Advanced Anomaly Detection for Commercial Infrastructure Protection

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Modern security systems incorporating AI (Artificial Intelligence) and Deep Learning have transformed the surveillance and security industries, assuring the safety and security of commercial infrastructures. Thanks to AI technologies like Deep Learning algorithms, security systems now include more advanced features such as real-time monitoring, intelligent activity identification, tracking, and anomaly detection. Even though these sophisticated algorithms are making significant contributions, there are still major gaps and unmet difficulties that necessitate innovative solutions. Traditional security procedures, which rely on human monitoring and rule-based systems, usually fail to address growing security threats in commercial infrastructures. There has never been a greater demand for a more sophisticated, adaptive, and proactive security paradigm. This project proposes an innovative approach for increasing business security by integrating cutting-edge Artificial Intelligence (AI) and Deep Learning technologies, specifically Convolutional Neural Networks (CNNs) integrated into an autonomous navigation based rover. The experiment's findings show that an autonomous rover can roam around a specified zone with a self-navigating system, precisely identifying and storing information about objects of interest, detecting unexpected events or suspicious activities in its surroundings, and responding appropriately. The project has achieved its unique initial goals, which included integrating several cameras for fast, real-time surveillance and instant security response with electrical and mechanical devices. This project is innovative in that it combines Deep Learning and AI techniques like Convolutional Neural Network (CNN) to develop a sophisticated security system with increased monitoring and threat detection skills with advanced management of mechanical equipment. By presenting an intelligent solution capable of proactively recognizing and responding to sustainability and possible security problems, this research contributes to the field of advanced surveillance systems. This project marks a substantial improvement in security technology by providing a comprehensive approach that integrates cutting-edge AI, deep learning, robotics, and real-time reporting to successfully protect commercial infrastructures.

Chapter 1

INTRODUCTION

1.1. Overture

In today's ever-changing world, safety and security have emerged as critical components of national development. People seek for a sense of security and calm in their own country. While Bangladesh has seen gains in security systems, there is still room for development, notably in the area of activity recognition-related security. To address this issue, a new solution has been created: a cutting-edge, AI and Deep Learning-based activity recognition security system. This innovative security system intends to simplify and improve the monitoring process by seamlessly recording and automatically analyzing real-time activity of persons at commercial areas. Individuals are no longer required to stand in front of security-mandated areas or use particular scanners to identify suspicious activity. Instead, the project aims to create and implement an autonomous surveillance rover that uses cutting-edge deep learning algorithms and powerful computer vision techniques. Its major goal is to improve safety and security by detecting objects and activities and discriminating between normal and possibly violent objects. The autonomous rover can conduct real-time surveillance, continually patrolling specific regions and responding quickly to possible threats. This approach ensures an advanced and well planned security procedure while maintaining the highest level of accuracy. Through autonomous navigation, the rover navigates the environment adeptly, surmounting obstacles, and optimizing its trajectory, thereby addressing crucial localization, mapping, and path planning challenges. The system efficiently processes vast volumes of CCTV/camera footage, employing advanced algorithms to extract pertinent information, track objects or individuals, and swiftly identify anomalies or potentially hazardous activities. The project entails seamless integration of hardware components and software infrastructure while ensuring scalability, robustness, and ethical considerations are meticulously addressed. The preservation of privacy will remain a paramount concern throughout all stages of development and deployment.

1.2. Engineering Problem Statement

The project shows expertise of adaptive identification, multi-camera arrangement development, and harmonic hardware-software fusion while overcoming challenging obstacles. The diversity of stakeholders, from crowded public areas to esteemed institutions, punctuates the need for a security canvas that is both smart and approachable.

The project addresses the complexity inherent in identifying and analyzing anomalous object and activity features accurately. Object recognition involves intricate algorithms and data processing to capture and compare facial characteristics with a vast database of known identities. This process requires a comprehensive understanding of complex image analysis and pattern recognition techniques. Moreover, the project involves adapting the security system to detect changes in activity over time. This adaptive capability requires continuous learning and updating of the system's knowledge base, incorporating new data and adjusting algorithms accordingly. Managing the dynamic nature of object alterations and ensuring accurate identification further adds to the complexity of the engineering problem. The integration of multiple cameras and the coordination of a surveillance rover through a micro-controller introduced additional technical challenges. Synchronizing the operation of multiple cameras, processing the captured data, and managing the flow of information between the cameras, the central server and to the response giving machinery requires careful engineering and system design.

Considering these factors, the chosen topic of developing a multiple-camera security system with AI and Deep Learning techniques with autonomous surveillance rover meets the conditions of a complex engineering problem. It encompasses intricate technical aspects, addresses challenges in facial recognition and adaptive identification, robotic path planning. By successfully tackling these complexities, the project aims to deliver a highly advanced and effective security solution.

1.3. Related Research Works

Security and surveillance systems, integral to diverse aspects of human life, prominently feature Closed-Circuit Television (CCTV) cameras, traditionally monitored by human oversight to ensure safety and deter criminal activities. However, recent efforts have been directed towards elevating the efficacy of surveillance systems through the incorporation of artificial intelligence (AI). This involves the deployment of algorithms to process CCTV footage, facilitating the identification of specific objects, such as weapons, or unusual behaviors. The collaborative attempts in integrating AI into surveillance mechanisms hold promise for diverse stakeholders, including commercial entities, private proprietors, and security organizations. The anticipated benefits include a reduction in human errors associated with comprehensive CCTV monitoring, thereby enhancing operational efficiency and effectiveness. Consequently, this integration is positioned to significantly enhance the overall effectiveness of surveillance systems, leading to a simultaneous decrease in the occurrence of criminal activities.

1.3.1. Earlier Research Work

Research provides a unique approach for detecting unusual events in multi-camera surveillance videos. Unlike traditional methods, which treat cameras independently, this framework employs a coupled hidden Markov Model (CHMM) to combine information from various streams during inference. The approach involves a two-stage training process: first generating a set of usual events using clustering and user feedback, then training a precise CHMM model. Unusual events are identified by comparing the likelihood of test segments with the CHMM model. The method is evaluated on real-world datasets, demonstrating its superiority in detecting rare or novel events by leveraging multiple camera perspectives. Their framework has been evaluated qualitatively on 56 hours of video collected by the camera network and quantitatively on the publicly available Terrascope Dataset. Notable contributions include the CHMM integration, efficient two-stage training, and successful experimental validations. Future work may involve incorporating identity information, adapting model complexity, and integrating explicit 3D locations of objects for enhanced detection [1].

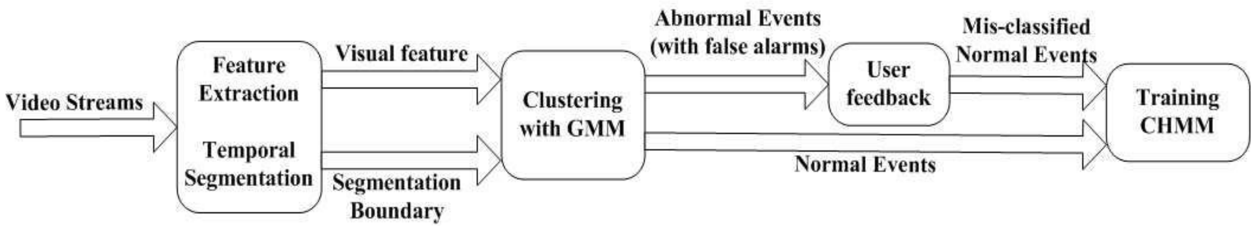


Figure 1.1: Overview of the training process

A Study provides an update on previous surveys and focuses on contextual abnormal human behavior detection, particularly in video surveillance applications. It identifies the existing methods and highlight key challenges in the field. Bayesian modeling approaches, including Latent Dirichlet Allocation (LDA), probabilistic Latent Semantic Analysis (pLSA), and Hierarchical Dirichlet Process (HDP), have been used for abnormal behavior detection in video data. Overall, while the paper provides a comprehensive review of existing methods and identifies key challenges in abnormal human behavior recognition, it does not explicitly discuss the limitations of the reviewed methods or propose solutions to address these limitations [2].

A different study presents an unsupervised method for detecting unusual activity in videos using simple features. Instead of relying on complex activity models or supervised feature selection, the approach involves segmenting the video and extracting features, then creating a prototype-segment co-occurrence matrix. This matrix is used to establish relationships between prototypes and video segments, aiming to satisfy a transitive closure constraint. The technique is inspired by document-keyword analysis and involves embedding prototypes and segments in an N-D Euclidean space. The paper introduces an efficient algorithm for co-embedding and validates the approach through experiments on real-life videos. The proposed method contrasts with model-based approaches that require defining and modeling "normal" activities, making it particularly useful for detecting unusual events in unconstrained environments. Their work emphasizes the importance of selecting relevant features for event comparison, balancing descriptiveness and robustness across varied video content. The algorithm's basis is in clustering similar video segments using co-occurrence information, where informative keywords are essential for effective clustering. Their system has demonstrated success in ground truth comparison on various sequences, involving the processing of over a million video frames in large-scale tests [3].

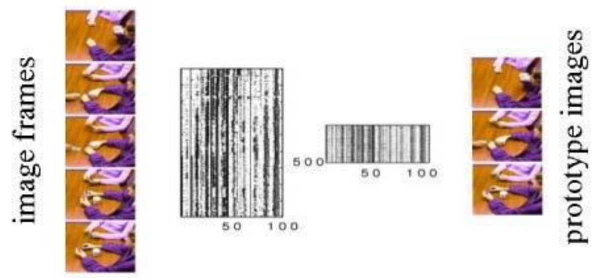


Figure 1.2: Create prototypes from set of features

The research based on the Surveillance-Oriented Event Detection in Video Streams tackles the challenge of identifies security-related events. It outlines two main avenues for analysis: explicit event recognition and anomaly detection. Explicit recognition involves a predefined knowledge base to identify and describe events, while anomaly detection autonomously builds event models to find common patterns and rare deviations. While explicit recognition offers high-level insights, it demands prior structure and expert input. In contrast, anomaly detection adapts dynamically but lacks semantic context, necessitating human assessment. The gaussian Karnel Method was used c for data training. The research introduces video processing techniques and highlights the persisting complexity in analyzing events due to subjectivity and real-world variations. The design system works perfectly fine in recognizing anomalies such as event of U-turn. The ongoing pursuit is to merge anomaly detection's adaptability with the semantic depth of explicit recognition [4].

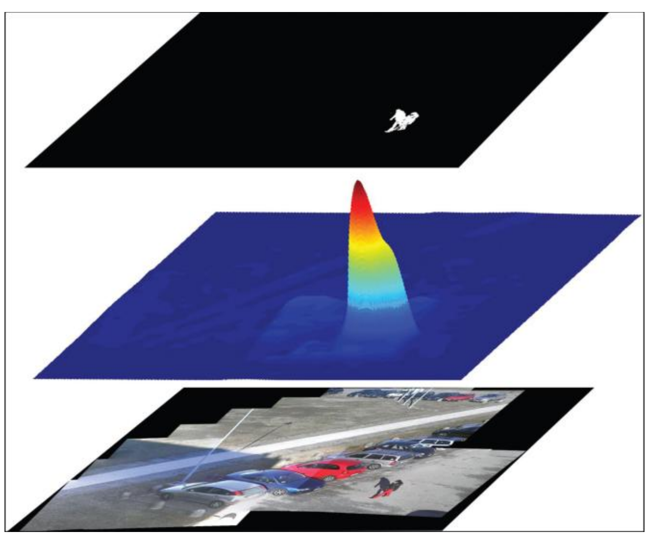


Figure 1.3: Detecting moving objects by comparing the current image with a background mosaic, with probability density function.

1.3.2. Recent Research Work

A Research presented an intelligent and automatic system designed to efficiently monitor crowds and identify abnormal activities during Hajj and Umrah. A lightweight CNN model is trained on a custom dataset to identify pilgrims in surveillance footage. Salient frames with pilgrims are processed by another lightweight CNN to extract spatial features. Utilizing a Long Short-Term Memory (LSTM) network, the system extracts temporal features from the processed frames. In the event of violent activity or accidents, the system triggers real-time alarms to notify law enforcement agencies, aiding in prompt and effective responses to prevent accidents and stampedes. Results indicate promising accuracy rates of 81.05% and 98.00% on publicly available violent activity datasets, demonstrating the system's efficacy. The system's ability to balance computational complexity makes it suitable for resource-constrained devices, potentially enhancing crowd monitoring during pilgrimages [5].

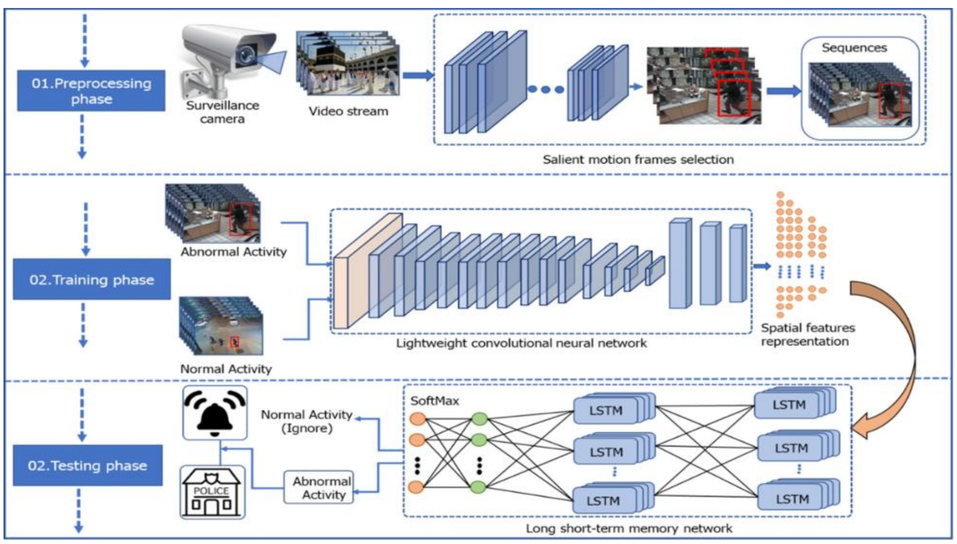


Figure 1.4: Framework of violent activity recognition.

Another research offered a revolutionary neural network technique called "AnomalyNet" that incorporates these fundamental features into a cohesive framework for anomaly identification. This block is designed to keep the temporal and spatial links between motion and appearance signals intact. As a result, it successfully removes noisy backgrounds, collects motion-related information, and compensates for data inadequacies. This block uses the transferability of neural networks from other tasks or domains to extract discriminative characteristics. It enables the model to learn and utilize information gleaned from many sources. This innovative recurrent neural network learns sparse representation and dictionary using an adaptive iterative hard-thresholding method (adaptive ISTA), which differs from typical sparse coding optimizers. This combination of 'L1-solver' and LSTM is a novel strategy that bridges the gap between these two approaches. The study illustrates AnomalyNet's cutting-edge performance in the job of anomalous event identification [6].

Figure 1.5: Normal and Abnormal frame detection

In another research a design is made of an optical flow-based framework for real-time moving object detection in unconstrained scenes, which outperforms state-of-the-art methods and utilizes a dual-mode judge mechanism for adaptation to different situations. The precision and frame rate of the optical flow estimation algorithm are crucial for the success of the framework. The framework consists of three main processes: optical flow estimating, background modeling, and foreground extracting. A dual-mode judge mechanism is introduced to heighten the system's adaptation to different situations. Two evaluation metrics are redefined for more properly reflecting the performance of the methods. The precision and frame rate of the optical flow estimation algorithm are crucial for the success of the framework [7].

