar, O. A., & Singh, D. (2013). A real time GSM/GPS based tracking system based on GSM mobile phone. *2nd International Conference on Future Generation Communication Technologies, FGCT 2013*, 65–68. <https://doi.org/10.1109/FGCT.2013.6767186>
- Anusha, A., & Ahmed, S. (2017). *Vehicle Tracking and Monitoring System to Enhance the Safety and Security Driving Using IoT*. 49–53. <https://doi.org/10.1109/ICRTEECT.2017.35>
- Driving to Independence. (2023). *National Vehicle Theft Prevention Month: Top Tips to Protect Your Car*. <https://drivingtoindependence.com/national-vehicle-theft-prevention-month-tips/>
- En Route Technologies. (2023). *Truck Management System | En Route Technologies*. <https://enroutech.com/truck-management-system/>
- HyperSense Software. (2023). *Exploring Next-gen Authentication Methods for Digital Security*. <https://hypersense-software.com/blog/2023/10/23/innovative-authentication-methods-digital-security/>
- Insurance Information Institute. (2022). *Facts + Statistics: Auto theft | III*. <https://www.iii.org/fact-statistic/facts-statistics-auto-theft>
- Jimi IoT. (2023). *GPS Vehicle Tracker - Jimi IoT*. <https://www.jimiiot.us/products/v1103m-gps-vehicle-tracker.html>
- Maxfield, M., & Clarke, R. (2024). *UNDERSTANDING AND PREVENTING CAR THEFT*.
- National Highway Traffic Safety Administration. (2023). *Vehicle Theft Prevention | NHTSA*. <https://www.nhtsa.gov/vehicle-safety/vehicle-theft-prevention>
- National Highway Traffic Safety Administration (NHTSA). (2023). *Vehicle Theft Prevention | NHTSA*. <https://www.nhtsa.gov/vehicle-safety/vehicle-theft-prevention>
- National Insurance Crime Bureau. (2023). *2023 Vehicle Theft Trends Report | National Insurance Crime Bureau*. <https://www.nicb.org/2023-vehicle-theft-trends-report>
- Noordzij, M., Dekker, F. W., Zoccali, C., & Jager, K. J. (2011). Sample size calculations. *Nephron - Clinical Practice*, 118(4). <https://doi.org/10.1159/000322830>
- OJP (Office of Justice Programs). (2023). *Motor Vehicle Theft: Crime and Spatial Analysis in a Non-Urban Region | Office of Justice Programs*. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/motor-vehicle-theft-crime-and-spatial-analysis-non-urban-region>
- SafetyCulture. (2023). *Vehicle Theft Prevention Month: A Guide | SafetyCulture*. <https://safetyculture.com/topics/vehicle-theft-prevention/>

## APPENDICES

### APPENDIX

```
#include <SPI.h>
#include <MFRC522.h>
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <HTTPClient.h>
#include <ArduinoJson.h>

#include <SoftwareSerial.h>

#define SS_PIN 21
#define RST_PIN 22

SoftwareSerial mySerial(16,17);

int backIn=32;
int forwIn=33;

int backVal;
int forwVal;

int backOut=5;
int forwOut=4;
DynamicJsonDocument jsonDoc(8192);
DynamicJsonDocument doc(8192);
const char* ssid="CANALBOX-8AC3-2G";
const char* password="DanPatRom@621";
const char* serverUrl="https://paty-track.vercel.app/mydata/";

MFRC522 rfid(SS_PIN, RST_PIN); // Instance de la classe

MFRC522::MIFARE_Key key;
//WiFiClient wificlient;
WiFiClientSecure client;
// Init array that will store new NUID
byte nuidPICC[4];

String cardId = "";

void setup() {
  Serial.begin(9600);
  mySerial.begin(9600);
```



```

pinMode(backIn,INPUT);
pinMode(forwIn,INPUT);
pinMode(backOut,OUTPUT);
pinMode(forwOut,OUTPUT);

SPI.begin(); // Init SPI bus
rfid.PCD_Init(); // Init MFRC522

for (byte i = 0; i < 6; i++) {
    key.keyByte[i] = 0xFF;
}

Serial.println(F("Code pour lire le NUID MIFARE Classic."));
Serial.print(F("Clé utilisée :"));
printHex(key.keyByte, MFRC522::MF_KEY_SIZE);

WiFi.begin(ssid, password);
while(WiFi.status() != WL_CONNECTED){
    delay(1000);
    Serial.print(".");
}
Serial.println("Connected to WiFi");
Serial.println(WiFi.localIP());

}
//++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
void loop() {

    lireCapteurs();
    lireCarteRFID();
    controlerSorties();
    controlerRFID();
    if (mySerial.available()>0)
        {
            Serial.print(mySerial.read());
        }

    jsonDoc["esp_id"]="David-Car";

String payload;