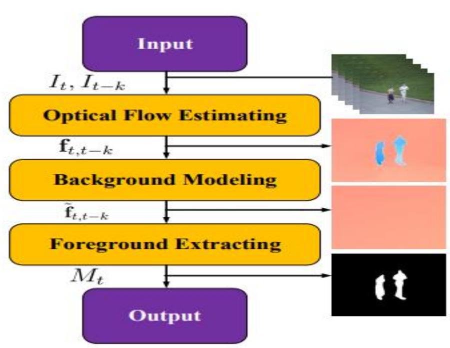


Figure 1.6: Visualization of the moving object detection frame work.

In a different study an algorithm based on a deep convolutional network to detect the A Chinese traffic sign has been proposed. It achieves real-time detection and reduces computational complexity. The proposed method is faster and more robust than existing methods, with a detection speed of 0.017 s per image, according to experimental results evaluated on the expanded Chinese traffic sign dataset and German Traffic Sign Detection Benchmark. The paper proposes a real-time Chinese traffic sign detection algorithm based on modified YOLOv2 and constructs the CCTSDB dataset. The algorithm uses an end-to-end learning model to achieve fast detection by employing multiple 1 × 1 convolutional layer in the intermediate layers and fewer convolutional layers in the top layers to construct a single convolutional network. The algorithm also uses a fine grid to divide the images to detect small sizes of traffic signs. The results evaluated on CCTSDB and GTSDB demonstrate that the proposed method is the fastest and more robust in real-world environments. Therefore, the proposed algorithm is effective in detecting Chinese traffic signs in real-time [8].

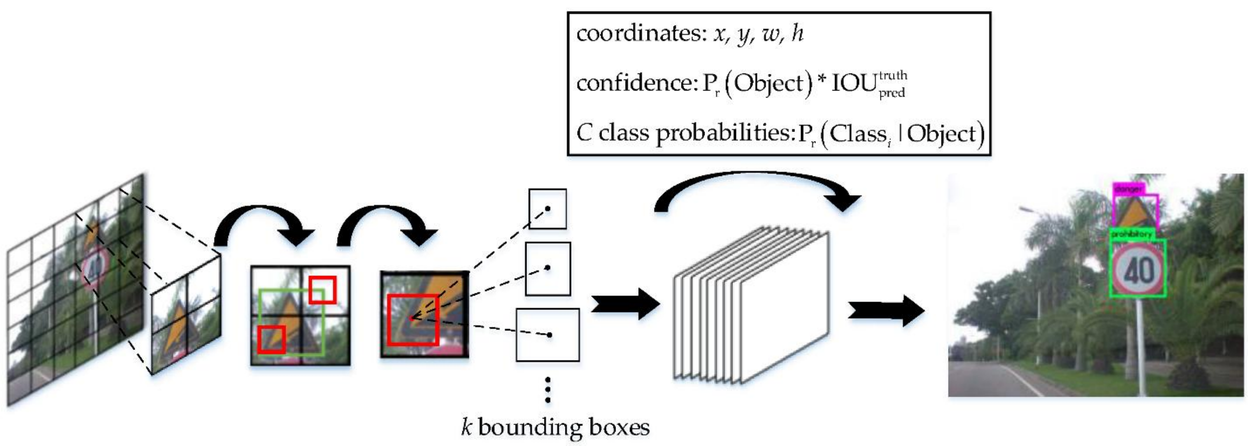


Figure 1.7: The Chinese traffic sign detection algorithm.

In separate research effort the recent advancements and challenges in background subtraction for moving object detection has been explored. Background subtraction is vital for video analytics, and its performance affects higher-level tasks. The emergence of deep neural networks has significantly impacted this field, overcoming challenges through advanced techniques. The review presents a comprehensive analysis of both conventional and recent developments, discussing challenges, benchmark datasets, and algorithms. The system have been very successful with the help of deep neural networks in handling challenges like night videos and shadows. The research work also underscores the need for more reliable solutions and robust frameworks to address remaining challenges in real-time applications [9].

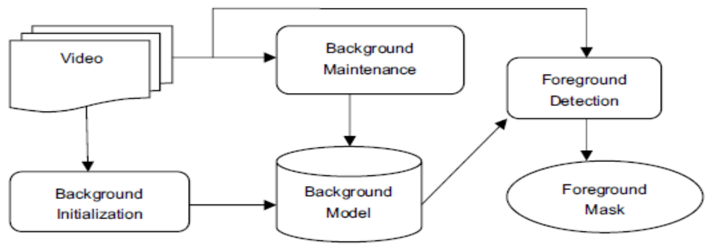


Figure 1.8: Generalized background subtraction process

1.4. Significance of the Project

The use of CCTV cameras in commercial places is of utmost importance for several reasons. First and foremost, CCTV cameras act as a powerful deterrent against potential criminal activities such as theft, vandalism, and unauthorized access. The mere presence of surveillance cameras can significantly reduce the likelihood of these incidents occurring, creating a safer environment for both employees and customers. Moreover, CCTV footage serves as valuable evidence in the event of any security breaches or disputes, aiding in investigations and ensuring accountability. It also helps in monitoring employee behavior, enhancing productivity, and identifying areas for improvement in business operations. By providing real-time monitoring capabilities, CCTV cameras allow business owners to respond promptly to emergencies or safety concerns, preventing potential damages or losses. The CCTV camera footage is examined by an authorized person using the traditional approach, which may have some drawbacks for commercial locations like markets, schools, universities, railways, airports, bus stops, etc. However, real-time analysis of all the footage is almost impossible. Our proposed model, which is based on artificial intelligence, can analyze the video in real time. This system will be able to detect any unusual behavior, such as smoking or brandishing a weapon (rifle, handgun, or knife) etc. The system is seamlessly integrated with an autonomous surveillance rover with a 2D LIDAR that leverages the capabilities to effectively monitor the entire designated area. As a result, the suggested model has a variety of applications. The system is intended to save the abnormal activity after classifying it in a database so that it can alert the user and save the record for them. As a result, it will lessen the danger of fatalities and let residential areas regain their tranquility. We will be able to enhance the CCTV camera settings for use in every model, which will be tailored to the particular site, by utilizing this project.

1.4. Critical Engineering Specialist Knowledge

The proposed system will be able to search, collect, and analyze anomalous object outlines and compare them with a given database that already is in existence by using Deep Learning techniques. The project involves the development of a highly professional and advanced security alongside with surveillance system that utilizes Deep Learning techniques to monitor the specified area for any kind of anomalous objects and events. These outlines of the anomalous objects will be compared with an existing database of known identities. Afterwards, an integral aspect of this system is its ability to automatically learn and adapt through artificial intelligence (AI), enabling it to identify the variation of objects, colour schemes, the structural design of any kind of weapon. In order to achieve accurate and reliable object detection and recognition, a combination of techniques was executed. In previous years, conventional techniques like Histogram of oriented Gradient (HOG), Haar Cascade were used to detect all kinds of object detection. In our project, we managed to execute the technique CNN (Convolutional Neural Network) as it has much accuracy and reliability. Moreover, CNN is much flexible and can adapt a wide range of object detection tasks where other mentioned techniques might require significant manual tuning. This choice was driven by the fact that these techniques have been shown to produce more precise and accurate results.

1.5. Stakeholders

Stakeholders with the greatest significance are the users who will interact with and benefit from the security system's capabilities. It could be educational institution owners, railway stations, airports, passengers or shop owners who wish to enhance their security measures. The surveillance system can be used by educational institutions to ensure the safety of their campuses. It has the ability to roam around entry points, detect anomalous events and issue immediate alerts. This helps prevent unauthorized entry, vandalism, and other undesirable activities in academic settings.

In railway stations, the security system, when integrated with access control mechanisms, can authenticate identities and provide secure access to restricted areas. This ensures that only authorized personnel have entry to critical zones such as platforms or control rooms. By incorporating advanced data analysis, the system can find great utility in airports. Cameras positioned strategically throughout the airport can effectively oversee key areas like terminals, entrances, baggage claim, and parking lots. This strategic arrangement assists in identifying suspicious behaviors, unlawful entry, and other security concerns. Leveraging the security system's computer vision capabilities, railway stations can detect and track suspicious objects or unattended baggage, facilitating swift responses while upholding the safety of both staff and passengers. Through appropriate software integration, facial recognition technology can be employed to identify individuals on watch lists or identify potential threats. This integration significantly enhances security measures in railway stations, augmenting the overall safety infrastructure.

Furthermore, in airports, the security system aids passengers by maintaining a watchful eye on critical areas, bolstering their sense of safety throughout their journey. It can also be of value to shop owners in various locations, deterring theft and safeguarding their premises. Additionally, law enforcement agencies can utilize the system to access captured images of criminals or suspects. By searching the system's camera database, they can determine the location and timeframe of certain individuals. This enhances their investigative capabilities and contributes to maintaining public security.

1.6. Objective of the Work

The main purpose of this project is to develop a sophisticated system for anomalous event detection aiming to enhance the safety and security measures through the utilization of autonomous robot operating system. The proposed approach will enable stakeholders including management, staff, customers, security officials or privet owners or others involve with surveillance system to swiftly recognize potential threats and respond effectively.

1.6.1. Primary goals:

- Identification of unusual or potential dangerous activity as smoking, carrying weapons
- Monitor multiple CCTV footages at once
- Inform property owners or security authority through server

The primary objectives of this project encompass several key facets. Firstly, the project is focused on the quick and precise identification and mitigation of unusual or potentially dangerous intentions. This necessitates the development of a vigilant system capable of detecting any acts that depart from typical behaviors and, as a result, addressing security issues in advance. Secondly, the system will be able to monitor multiple cameras at once as traditional way of monitoring CCTV cameras sometimes fails to detect activities leading to harmful situations. Thirdly, this system intends to warn property owners or security authorities as soon as potential security threats develop. By doing so, the initiative hopes to promote faster reaction times and proactive intervention to mitigate possible dangers. So, the fundamental objective is to use technology to build a monitoring architecture that maximizes awareness and response.

1.6.2. Secondary Goals:

- Development of an autonomous navigation rover
- Maintain Indoor surveillance

In addition to the primary goals, the project has multiple secondary goals: first, The project aims to build an autonomous navigation robot outfitted with advanced technology that can patrol and monitor the designated area efficiently. The robot will be programmed to navigate autonomously, detecting and avoiding obstacles in its path using advanced algorithms. The autonomous rover will be outfitted with dependable communication systems to ensure that it maintains contact with the central system (IoT server) and can quickly relay information about anomalies it detects. The project's also core objective is to maintain comprehensive indoor surveillance across the specified area. The system will provide uninterrupted surveillance coverage, day and night, without relying on human intervention. Both the Web cameras and the autonomous rover will be integral in achieving this continuous monitoring.

1.7. Organization of Book Chapters

The book's information will be separated into chapters. Here are the specifications on how the content will be linked and carried over from chapter to chapter.

Chapter-2: Project Management

This chapter will go through the management techniques for the capstone project in great depth. It will start with the presentation of a project Gantt chart, which will detail the project's timetable and important milestones, assisting in planning and tracking progress. Various related concerns, such as opportunities, threats, and weaknesses, will then be examined, offering a thorough grasp of the external and internal aspects that will impact the project's success. Economic models will also be reviewed in order to determine the project's financial feasibility and profitability in the future. Furthermore, management tenets, which include core concepts and practices, will be investigated to guide future project execution. Finally, project cost analysis will be discussed, which will evaluate predicted costs and facilitate resource allocation. By addressing these aspects, the chapter will contribute to comprehensive future project management, ensuring successful outcomes.

Chapter-3: Methodology and Modeling

This chapter will provide an in-depth examination of the project's modeling. It will go through many areas of system design and implementation. The chapter will begin with the system's block diagrams, which provide a visual depiction of the system's components and linkages. These block diagrams aid in comprehending the system's general design and operation.

In addition, the chapter will provide a flow chart of codes depicting the project's step-by-step sequence of instructions and actions. This flow chart will clarify the program's or algorithm's logical flow, making it easier to understand the implementation details and decision-making process within the system. This chapter will also address simulations, which enable for testing and evaluating the system's performance under various settings and scenarios. Simulations allow you to evaluate the behavior of the system, discover any bottlenecks or defects, and fine-tune the design parameters. The project team may test the system's efficacy and efficiency using simulations, making appropriate tweaks or optimizations as needed.

The chapter gives a complete understanding of the project's modeling by integrating these characteristics. It gives readers a clear visual representation of the system's structure, logical flow of operations, and performance evaluation. These insights are critical for determining project viability, robustness, and overall effectiveness.

Chapter-4: Project Implementation

The completed project will be the major focus of this chapter. The constructed electronic structures and parts will be presented, and the principles of operation will be described. There will be a full overview of the many components and systems that will be created as part of the project. Each component will be thoroughly detailed, emphasizing its purpose, functioning, and contribution to the broader system.

In addition, the function of each proposed electronic component and system will be detailed, revealing the fundamental mechanisms and principles that will regulate their operation. This discussion will provide readers with insights into the project's technical features, allowing them to understand the operation of each component and how they will operate together to produce the intended results.

Diagrams, schematics, or circuit layouts may also be included to illustrate the design and configuration of electrical components and systems graphically. These visual aids will improve knowledge of the project's execution by depicting the links and interactions between various components.

This chapter will provide readers with a thorough grasp of the project's future execution by detailing the intended electronic components and systems, as well as their operating principles. It will emphasize the technical knowledge and inventiveness required in the design and development of electronic systems.

Chapter-5: Results Analysis & Critical Design Review

This chapter will present the overall outcome of the structure. The emphasis will be on displaying the system's accomplishments and achievements. The chapter will offer a thorough assessment of the system's performance, examining its efficacy and efficiency in achieving the targeted goals.

A complete performance study will also be carried out, comparing the actual results achieved from the installed system with the projected and postulated outcomes. This comparison will aid in assessing the system's accuracy and dependability, emphasizing any gaps or variations between predicted and actual performance. The study will give important insights into the system's capabilities, limits, and potential areas for development.

The chapter may include statistical data, graphs, or visual representations to present the performance analysis in a clear and concise manner. These visual aids will facilitate the understanding of the system's performance trends and patterns, enabling readers to grasp the significance of the results.

This chapter will offer a full picture of the project's successes and the efficacy of the implemented solution by exhibiting the system's conclusion and conducting a comprehensive performance analysis. It will validate the project's objectives and illustrate how well the system accomplished those objectives. The performance study results and insights will add to the overall assessment of the system's success and potential for future uses or modifications.

Chapter-6: Conclusion

This will be the concluding section of the paper's last chapter. This chapter will have some discussion on the overall project, limitations and improvement of the project. This chapter will also contain the survey result on the impact on the environment and society and full summary.

Chapter 2

PROJECT MANAGEMENT

2.1. Introduction

Anomalous Event Detection for Enhanced Security in Commercial Infrastructures addresses the imperative need for heightened security measures. In the face of evolving threats, this innovative system utilizes cutting-edge technology to proactively identify and mitigate anomalous events, providing a dynamic shield for commercial infrastructures.

The project was planned, coordinated, and successfully managed through the application of adequate engineering management concepts. This project has a well-organized structure that includes a detailed project plan outlining the goals, schedule, essential assets, and the future scope of the work. Active involvement of stakeholders, such as end users, project supervisors, and team members, during the planning phase was necessary to promote alignment across differing perspectives. By incorporating a wide range of perspectives and factors, this method attempted to guarantee coherence and improve the planning process overall efficacy.

Initially the project was planned defining the objective of the project, and the future scope of the project considering all the risk factors aligned with project. A methodical approach was taken to identify risks, assessing their impact and likelihood, formulating mitigation strategies, and continuously monitoring hazards, miscalculations, and potential issues that could impact project progression. The task of the project was divided into sections like Software creation and Hardware creation to complete the project smoothly.

Since project execution stands as a pivotal component in project management, the successful realization of tasks such as implementing the project plan, managing team members adaptability and efforts, and monitoring progress of the project against milestones has been accomplished successfully. Executing the project plan, overseeing team members, and tracking progress against milestones have all been integral to project execution a crucial element in effective project management. This entailed the conduct of regular meetings, provision of status updates, and building seamless communication between the project team and stakeholders.

Maintaining a steadfast commitment to quality management was paramount throughout the project. The team undertook accountability for guaranteeing that the security system conforms to the essential quality criteria. Important steps in the quality management process included extensive testing, verification, validation, and thorough documentation of the system's architecture and execution.

The final stage was carried out with signifying the completion of the development, testing, accuracy, and implementation of the security system. This included giving end users access to the functioning system, conducting a thorough analysis of lessons learned, and assessing how well the project accomplished its objectives. The project was carefully planned and managed to guarantee its success by abiding by recognized engineering management standards, including risk management, quality management. These guiding principles collectively played a pivotal role in the project's overall success, ensuring alignment with essential guidelines.

2.2. S.W.O.T. Analysis

The acronym S.W.O.T. stands for Strengths, Weaknesses, Opportunities, and Threats. This tool is utilized in strategic planning by project managers to evaluate the benefits and drawbacks of their projects, as well as to identify possible future opportunities and risks.

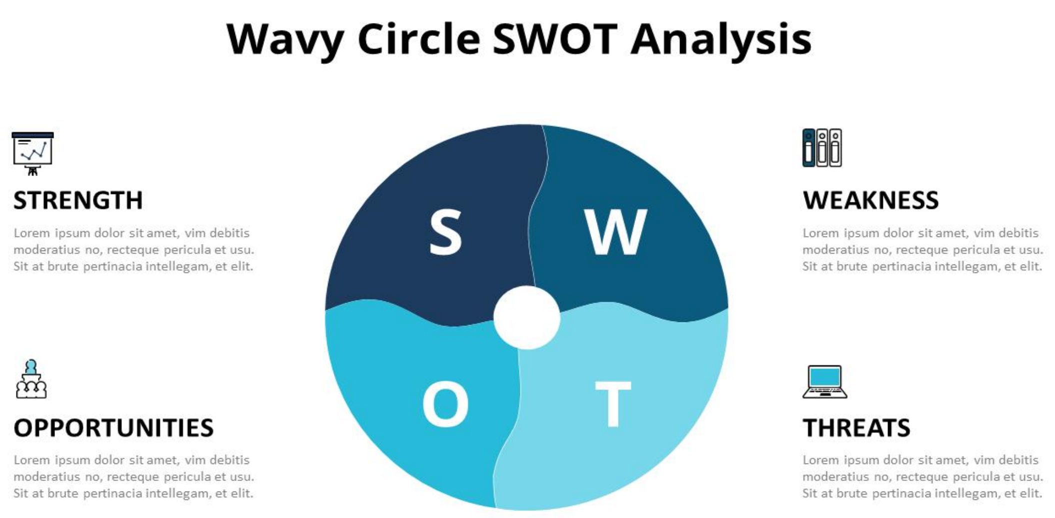


Figure 2.1: S.W.O.T Circle

- **Strength:**

In the residential neighborhoods, many people travel there for personal reasons. Some are traveling to visit a relative, while others are seeking homes. As a result, various types of people have diverse behaviors toward their environment. Some pessimistic individuals take risky actions to achieve their desired. These individuals are occasionally unknown individuals who do not exist in society. Following an incident, the individuals can be identified by using a security system. Thus, by examining their photo and duration data, this research may detect these kinds of unidentified suspects, which is crucial for developing our CCTV security system. Some residents of higher social classes own private vehicles. They are securely parking their car in their garage. A watchman opens the gate and closes it at a set time when someone leaves their automobile and enters the dwelling. Certain extra features, such as the ability to unlock the garage gate by verifying the owner's or shareholders' vehicle, should be included in order to lower the watchman expense of the system. A crime that ought to injure people does, in a way, work. Assume that by predicting criminal behavior based on the identification of potentially dangerous equipment such as firearms, knives, fire, etc., we may lessen crime and promote safety in residential areas. The weapon detection portion is therefore more advantageous for public use.

- **Weaknesses**

In order to achieve high accuracy, the system needs to acquire additional data on an item, which causes it to slow down. For example, to analyze data about an unknown individual, the system needs to retain a minimum of 50 sides of their picture before it can validate the resultant facial expression. If additional object data is used in an attempt to improve result accuracy, the system should operate more slowly.

- **Opportunities**

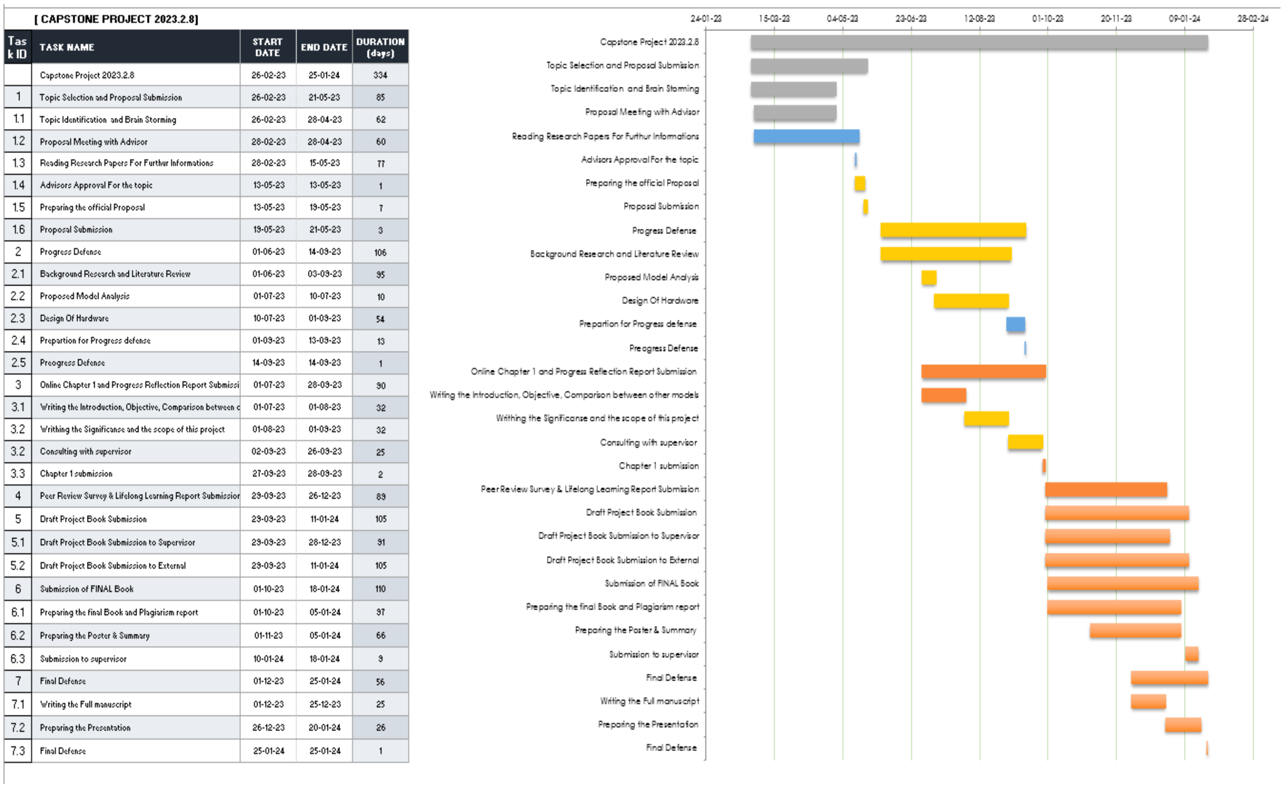
This project, aimed at enhancing residential safety and community well-being, possesses significant potential for broad implementation. Its expansive applicability stems from its inherent flexibility and adaptability, attributes that are essential in addressing the diverse needs of various neighborhoods. A key aspect of this project is the role of the admin forum, which plays a pivotal part in customizing the system. By enabling the forum to modify and adjust the system, it can be transformed into an open platform, thereby increasing its accessibility and relevance to different communities. This level of adaptability ensures that the system can be fine-tuned to meet specific local requirements, making it a versatile tool for community improvement

- **Threats**

The efficacy and reliability of a CCTV (Closed-Circuit Television) system are highly dependent on the quality of the equipment used, the strategic placement and angle of the cameras, and the configuration of the entire setup. Utilizing low-quality CCTV equipment can lead to several detrimental effects on the system's overall performance. These effects can range from poor image and video quality, which hampers the identification and analysis of footage, to frequent system breakdowns that can compromise security. In critical security applications, such equipment can be a significant liability, leading to gaps in surveillance and increased vulnerability. The selection of cameras is a pivotal aspect of an effective CCTV system. Cameras with the appropriate viewing angles are crucial to capture the necessary field of view. This is not just a matter of capturing a wider area, but ensuring that the specific areas of interest are under constant and clear surveillance. The right camera should provide a balance between wide coverage and sufficient detail to identify individuals or objects. Furthermore, factors like lighting conditions, potential obstructions, and required resolution also influence the choice of camera and its placement

2.3. Schedule Management

Schedule management involves the creation, maintenance, and communication of project schedules, encompassing both time and resource aspects. It entails establishing policies, defining procedures for implementation, and documenting project plans. Schedule management is essential for the planning, execution, development, and control of project management schedules.



[CAPSTONE PROJECT 2023.2.8]

Task ID	TASK NAME	START DATE	END DATE	DURATION (days)
	Capstone Project 2023.2.8	26-02-23	25-01-24	334
1	Topic Selection and Proposal Submission	26-02-23	21-05-23	85
1.1	Topic Identification and Brain Storming	26-02-23	28-04-23	62
1.2	Proposal Meeting with Advisor	28-02-23	28-04-23	60
1.3	Reading Research Papers For Furthur Informations	28-02-23	15-05-23	77
1.4	Advisors Approval For the topic	13-05-23	13-05-23	1
1.5	Preparing the official Proposal	13-05-23	19-05-23	7
1.6	Proposal Submission	19-05-23	21-05-23	3
2	Progress Defense	01-06-23	14-09-23	106
2.1	Background Research and Literature Review	01-06-23	03-09-23	95
2.2	Proposed Model Analysis	01-07-23	10-07-23	10
2.3	Design Of Hardware	10-07-23	01-09-23	54
2.4	Prepartion for Progress defense	01-09-23	13-09-23	13
2.5	Preogress Defense	14-09-23	14-09-23	1
3	Online Chapter 1 and Progress Reflection Report Submissi	01-07-23	28-09-23	90
3.1	Writing the Introduction, Objective, Comparison between c	01-07-23	01-08-23	32
3.2	Writhing the Significanse and the scope of this project	01-08-23	01-09-23	32
3.2	Consulting with supervisor	02-09-23	26-09-23	25
3.3	Chapter 1 submission	27-09-23	28-09-23	2
4	Peer Review Survey & Lifelong Learning Report Submissior	29-09-23	26-12-23	89
5	Draft Project Book Submission	29-09-23	11-01-24	105
5.1	Draft Project Book Submission to Supervisor	29-09-23	28-12-23	91
5.2	Draft Project Book Submission to External	29-09-23	11-01-24	105
6	Submission of FINAL Book	01-10-23	18-01-24	110
6.1	Preparing the final Book and Plagiarism report	01-10-23	05-01-24	97
6.2	Preparing the Poster & Summary	01-11-23	05-01-24	66
6.3	Submission to supervisor	10-01-24	18-01-24	9
7	Final Defense	01-12-23	25-01-24	56
7.1	Writing the Full manuscript	01-12-23	25-12-23	25
7.2	Preparing the Presentation	26-12-23	20-01-24	26
7.3	Final Defense	25-01-24	25-01-24	1

Figure 2.2: Project Timeline

2.4. Cost Analysis

One of the most crucial parameter in project management is cost analysis. This cost analysis was created in order to compare the project plan's gains and expenses. As the system’s main concern is to detect anomalous events and inform to the authority, the system can also be operated without the rover with just the web cameras connected with the computer.

Table 2.1: Cost Analysis of the Project without Surveillance Rover

Component’s Name	Price (BDT)	Quantity	Total Price (BDT)
Web Camera	3000	2	6000
API and Web	10000	1	10000
Total			16000

Table 2.2: Cost Analysis of the Project with Surveillance Rover

Component's Name	Price (BDT)	Quantity	Total Price (BDT)
Raspberry Pi 4	15000	1	15000
Web Camera	3000	3	9000
LIDAR	20000	1	20000
Motor	1500	6	9000
Motor Driver	1600	2	3200
ESP32	575	1	575
Wheel	700	6	4200
Battery, BMS	5000	1	5000
Body	5000	1	5000
Pi Display	3500	1	3500
API and Web	10000	1	10000
Others			400
Total			84875

The formula presented below is used to compute the standard deviation based on the projected estimation of the total project cost and the final implemented cost, as indicated in table 2

$$\sigma^2 = \sqrt{\frac{1}{N}} \sum_{i=1}^{N} (x_i - \mu)^2$$

Where:

N= Total number of quantities.
μ = Mean value
xi = Individual cost

Mean= $\frac{\Sigma x}{N}$

Where Σ x = Total Cost

Variance, $\sigma 2 = \frac{(x_i - \mu)^2}{N}$

N = 11

Table 2.3: Statistical analysis of cost of the project

Name	Total Cost(BDT)
$\sum X$	84875
M	7073
σ^2	34300620
σ	5859

Therefore, the overall standard deviation is 5859 (BDT). Which can be considered acceptable.