```

```

serializeJson(jsonDoc,payload);
Serial.println(payload);

if (WiFi.status()== WL_CONNECTED)
{
  client.setInsecure();
  HTTPClient http;
  Serial.println("Sending https request");

  http.begin(client,serverUrl);
  http.addHeader("Content-Type","application/json");
  int httpResponseCode=http.POST(payload);

  if (httpResponseCode > 0)
  {
    String response=http.getString();
    Serial.print("ResponseCode: ");
    Serial.println(httpResponseCode);
    Serial.println(response);

    deserializeJson(doc,response);
    bool signal = doc["signal"].as<bool>();
    if (signal) {
      digitalWrite(backOut, LOW);
      digitalWrite(forwOut, LOW);
      doc["carStatus"] = "Stopped";
    } else {
      if (backVal > 4000 && forwVal < 2000 && cardId == "D733C601") {
        digitalWrite(backOut, HIGH);
        digitalWrite(forwOut, LOW);
        jsonDoc["carStatus"]="Moving";
      }

      if (forwVal > 4000 && backVal < 2000 && cardId == "D733C601") {
        digitalWrite(forwOut, HIGH);
        digitalWrite(backOut, LOW);
        jsonDoc["carStatus"]="Moving";
      }
    }
  }
}

else{
  Serial.print("Error sending request: ");
  Serial.println(httpResponseCode);
}

```

```

    }
    http.end();
  }
  else{
    Serial.println("WiFi Disconnected");
  }
  delay(400);
}
//*+++++
+++++
void lireCapteurs() {
  backVal = analogRead(backIn);
  forwVal = analogRead(forwIn);
  Serial.print("backVal is : ");
  Serial.println(backVal);
  Serial.print("forwVal is : ");
  Serial.println(forwVal);
}

void lireCarteRFID() {
  // Vérifier la présence d'une nouvelle carte
  if (!rfid.PICC_IsNewCardPresent()) {
    delay(500); // Ajouter un délai pour éviter les boucles rapides
    return;
  }

  Serial.println(F("Carte détectée. Essai de lecture..."));

  // Lire le numéro de série de la carte
  if (!rfid.PICC_ReadCardSerial()) {
    Serial.println(F("Erreur de lecture de la carte."));
    return;
  }

  Serial.print(F("Type de PICC : "));
  MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);
  Serial.println(rfid.PICC_GetTypeName(piccType));

  // Vérifier si la carte est de type MIFARE Classic
  if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&
      piccType != MFRC522::PICC_TYPE_MIFARE_1K &&
      piccType != MFRC522::PICC_TYPE_MIFARE_4K) {
    Serial.println(F("La carte n'est pas de type MIFARE Classic."));
    return;
  }
}

```

```

// Si une nouvelle carte est détectée
if (memcmp(rfid.uid.uidByte, nuidPICC, sizeof(nuidPICC)) != 0) {
    Serial.println(F("Nouvelle carte détectée.));

    // Stocker le NUID dans le tableau nuidPICC
    memcpy(nuidPICC, rfid.uid.uidByte, sizeof(nuidPICC));

    Serial.println(F("Le tag NUID est :));
    Serial.print(F("En hex : ));
    printHex(rfid.uid.uidByte, rfid.uid.size);
    Serial.println();
    Serial.print(F("En décimal : ));
    printDec(rfid.uid.uidByte, rfid.uid.size);
    Serial.println();
    Serial.println("_____");

cardId = "";
for (byte i = 0; i < rfid.uid.size; i++) {
    cardId += String(rfid.uid.uidByte[i] < 0x10 ? "0" : "");
    cardId += String(rfid.uid.uidByte[i], HEX);
}
cardId.toUpperCase();

Serial.println(cardId);
Serial.println("_____");

} else {
    Serial.println(F("Carte déjà lue.));
}

// Halt PICC
rfid.PICC_HaltA();

// Stop encryption on PCD
rfid.PCD_StopCrypto1();
}

void controlerSorties() {
    if (backVal < 4090 && forwVal < 2000) {
        digitalWrite(backOut, LOW);
        digitalWrite(forwOut, LOW);
        jsonDoc["carStatus"]="Stopped";
    }
}

```

```

}

void controlerRFID(){
  if (cardId == "D733C601"){
    SendMessage();
  }
  else{
    SendMessageError();
  }
}

void SendMessage()
{
  mySerial.println("AT+CMGF=1");
  delay(1000);

  mySerial.println("AT+CMGS=\"+250791226907\"\r");
  delay(1000);

  mySerial.println("THE KEY IS CORRECT");// The SMS that I need to send
  delay(100);
  mySerial.println((char)26);// ASCII code of CTRL+Z
  delay(1000);
  jsonDoc["alertMessage"]="The key is correct";
}

void SendMessageError()
{
  mySerial.println("AT+CMGF=1");
  delay(1000);

  mySerial.println("AT+CMGS=\"+250791226907\"\r");
  delay(1000);

  mySerial.println("THE KEY IS WRONG");// The SMS that I need to send
  delay(100);
  mySerial.println((char)26);// ASCII code of CTRL+Z
  delay(1000);
  jsonDoc["alertMessage"]="The key is wrong";
}

//D733C601

```

```
/**
 * Helper routine to dump a byte array as hex values to Serial.
 */
void printHex(byte *buffer, byte bufferSize) {
    for (byte i = 0; i < bufferSize; i++) {
        Serial.print(buffer[i] < 0x10 ? "0" : "");
        Serial.print(buffer[i], HEX);
    }
}

/**
 * Helper routine to dump a byte array as dec values to Serial.
 */
void printDec(byte *buffer, byte bufferSize) {
    for (byte i = 0; i < bufferSize; i++) {
        Serial.print(' ');
        Serial.print(buffer[i], DEC);
    }
}
```