2.5. P.E.S.T Analysis

Political, Economic, Social, and Technological (PEST) Analysis is a management approach that allows a company to analyze the important outside factors that influence its operations to improve its market competitiveness. These four sections represent the foundation of this paradigm, as shown by the acronym [10]. Here given the external aspects that can have an impact on the success of an anomalous event detection capability-based autonomous rover to conduct a PEST analysis:

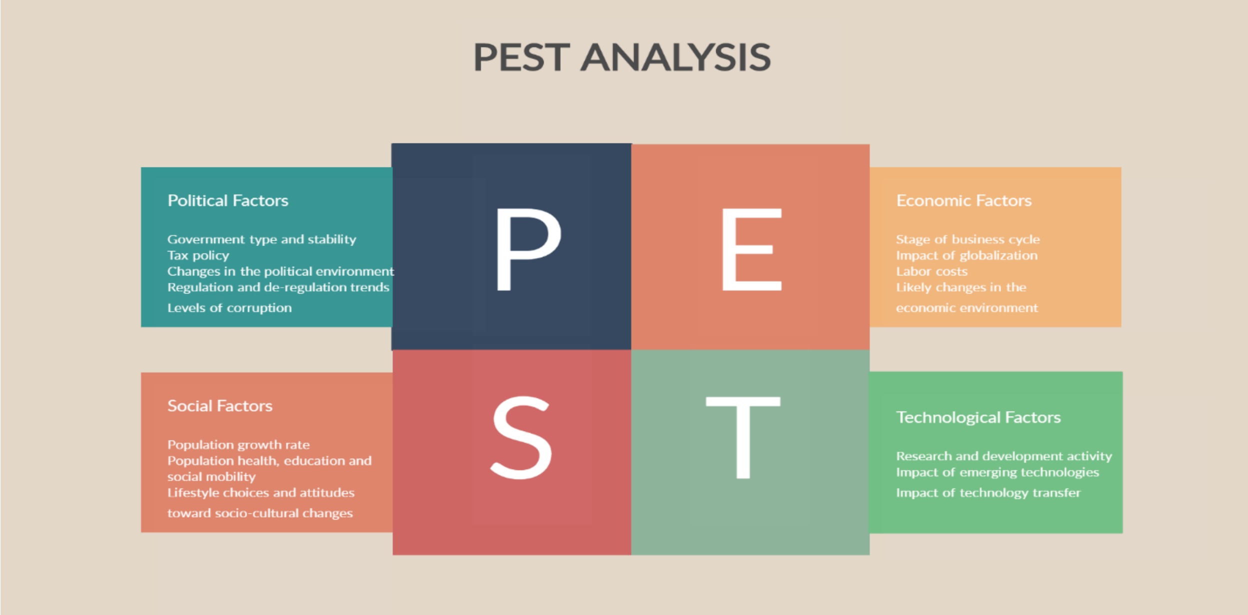


Figure 2.3: P.E.S.T Analysis

- **Political Factors:**

Object and activity-based security systems create significant political issues, including possible abuses of privacy and civil rights owing to the capture and storing of persons' belongings without their consent, as well as the possibility of misuse and illegal access to these. These systems allow for widespread monitoring, raising concerns about the balance between security and individual liberties, while also displaying biases that disproportionately affect underprivileged populations. Public trust is further eroded by a lack of openness and accountability, as well as reliability difficulties. The risk of function and purpose creep, in which technology goes beyond its intended use, highlights the importance of democratic supervision and regulation to guarantee responsible implementation. These issues may affect the design and implementation of the system, particularly in sensitive locations like airports and government buildings. Due to various laws, cultural distinctions, and political difficulties, international relations might affect how the system is adopted in other nations.

- **Economic Factors:**

The financial cost of deploying an advanced security system that combines AI and machine learning may be a major obstacle to adoption, especially for smaller businesses and organizations. Economic downturns can affect system adoption because businesses and people may prioritize other expenditures. The application of AI and machine learning in security systems may result in job losses in the security business. According to the World Economic Forum, AI will have a significant influence on the employment market, both generating new jobs and eliminating current ones. In particular, it is anticipated that the usage of AI will result in the loss of 75 million jobs globally by 2025 and the creation of 133 million new jobs. It is anticipated that this will lead to a net increase of 58 million employment [11]. The project, on the other hand, delivers a low-cost security solution by utilizing open-source software and low-cost hardware components. This cost-conscious approach has the potential to increase accessibility by making the system more accessible to individuals or organizations with low financial resources. Furthermore, the creation of jobs in the technology and security industries may be aided by the development, installation, and maintenance of the security system. Skilled individuals may be needed for a variety of jobs, such as system design, coding, installation, and continuous maintenance, creating job opportunities and promoting economic growth in these regions.

- **Social Factors:**

The system's adoption may be affected by how people and organizations determine security. The adoption of object and activity-recognition-based security systems is heavily influenced by people's and organizations' perceptions of security. Privacy concerns generated by AI and machine learning in such systems may lead to hesitancy or opposition to their implementation. Individuals may be concerned about their possessions being monitored and scanned without their knowledge or consent, which can undermine trust and impede adoption. The level of adoption is also influenced by the amount of education and understanding about the benefits and limits of current security solutions that incorporate AI and machine learning. However, if individuals and organizations are adequately informed about the benefits, such as enhanced surveillance capabilities and improved identification accuracy, as well as the potential drawbacks, such as privacy violations or biases then they can make more informed decisions about adoption. Efforts to educate the public on the operation, limits, and safeguards included in activity recognition systems can help encourage acceptance and increase adoption rates. Clear information on how data is gathered, handled, and secured, as well as concerns about potential abuse or unauthorized access of objects, may help create trust and ease privacy worries. Furthermore, highlighting the possible societal advantages of facial recognition-based security systems, such as crime prevention, public safety, and increased efficiency in law enforcement or border control, can help. Finally, balancing privacy and security is critical in molding public image and adoption of facial recognition technology.

- **Technological Factors:**

Surveillance systems that incorporate AI and machine learning benefit from significant technological advancements, which may result in more complicated and cutting-edge solutions. These advancements increase the efficiency and precision of security systems by allowing them to process and analyze huge amounts of data in real time, including object detection and activity recognition. In the end, determining public opinion and acceptance of object and activity detection technology requires striking a balance between privacy and security. Promoting openness, ensuring robust privacy protections, and engaging in open interactions with the public are critical initial steps in creating an environment that encourages the deployment of AI-powered security solutions. However, it is critical to understand that technological adoption involves dangers and weaknesses. AI-powered security systems' networked nature can leave them vulnerable to hacks or illegal access. Hackers or malevolent actors may exploit system vulnerabilities, jeopardizing its integrity and possibly gaining unauthorized access to sensitive data, or even disabling vital security functions. To address these concerns, it is critical to build security systems that incorporate strong safeguards and countermeasures against cyber threats. This entails installing strong encryption techniques, constantly updating software and firmware to address known vulnerabilities, performing extensive security audits, and developing comprehensive security procedures and best practices.

2.6. Professional Responsibilities

Within the project, we assumed diverse professional duties. This encompassed the design and development of the system, where we applied AI and machine learning to construct a secure, reliable, and scale-able system that adhered to industry standards. Our attention was directed toward ensuring the safety and security of the system by identifying and addressing potential risks. We sustained our professional skills through continuous learning and active participation in training programs, staying informed about the latest advancements in security systems, AI, and machine learning. Upholding professional ethics, we prioritized integrity, honesty, and privacy, using permissible images and data. Additionally, we guaranteed compliance with regulatory requirements, covering data protection, privacy laws, cyber security rules, and industry standards. Our dedication involved a thorough evaluation of each component to safeguard the rights and confidentiality of stakeholders and users.

2.6.1. Norms of Engineering Practice

Problem Identification and Requirements: The initial stages involve identifying problems in society and determining project requirements. In the security system project, ethical issues with conventional systems were recognized, while the Anomalous Event Detection project focused on factors such as object and activity detection.

Design and Analysis: In both projects, the design phase considers various variables such as cost, efficiency, safety, and viability. For the Anomalous Event Detection project, engineers follow specific design guidelines for railway and control systems, optimizing performance and mitigating risks. Analytical techniques and simulations are employed to evaluate system performance.

Maintenance and Support: Continual maintenance and support are integral, involving regular updates, bug fixes, and system upgrades in both projects.

Documentation and Standards: Comprehensive documentation is maintained throughout the project life-cycle, adhering to relevant engineering standards. For the Anomalous Event Detection project, this includes design documents, technical specifications, and safety protocols set by international organizations like IEC and IEEE.

Quality Assurance and Project Management: Both projects follow engineering guidelines for testing and quality assurance, including unit testing, integration testing, and system testing. Project management principles are applied to define objectives, establish plans, allocate resources, manage risks, and monitor progress, ensuring successful resolution and delivery of reliable and efficient systems.

2.6.2. Individual Responsibilities and Function as Effective Team Member:

Tasks of Member (Leeon, Masud Raihan)

- Hardware implementation
- Programming (Algorithm)
- Circuit simulation
- Equipment management
- Cost management
- Writing chapter 2,4

Tasks of Member (Billah, Mohtasim)

- Hardware assembly
- Program bug detection
- 3D Modelling
- Project management
- Result Analysis

- Writing chapter 1,3,5,6
- IEEE paper writing

Tasks of Member (Romim, Md. Abu Ayaz)

- Component Collection
- Hardware testing
- Poster design
- Preparing block diagram and flowchart
- Writing paper summary
- Writing chapter 2,4,5,6

Tasks of Member (Rahman, Md. Shajidur)

- Proteus simulation
- Data collection
- Writing chapter 1,2,3,6
- Preparing the poster
- Preparing the presentation slides

2.7. Management Principles and Economic Models

The use of engineering management models and concepts in the Advanced Security System using AI Machine Learning by Raspberry Pi project has contributed to its timely, effective, and high-quality completion. Engineering management models and principles have been applied to the project of an Advanced Security System using AI Machine Learning with Raspberry Pi and other peripherals.

Agile engineering management: Rapid delivery, flexible planning, and customer collaboration are the main goals of agile engineering management. It is a cooperative, iterative process. The development process of the security system has been managed using this technique, which includes frequent feedback loops from external and supervisory sources in addition to continuous programming, integration, and testing.

Total Cost of Ownership (TCO): This model takes into account the total cost of a project over the course of its development, maintenance, and replacement phases. Finding cost-effective solutions that were initially more expensive but offered more accurate long-term value was made easier with the help of TCO. For instance, it was still difficult to find a Raspberry Pi 4B, even though the cost of the other parts was the same. We had to investigate used components in order to make up for the shortage.

Risk Management: The idea of risk management entails identifying possible risks, assessing their likelihood and effects, and developing mitigation strategies. Throughout the design and development of the security system, this concept has been applied to the creation of methods to lower risks such as hardware malfunctions, servo motor alignment, and sensors.

Open-Source Software: The fact that open-source software is usually free helps to lower the initial and continuing costs of development and maintenance. Rather than starting from zero, the project team could have leveraged preexisting open-source libraries and tools for security and machine learning.

Prioritize Functionality: Instead of trying to create a comprehensive solution, the project team has chosen the security system's most important features and functionalities. By using this approach, the cost and duration of development would have been decreased while maintaining a functional and effective service.

2.8. Summary

"Anomalous event detection for enhanced security for commercial infrastructures" project was managed systematically and effectively, resulting in a successful completion. The project followed established engineering management principles, including project planning, risk management, and stakeholder engagement. A clear project plan with defined objectives and milestones was established, enabling the team to track progress and ensure timely completion. Risks were identified and managed

(AIUB) 25 Proactively, ensuring that potential obstacles were addressed promptly. Stakeholder engagement was a key focus, with regular communication and collaboration to gather requirements, address concerns, and ensure their support throughout the project. Additionally, economic considerations were taken into account, with cost-benefit analysis and life cycle cost analysis conducted to ensure a cost-effective solution. By following these systematic management approaches, the project team effectively coordinated efforts, mitigated risks, and delivered a successful anomalous event detection-based surveillance system.

Chapter 3

METHODOLOGY AND MODELING

3.1. Introduction

The project "Anomalous Event Detection for Enhanced Security for Commercial Infrastructures" implemented several basic engineering theories and methods to achieve its objectives. Here we discuss some step-by-step procedure:

Deep Learning and artificial intelligence (AI): The project uses AI techniques, particularly Deep Learning, to create models capable of analyzing and comprehending visual data received from several cameras. Convolutional Neural Networks (CNNs), a type of Deep Learning technique, offers the ability to identify, recognize, and track objects.

Computer Vision: The multiple-camera system's visual data needed to be processed and analyzed using computer vision algorithms. To distinguish objects, detect motion, and extract relevant data from video feeds, techniques such as image segmentation, feature extraction, and picture classification were employed.

Image processing: Image processing techniques were used to improve the quality of the obtained photographs. Noise reduction, picture filtering, edge detection, and image enhancement techniques are used to prepare input data for later analysis and decision-making.

Collecting Data and Annotation: To train the AI models, the research required collecting and annotating large quantities of photographs or videos. To provide the models with real-world data to train from, this process required thorough data labeling and annotation.

Data preprocessing: Before the data was fed into the AI models, multiple preprocessing approaches were applied to ensure it was in the correct format and to improve model performance, including scaling, normalization, and data augmentation.

Model Training and Optimization: The project required creating Deep Learning models from the obtained and annotated data. To improve the models' precision and effectiveness, techniques such as transfer learning, hyperparameter optimization, and model fine-tuning were used.

Performance Evaluation: The study employed approaches to assess the effectiveness of AI models in recognizing and classifying objects of interest while also giving the needed security outcomes. These strategies included precision, recall, accuracy, and the F1 score.

3.2. Block Diagram and Working Principle

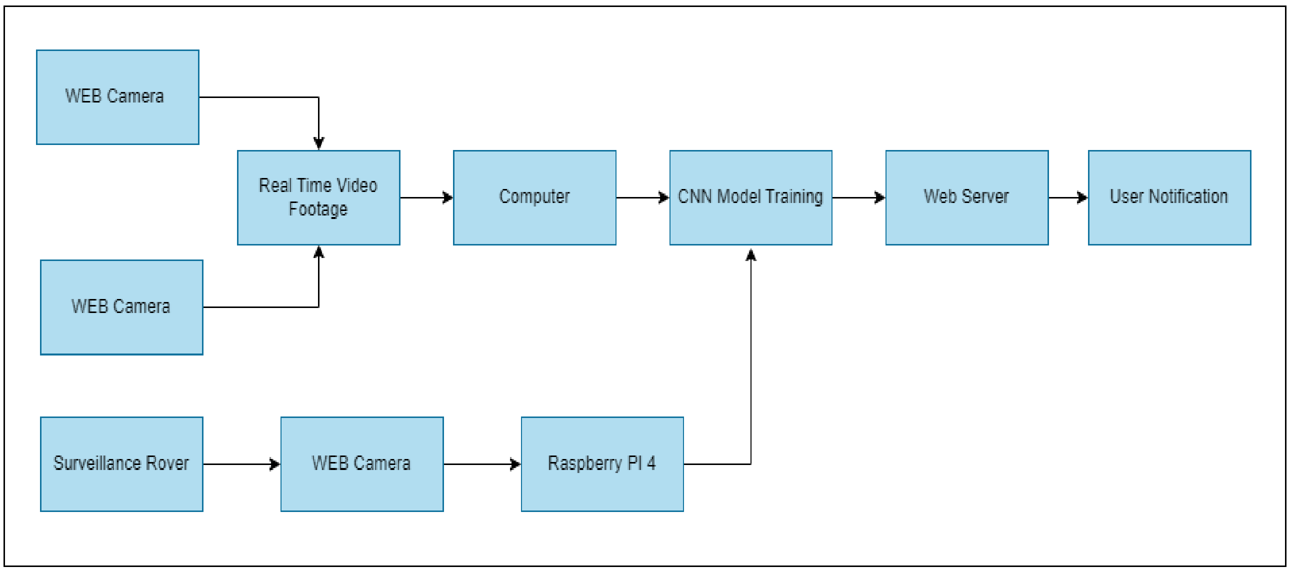


Figure 3.1: Block diagram of the system

In figure 3.1, the system integrates both stationary Web cameras and a mobile surveillance robot to provide comprehensive video surveillance. It utilizes a Convolutional Neural Network (CNN) model for intelligent video analysis and notification.

Web cameras scan the areas, keeping a constant eye on everything and the Real-time footage gets sent to a computer, where a trained CNN model scans for anything suspicious. If the CNN sees something out of place, it sends an alert to the web server. The web server translates the alert into a notification, instantly letting you know something's up.

On the other hand the surveillance rover patrols, equipped with another camera capturing hidden corners and dynamic areas. Video footage from the rover travels to the computer, joining the stream from the Web cameras. The CNN model examines the rover's footage, applying its trained knowledge to identify potential threats or events. If the CNN finds anything noteworthy, it triggers an alert, relayed by the web server to keep you informed, no matter where the rover discovers something abnormal. Both the Web camera and rover work together, feeding the same AI analysis system. Their combined vision and the CNN's intelligence create a comprehensive and proactive security system.

Working Principle of Software and Hardware:

Software:

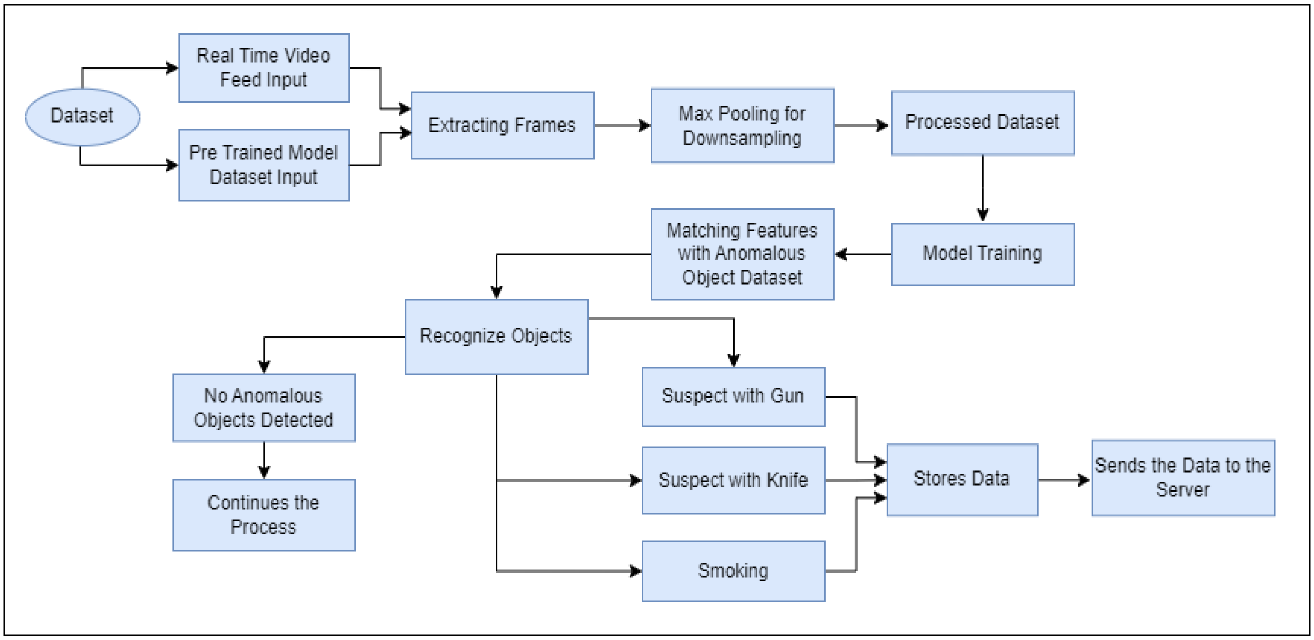


Figure 3.2: Working principle of the Algorithm.

This project's dataset includes anomalous occurrences of gun, knife, and smoking behaviors obtained from the internet, as well as a managed in-house dataset. To improve the datasets, they were processed using a Convolutional Neural Network (CNN) architecture with max-pooling layers.

During model training, the CNN learns unique characteristics linked with weapons, knives, and cigarettes. The system compares these traits to anomalous item databases to aid in accurate detection. When such things are detected, data is captured and instantly transferred to a web server for user notice. If no suspicious items are found, the system effortlessly resumes its processing cycle. This method enables real-time knowledge of security issues while reducing unnecessary notifications. The system's efficiency stems from its sophisticated analysis of visual data, which provides a reliable solution for threat detection in situations prone to security hazards such as guns, knives, and smoking.

Hardware:

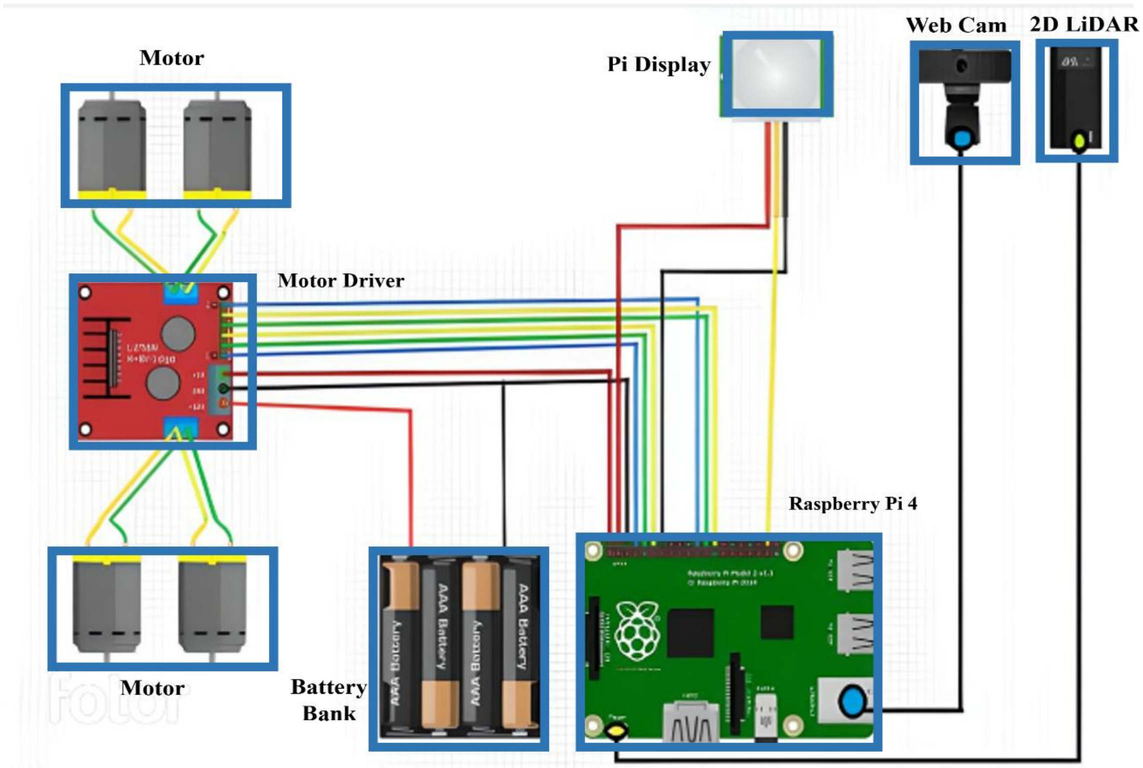


Figure 3.3: Working principle of the Hardware.

In this novel rover system, two separate batteries serve critical roles in powering its many components. The first, a powerful 30000mAh battery, is dedicated to powering the Raspberry Pi 4, which controls the Pi display. This display acts as the visual interface, giving real-time input from the webcam and recording the rover's surroundings. Simultaneously, a second powerhouse appears in the shape of a 50000mAh battery, which is solely dedicated to pushing the rover's six servo motors and wheels. These wheels handle the weight of the whole rover body, ensuring smooth and controlled movement across a variety of terrains.

At the heart of the system is a motor driver circuit that is tightly coupled to a microprocessor. This circuit gets precise instructions from the microcontroller, determining when to start or stop movement and controlling the rover's speed. This thorough orchestration ensures that the Raspberry Pi, motor driver, and servo motors work together seamlessly, allowing for accurate and responsive navigation.

The Raspberry Pi display, in addition to displaying the rover's perspective via the camera feed, is critical for data processing and interpretation. This data is critical to the rover's autonomous navigation capabilities. A LIDAR sensor, strategically positioned to send beams in all directions, rounds out this capability. This LIDAR system functions as the rover's eyes, attentively scanning the surroundings, finding obstructions, and delivering vital data to facilitate obstacle avoidance during autonomous navigation.

3.3. Modeling

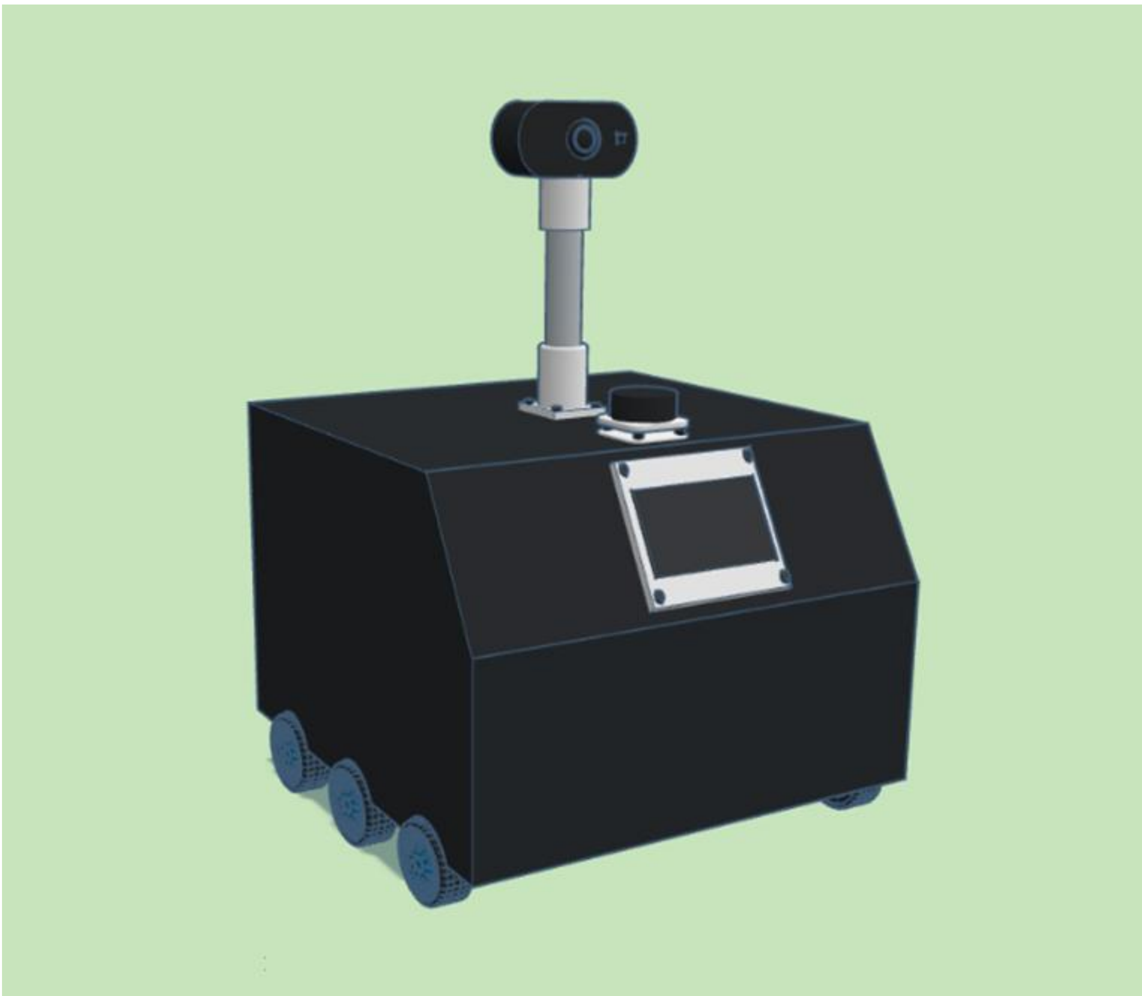


Figure 3.4: 3D Model of the Rover (Front View)

In Figure 3.4 and 3.5, the autonomous navigation system was designed using Fusion 360 software, resulting in a sophisticated 3D model that represents toughness and longevity. The rover's sturdy structure is designed to withstand external forces and potential damage, allowing it to operate seamlessly inside commercial environments.

A 7-inch Pi display, powered by a Raspberry Pi embedded within the rover, takes center stage. This high-resolution display is used as a visual interface to monitor and operate the rover's autonomous functions. A LIDAR is strategically positioned at the rover's top and front, producing beams to detect objects in its surroundings. This technical marvel improves the rover's capacity to navigate successfully, delivering important data for educated decision-making as it moves forward. The webcam, a critical component for visual surveillance, is properly integrated into the rover's design. A precision-engineered platform, perfectly built into the top, allows for height adjustments, allowing the camera to capture clear and unobstructed images. The stand's versatility allows for dynamic adaptation to various conditions, guaranteeing optimal visual data capture. The six wheels beneath the surface push the rover with accuracy and control. These wheels, powered by six motors and delicately managed by a dual motor driver circuit discretely contained within the rover's body, give the rover the locomotion it needs to negotiate varied terrains.

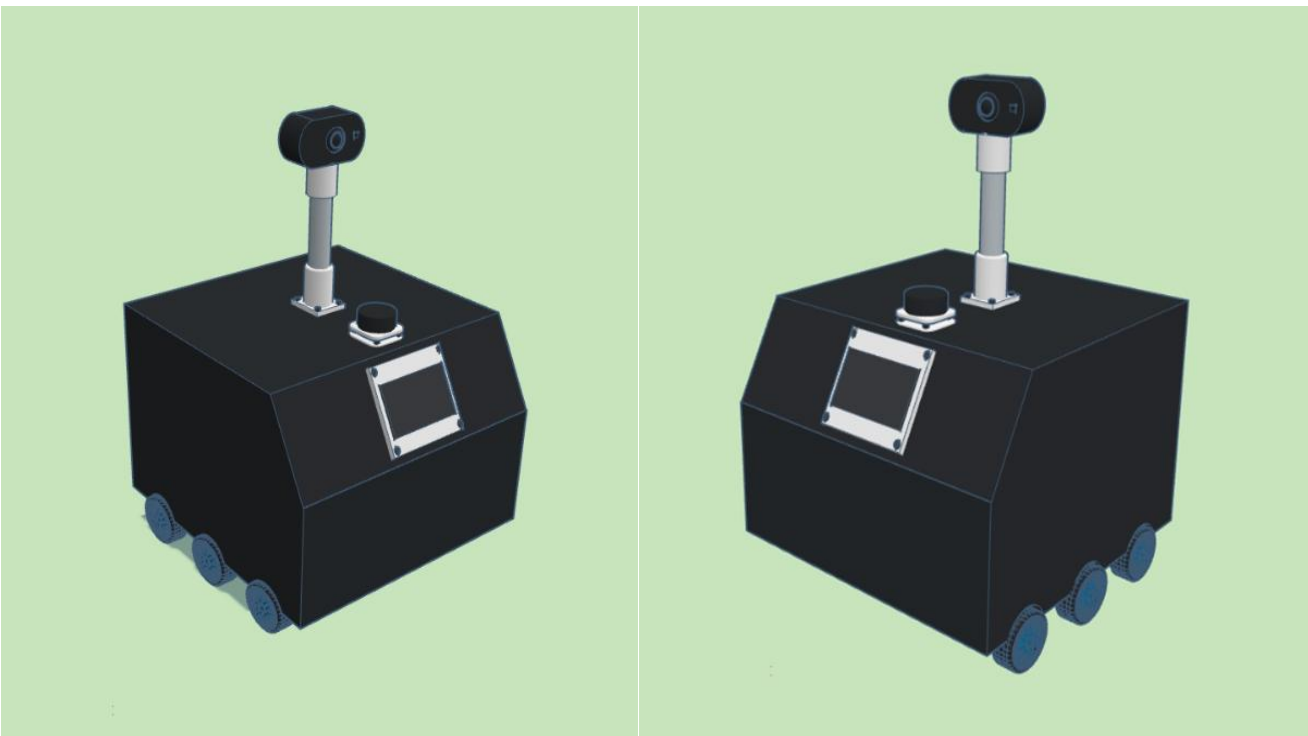


Figure 3.5: 3D Model of the Rover (Both Sides View)

The complete 3D model is precisely constructed, with precise measurements and realistic representations of each component. The Fusion360 software is used to build realistic 3D models of each component, allowing the entire rover system to be constructed. Overall, this 3D model shows the whole system with wheels, servo motors, a web camera with stand, and a LIDAR that are all perfectly incorporated into an efficient and effective design.

3.4. Summary

We summarize the complete process of developing and implementing the system by outlining the approach and modeling of the "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures".

The first part entails developing a robust algorithm, which is a rigorous procedure that includes creating and curating datasets containing the required anomalous items. This recurrent cycle of dataset development and algorithm training necessitates a large amount of data to attain precision and accuracy.

In the second phase, the building of the rover takes center stage, demanding the painstaking assembly of critical components. The difficulty increases as the goal is to develop the rover into an independent creature. Achieving this autonomy necessitates a complicated integration procedure that smoothly incorporates a web camera into the rover's architecture. Notably, the arrangement dynamically expands to incorporate two web cameras linked to a computer serving as a CCTV system, as well as the incorporation of a mobile IP camera for increased surveillance capabilities.

The last phase includes the harmonic integration of hardware and software components, resulting in a synchronized system. This unity allows for continuous communication between the rover and its algorithmic brain, resulting in autonomous activity detection

Chapter 4

PROJECT IMPLEMENTATION

4.1. Introduction

The successful implementation of any project is a very crucial stage that transform the theoretical concepts into Practical solutions. In the context of our project “Anomalous Event Detection for

Enhanced Security in Commercial Infrastructures", this section explores addresses the details in transforming the suggested framework into a workable and deployable system. This section's main objective is to give a thorough overview of the tactics, procedures, and methods used to implement our innovative anomaly detection system.

The security environment for commercial infrastructures has changed dramatically in recent years, necessitating the use of cutting-edge technologies to counter new threats. Our project uses cutting-edge techniques for identifying anomalies to improve security protocols in order to overcome this challenge. As we embark on the implementation phase, it becomes imperative to outline the various components, technologies, and workflows that will be integrated to create a robust and efficient system capable of identifying and responding to anomalous events.

As an essential first step, the simulation phase takes on a fundamental role in starting the project's trajectory. Through the creation of a graphical interface, we clarify the complex dynamics of data flow and component interactions, providing a thorough overview of the operational complexities of the Autonomous robot. As a foundational work, this simulation greatly aids in the development of a plan for in-the-moment execution. It provides priceless insights into how data gathering, analysis, and reaction processes are coordinated, guaranteeing a high degree of security in commercial infrastructures.

The data training procedure for the event detection process happens concurrently with the simulation process. It is just as crucial to develop the appropriate anomaly detection system as it is to obtain our robot's visual representation. These two sections functioned as an essential transitional element, connecting theory and application.

The pivotal phase of our project materializes through the integration of the anomaly detection algorithms with the autonomous navigation system of the robot. The robot's purposeful placement of cameras enables it to function as an eye system that can gather necessary information quickly for analysis. Using smart algorithms, we turn our theoretical ideas into practical tools, finely tuned to spot any unusual events and make sure our system works well in the real world.

This stage represents a paradigm shift in the way that security in commercial infrastructures is approached, acting as the furnace in which theoretical foundations are turned into a workable solution. The "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" project seeks to rewrite security procedures through this thorough execution, bringing in a new era of increased safety and security in the world security and surveillance system.

4.2. Required Tools and Components

4.2.1. Software Tools:

Thonny Python IDE: Thonny is a user-friendly Python Integrated Development Environment (IDE) that prioritizes simplicity for both new and experienced programmers. Its simple interface and built-in Python interpreter make development easier, eliminating the need for additional installations. Thonny's integrated debugger makes troubleshooting easier with features such as breakpoint setting and variable inspection.

We have chosen to program the Raspberry Pi in our project using the Thonny Integrated Development Environment (IDE), with two main goals in mind: autonomous navigation using LiDAR capabilities and the identification of anomalous events using a predetermined algorithm. Python compatibility and Thonny's user-friendly interface have been crucial in helping to write code for these tasks quickly and effectively. Thonny helps to integrate LiDAR data into the Raspberry Pi's control system so that algorithms for accurate path planning and obstacle avoidance can be created for autonomous navigation. In addition, Thonny acts as the programming platform for our proprietary algorithm on the Raspberry Pi, enabling real-time visual data analysis for the purpose of detecting and reacting to unusual events.

Proteus 8 Professional: During the project development phase, we used Proteus to simulate the autonomous robot and evaluate how each component functions and interacts in a simulated setting. Before the robot was physically implemented, we were able to model and simulate its behavior in a variety of scenarios thanks to Proteus, a powerful simulation platform. This simulation made it easier to assess the autonomous navigation system thoroughly and gave insights into the contributions made by various parts, including motor controllers, LiDAR sensors, and navigation algorithms, to the system's overall performance. We were able to test and improve our autonomous navigation strategies with Proteus, which made sure that every component worked together and synchronized in a simulated environment. This approach not only expedited the development process but also proved instrumental in recognizing possible obstacles and refining the auto navigating robot's efficiency prior to its implementation in the real world.

AutoCAD Fusion 360: Our autonomous robot's development was greatly aided by Autodesk Fusion 360. We were able to precisely design and visualize each part of our robot, including the motors, sensors, and chassis, by utilizing its parametric modeling capabilities. The cloud-based collaboration features of the software enabled smooth teamwork by enabling multiple team members to contribute to the design process at the same time. Fusion 360's versatility went beyond simple modeling, allowing us to assess the design's functionalities in addition to its aesthetics. The robot's physical construction was guided by the 3D models created in Fusion 360, which also ensured that the structural integrity and spatial relationships of every component were carefully verified prior to fabrication.

4.2.1.1. Libraries

In Python development, a library is a collection of pre-written code modules or functions that provide a variety of resources to help and expedite the coding process. These libraries are designed to integrate seamlessly into Python projects or scripts, eliminating the need for developers to build everything from the ground up. Python libraries cover a wide range of topics, including data manipulation, scientific computing, machine learning, and image processing. Each library specializes in a specific field, providing readily usable functions, classes, and methods that can be easily incorporated into Python scripts, promoting efficiency and code reuse.

TensorFlow: TensorFlow, an open-source machine learning framework created by the Google Brain team, is built on several foundational theories. TensorFlow's key component, neural networks, are inspired by the human brain and are made up of layers of interconnected nodes. The framework supports a variety of neural network architectures, such as Convolutional Neural Networks (CNNs) for image-related tasks and Recurrent Neural Networks (RNNs) for serial data processing.

Our project relies on TensorFlow, an open-source machine learning framework developed by the Google Brain team, to train data for detecting anomalies. TensorFlow is built on the foundational concept of tensors, representing multidimensional arrays crucial for data manipulation. Its dynamic computational graph enables efficient execution of complex machine learning models. In our implementation, TensorFlow's versatility and adaptability empower us to design and train models capable of discerning patterns associated with anomalous objects. This choice facilitates seamless integration, allowing our system to efficiently learn from diverse datasets and contribute to the success of our anomaly detection project.

GPIO: In our rover project, Thonny Python's GPIO library became instrumental in precisely controlling servo motors. We rigorously tested the rover's movements and fine-tuned sensor readings using GPIO operations. The library's flexibility allowed us to seamlessly debug and make necessary adjustments, ensuring optimal hardware control. This hands-on approach not only streamlined development but also revealed the intricate interplay between software and the rover's components.

Mediapipe: We improve our object detection and anomaly identification tasks in our project by utilizing the capabilities of the MediaPipe library. Google created MediaPipe, a flexible library for creating multimodal pipelines that is especially useful for real-time processing of visual data. We were able to incorporate pre-built elements like hand tracking, object detection, and pose estimation thanks to its modular architecture, which made it easier to extract important features from a variety of visual inputs. Our anomaly detection system gained important insights into the spatial relationships and object movements within the visual data by integrating MediaPipe. The library's efficiency and ease of use contribute to the seamless integration of these components, ultimately improving the accuracy and robustness of our system in identifying anomalous objects based on their dynamic visual characteristics.

OpenCV: Our project relies heavily on OpenCV, an open-source computer vision library that improves our capacity for processing and analyzing visual data. OpenCV is a crucial part of our anomaly detection system because of its extensive tool and algorithm library, which makes it possible to use it for a variety of computer vision applications. For tasks like object recognition, feature extraction, and image preprocessing, we use OpenCV. With its vast array of filtering, transformation, and image manipulation functions, we can improve the visual data quality prior to feeding it into our detection models. OpenCV's ability to support a wide range of computer vision algorithms, such as contour analysis, edge detection, and object tracking, enables our system to efficiently recognize and decipher patterns in the visual input. Our anomaly detection solution's flexibility and accessibility are further enhanced by the library's cross-platform compatibility and integration with languages like Python.

Requests: The requests library is crucial for our project because it allows smooth communication between various components and outside services. Requests is a Python library that makes submitting HTTP requests easier, facilitating effective communication between our system and outside web services and APIs. For tasks like retrieving external data, submitting requests to cloud-based services, or integrating with online resources, this capability proves to be indispensable. We used the request library to connect with server to send the information of the detected anomalies. The requests library enhances the overall functionality and connectivity of our anomaly detection system by allowing us to programmatically handle HTTP protocols, control authentication, and communicate with external servers. This library's ease of use and adaptability make it a useful tool for expediting our project's data retrieval and communication procedures.

4.2.2 Hardware Components

Raspberry Pi: The central brain of our rover is powered by a Raspberry Pi. Specifically, we've opted for the Raspberry Pi 4 Model B with 4GB of RAM due to its convenient and user-friendly nature. For our project focused on identifying unusual activities, we've harnessed the power of this compact computing device. Our code, crafted using Thonny Python, finds its home within the Raspberry Pi.

Raspberry Pi is connected to three components. These are Webcam, LCD Display, LiDAR. Within the rover, the Raspberry Pi takes on a dual role. Firstly, it assumes control over the LiDAR system. Secondly, it engages in image processing to pinpoint any abnormal activities. Once anomalies are detected, the Raspberry Pi swiftly communicates this information to the server, ensuring a seamless flow of data for analysis and response.

ESP32: To enable seamless control of our rover, we've implemented the ESP32 for Bluetooth functionality. This feature allows us to wirelessly initiate and halt the servo motor's operation. The ESP32 acts as a reliable interface, providing the convenience of remote control for starting and stopping the rover's servo motor with just a simple Bluetooth command.

LCD Display: In our rover system, we've integrated a 7-inch LCD display for a comprehensive user interface. This display serves as a visual platform where we can observe, manage, and input Python code directly into the Raspberry Pi.

LiDAR: Within our rover design, we've integrated a Lidar system crucial for obstacle detection. This Lidar operates by emitting laser beams in a complete 360-degree span, thoroughly scanning the rover's surroundings. As these laser beams encounter obstacles, they bounce back to the Lidar sensor.

Buzzer (Active): We've incorporated a 5V active buzzer into our setup, connecting it to the ESP32. The purpose of this buzzer is to act as an alert mechanism. In the event that the Raspberry Pi detects any form of abnormal activity, the buzzer is triggered and turns on.

Webcam: In our project configuration, we've integrated three webcams for comprehensive surveillance. The primary webcam is affixed to the top of the rover, while the other two are strategically positioned as similar as CCTV cameras in distinct locations. The collective purpose of these webcams is to identify any abnormal activities in the rover's surroundings.

Motor Driver Circuit: To regulate the speed of the six servo motors in our system, we've employed two motor driver circuits. These circuits play a pivotal role in controlling the functionality and speed of the servo motors.

LiPO Battery Bank: Our rover is powered by a pair of LiPo (Lithium Polymer) battery banks, each serving a specific purpose. The first, a robust 50000mAh unit, takes charge of energizing the six servo motors, ensuring their smooth operation. Meanwhile, the second battery bank, with a capacity of 30000mAh, is dedicated to powering the Raspberry Pi and a 7-inch LCD display.

4.3. Implemented Model

The "Anomalous Event Detection for Security Enhancement of Commercial Infrastructure" project signifies an important milestone in the field of electrical and electronic engineering security technology. Carefully crafted to enhance the security and effectiveness of commercial infrastructure, this novel system is a complex tapestry woven with predictive models and state-of-the-art instruments.

Fundamentally, this system keeps a close eye on important factors in real time, like the identification of unusual occurrences, to guarantee a safe and smooth functioning. By utilizing cutting-edge image processing technologies, the integrated models exhibit forecasting and decision-making precision that has never been seen before. Specially designed to break down complex data, these models allow for quick reactions to possible security threats, increasing the safety factor overall.

In addition to its critical security improvements, the system performs a delicate dance of optimization in commercial infrastructure, reducing interference through prudent security protocol management based on real-time assessments. This is an amazing example of how engineering principles and predictive analytics can work together, greatly improving the efficiency and safety of commercial spaces. The cleverness of electrical and electronic engineering is demonstrated by the seamless integration of this cutting-edge system, which tackles critical issues in protecting and strengthening the robustness of our business infrastructure.

4.3.1. Simulation Model

The dynamic perform of real-time data captured by the camera holds the true meaning of the project, which defies simulation. It carefully sorts through this data, carefully piecing together the anomalous fabric. The graceful choreography of the auto-navigating robot is demonstrated by our simulation, which is a symphony created by the harmonious interaction of technology with the constantly changing world it lives in.

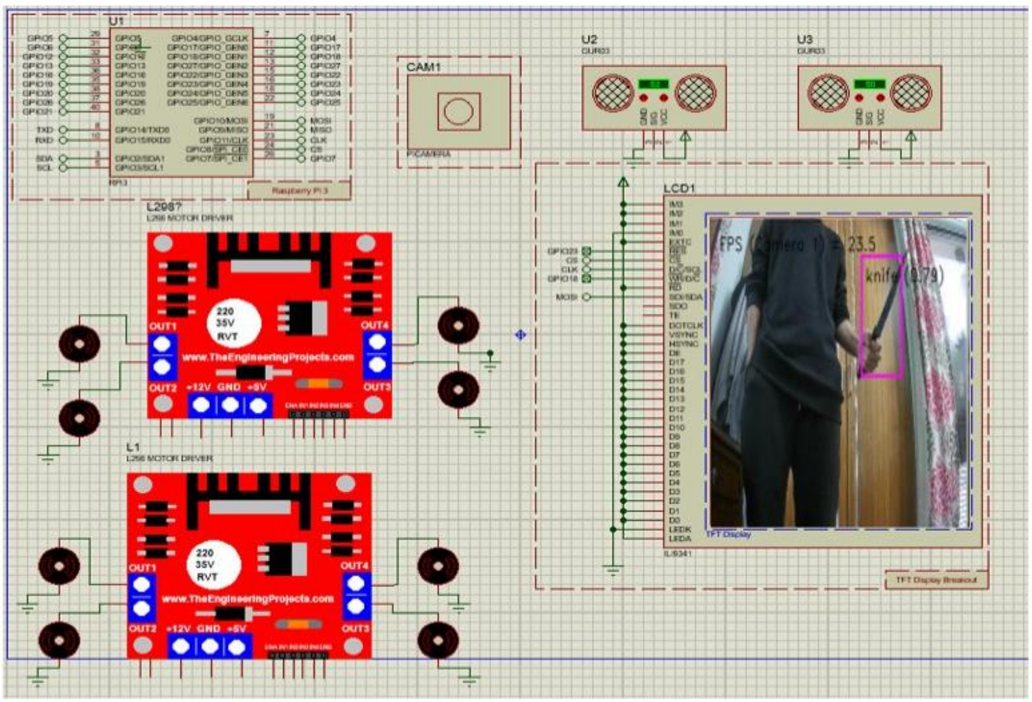


Figure. 4.1: Proteus simulation of the system

The rover is intricately designed with a Raspberry Pi 4 GB at its core, leveraging a lidar sensor for sophisticated autonomous navigation and a webcam to employ artificial intelligence for anomaly detection within commercial infrastructures. To ensure robust operation, the rover is powered by two LiPo batteries a 30000mAh battery dedicated to running the Raspberry Pi and the display, and a separate 50000mAh battery specifically tasked with powering six stepper motors interconnected through two motor driver circuits. Additionally, an ESP32 module is integrated into the system to serve as Bluetooth switches, providing a convenient means to activate the rover remotely.

4.3.2. Hardware Model

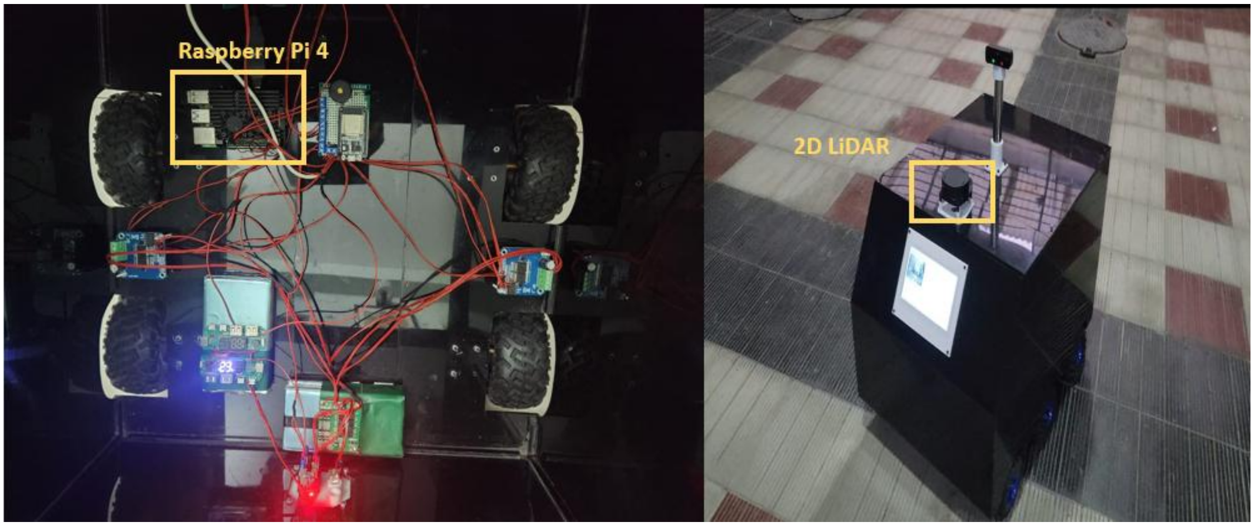


Figure. 4.2**:** Raspberry pi and LiDAR of the rover

The Raspberry Pi facilitates autonomous rover navigation by interfacing with a 2D LiDAR sensor. Processing real-time data from the LiDAR, the Raspberry Pi enables the rover to make informed decisions, ensuring dynamic and obstacle-aware movement. This integration forms a robust system for precise and autonomous navigation in varied environments.

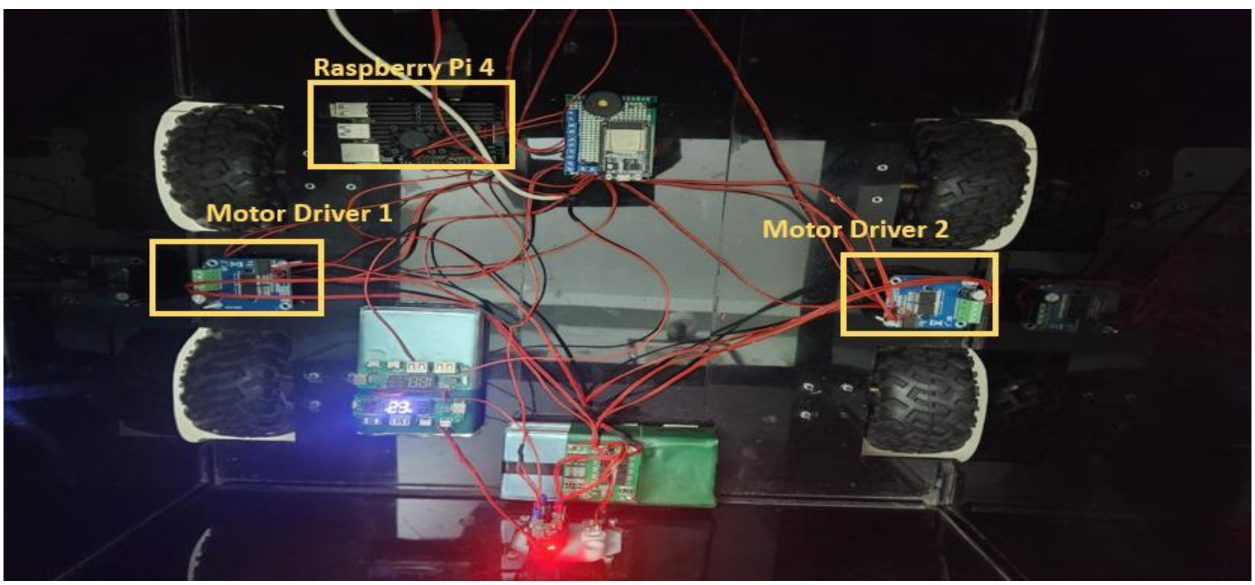


Figure 4.3: Raspberry pi and Motor Driver of the rover

Guided by LiDAR data, the Raspberry Pi controls the rover's movement through two motor drivers, each managing three motors. These motor drivers interpret directional input from the Lidar, translating it into precise commands for the six motors. This integration allows the rover to dynamically adjust its movement, ensuring responsive and accurate navigation based on the environmental feedback received from the LiDAR sensor, showcasing a sophisticated control system for autonomous mobility.

Figure 4.4: Raspberry pi and Web cam of the rover

The Raspberry Pi connects to an AI-equipped webcam for instant recognition of guns, knives, and smoking. Detected images are promptly sent to a web server, fortifying security by enabling quick identification and centralized management of potential threats through seamless communication.

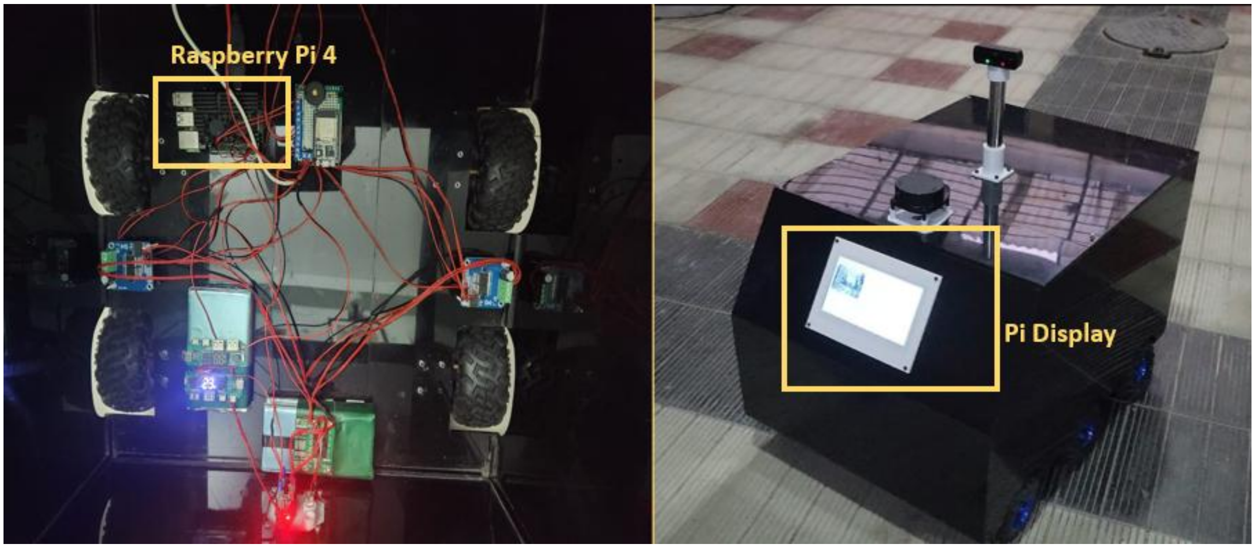


Figure. 4.5: Raspberry pi and Pi display of the rover

The AI program runs on the connected display, utilizing the Raspberry Pi's processing power. This setup enables real-time analysis and display of detected anomalies, enhancing situational awareness by presenting immediate visual feedback on threats like guns, knives, and smoking.

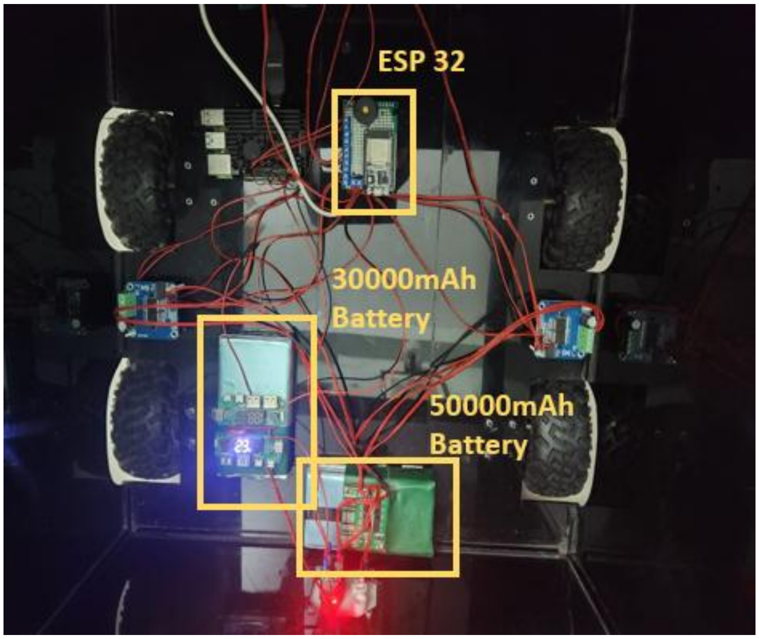


Figure. 4.6: Power supplies of the rover

The rover operates on a dual-battery system, comprising a 30,000mAh and a 50,000mAh battery. This design ensures extended operational endurance, allowing the rover to perform autonomously for prolonged periods by efficiently managing power consumption with the combined capacity of both batteries.

Figure. 4.7: Front View and Side View of Rover

The system is programmed to initiate forward movement only when the Lidar sensor does not detect any obstacles within its scanning range. In practical terms, this means that as the rover navigates its environment, it continuously assesses the data from the Lidar sensor. If the sensor signals the absence of obstacles in the rover's intended path, the control system activates the forward movement, allowing the rover to autonomously proceed while actively avoiding detected obstacles.

Figure 4.8: Autonomously Moving Forward

Upon analysis of Lidar data, if the sensor identifies obstacles ahead, the control system triggers a rightward maneuver. This decision-making process is designed to enable the rover to autonomously navigate around obstacles, showcasing the adaptability and responsiveness of the system in the face of impediments, ultimately ensuring a safer and more efficient traversal of its environment.

Figure 4.9: Autonomously Moving Right

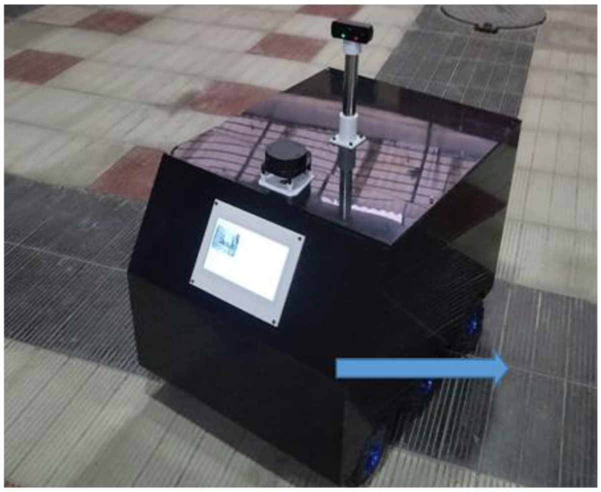


Figure 4.10: Autonomously Moving Left

It is programmed to initiate a leftward movement when obstacles are detected both in the frontal and right directions. Upon processing Lidar data, if the sensor identifies obstacles in these specific areas, the control system triggers a leftward maneuver. This strategic decision allows the rover to autonomously navigate around obstacles by moving to the left, showcasing its ability to adapt to complex environments and ensuring obstacle avoidance in the specified directions for enhanced safety and efficiency.

4.4. Summary

The implantation of the "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" ends practical execution of the proposed solution. To fortify security in commercial infrastructures, the implementation involves deploying advanced anomaly detection techniques. The project utilizes cutting-edge technologies such as machine learning algorithms, cameras, and data analytics to continuously monitor and analyze diverse data sources. Implementation steps include the integration of anomaly detection models into existing security systems, and also creating an autonomous robot integrated with cameras, establishment of a robust data pipeline, and the deployment of real-time monitoring solutions.

The pivotal success of this project, is anchored in the system's adeptness at making swift, data-driven decisions in real-time. When an anomalous event unfolds within the commercial infrastructure, the automated detection mechanisms promptly initiate responsive actions, fortifying security measures. Because of the system's flexibility, it can be implemented widely and efficiently in a variety of commercial environments. The project intends to improve the overall security resilience of commercial infrastructures by reducing risks and protecting vital assets through real-time monitoring and quick response mechanisms.

Chapter 5

RESULT ANALYSIS & CRITICAL DESIGN REVIEW

5.1. Introduction

The "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" paper's Results Analysis & Critical Design Review section evaluates the proposed model's efficacy and capacity to handle the intended issues. To achieve these findings, some thorough strategies were used.

This advanced security system project efficiently combines several software and hardware components. The project provides code authentication, simulation, and circuit integrity by using industry-standard tools like the Thonny Python IDE and the Proteus Design Suite. The Raspberry Pi 4B is the primary CPU, rigorously picked for its specs, while the camera and lidar specifications are thoroughly validated.

Python programming, with TensorFlow and mediapipe libraries, enables the creation of a wide range of security measures, such as image processing and motion tracking. The integration extends to an autonomous rover with servo motors for wheel control, which ensures accurate mobility. The success of the project depends on the careful measurement and verification of each parameter, assuring optimal performance and giving a unique solution at the junction of hardware and software.

After gathering all of the essential traditional data, we began real-time data collecting. The outcomes were what we expected. The results showed the following outcomes:

- **High Accuracy in Anomaly Detection:** The experiment demonstrates extraordinary accuracy in identifying abnormal things including weapons, knives, and smoking. It required extensive training with various datasets improves the algorithm's grasp of aberrant patterns.
- **Real-Time Response Speed:** A swift and quick response to anomalous behaviors guarantees that appropriate actions are done. Real-time reporting to the web server ensures that users receive quick messages, which improves overall situational awareness.
- **Multiple Camera Monitoring:** The integration of multiple cameras improves the project's surveillance capabilities by offering a complete and panoramic picture of its surroundings. This multi-camera arrangement improves detection accuracy and allows more sophisticated investigation of anomalous events in commercial areas.
- **Multiple Anomalous Object Detection:** The project's effective algorithm shows the remarkable capability to recognize numerous abnormal objects within the same video

frame. This concurrent detection capability increases the system's efficiency in detecting and responding to various security threats in real-time.

- **Comprehensive User Interface:** The web server offers users with a complete interface that displays the time and incidence of abnormal occurrences. Users may quickly access and evaluate data, enabling more informed decision-making and increasing security standards.
- **Seamless Autonomous Navigation:** The autonomous rover effectively navigates commercial environments, proving the algorithm's real-world effectiveness.It interacts with the same algorithm, ensuring constant and reliable anomaly detection capabilities during rover patrols.

5.2. Result Analysis

The "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" has produced impressive results, but a closer look uncovers certain abnormalities that require addressing. These conclusions were achieved by analyzing the system's performance under various scenarios.

Firstly, the system is built on a trained algorithm that was developed after prolonged exposure to a variety of datasets containing anomalous objects such as weapons, knives, and smoking incidents. The program has learned to recognize and respond to these specific items after a thorough learning procedure. The system interacts with its surroundings fluidly, relying on its taught understanding, notably through the lens of its camera. The system applies its accumulated experience in real time, applying a unique frame-by-frame analysis that allows for quick and precise identification. Notably, it goes beyond simple recognition, using its camera vision to carefully square label any identified abnormal things.

Secondly, the rover equipped with the same powerful camera system, navigates commercial environments autonomously and is completely connected with the algorithm designed to identify anomalies. As the rover moves across commercial settings, its camera, coordinated with the predefined algorithm, performs continuous surveillance. When aberrant items are detected, the rover responds quickly and decisively. This dynamic approach guarantees that the rover becomes an active and watchful security presence, monitoring commercial places autonomously and responding quickly to possible threats.

All identified anomalous behaviors are instantly forwarded to a dedicated web server, resulting in a more efficient channel for user access. This comprehensive method allows users to easily trace the recurrence of abnormal occurrences, pinpointing both the precise time and the specific day on which they occurred. This rapid data transfer not only provides prompt documenting of abnormal occurrences, but it also serves as an important component in developing safety measures and triggering timely user notifications.

5.2.1. Simulated Result

Simulation usually refers to a specific software or environment where the entire project may be simulated before being implemented in hardware. The project model may be examined in a simulator, with outcomes comparable to those anticipated from the hardware. However, since our project primarily aimed to analyze and detect anomalous objects or events in real time, the use of simulating software was not suitable. Instead, we employed Thonny to train the dataset to align with the real-time information obtained from the camera. Initially, this simulation was conducted on a laptop and later implemented on the Raspberry Pi. The project underwent testing under various conditions, using different objects as models for the test cases. The following is a list of the test cases:

i. Detection of Gun using Single Camera
ii. Detection of Gun using Multiple cameras at the same time
iii. Detection of Knife with single camera
iv. Detection of Knife with multiple cameras at the same time
v. Detection of Cigarette with single camera
vi. Detection of Cigarette with Multiple cameras at the same time
vii. Detecting Multiple Object same time with Different Cameras

Detection of Gun using Single Camera: Using only one camera, the system can detect a gun with ease from different perspectives. It also proves that it can recognize the item in changing circumstances. Because the CNN method uses pre-trained data, the system recognizes the item quickly and with minimum processing time. This is an impressive level of efficiency.

Figure 5.1: Detection of Gun using Single Camera at gate and room

Figure 5.2: Detection of Gun using Single Camera at garage

Detection of Gun using Multiple cameras at the same time: When detecting a gun using multiple cameras simultaneously, the system exhibits success. It demonstrates the ability to recognize the gun concurrently with both cameras, and there is no significant delay in the process.

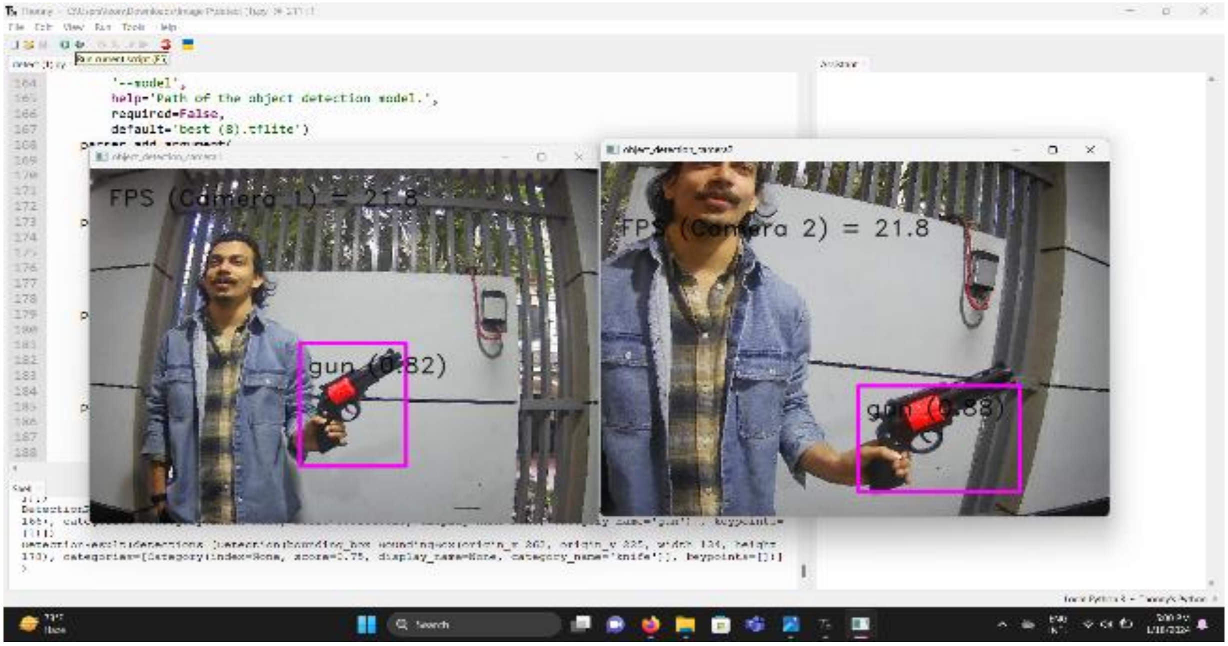


Figure 5.3: Detection of Gun using Multiple cameras at the same time at garage

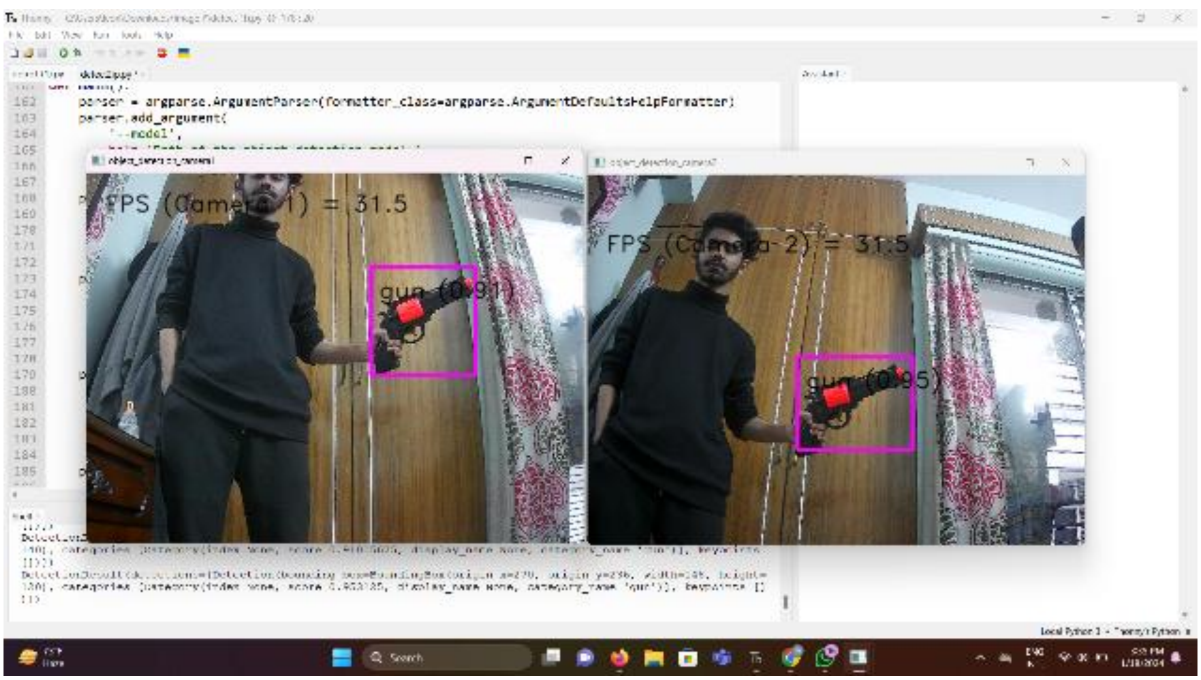


Figure 5.4: Detection of Gun using multiple cameras at the same time at room

Detection of Knife with single camera: Detecting knives posed a significant challenge due to their nature. The shiny surface of the knives reflects light, causing variations in the RGB values captured by the camera. This made it challenging to match these values with the pre-trained data for knife detection. Despite these difficulties, the system impressively achieves a very high success rate in rapidly detecting knives with single camera.

Figure 5.5: Detection of Knife with single camera at room and garage

Detection of Knife with multiple cameras at the same time: Using numerous cameras at the same time makes knife detection a little trickier. Each camera experiences a varied influence from the angle of light fluctuation on the RGB values, leading to somewhat bigger input data. Consequently, there is a slight lag in the simultaneous detection of knives using both cameras.

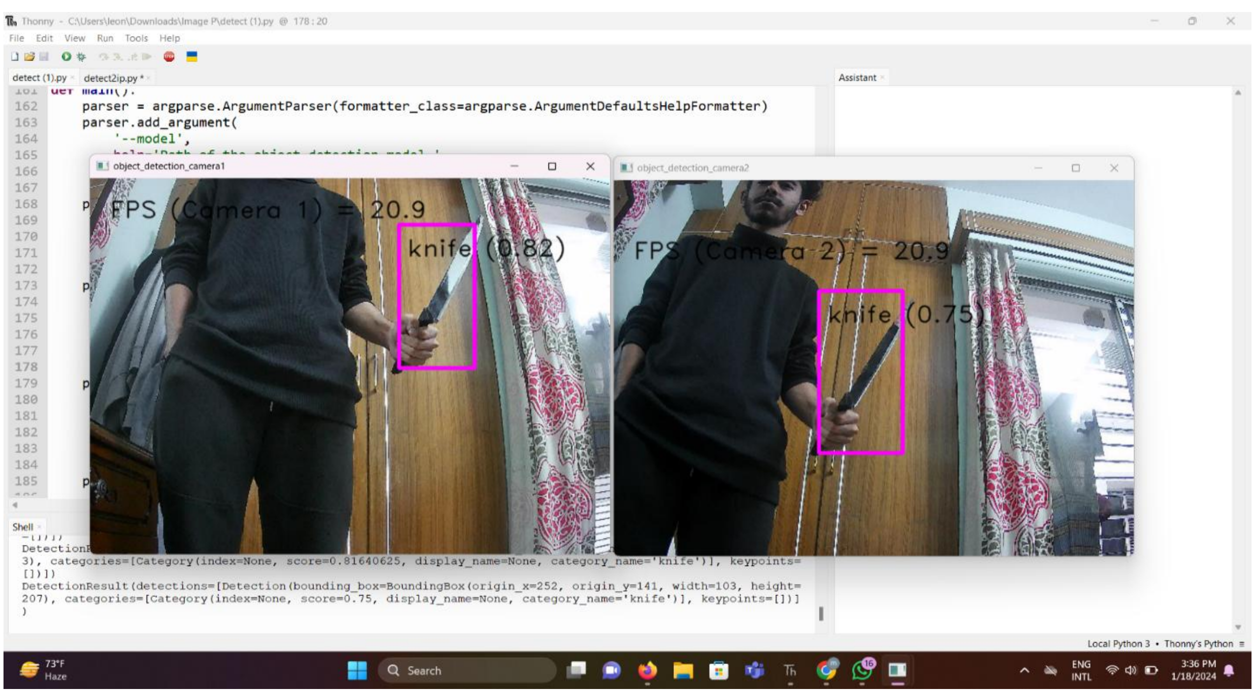


Figure 5.6: Detection of Knife with multiple cameras at the same time at room

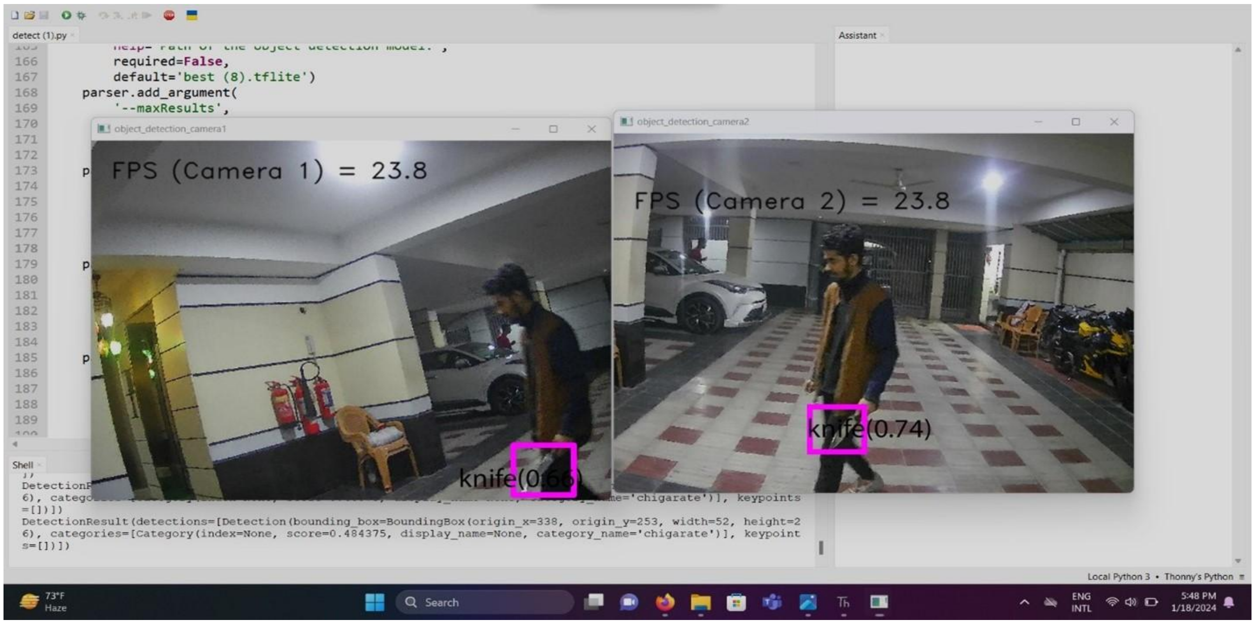


Figure 5.7: Detection of Knife with multiple cameras at the same time at garage

Detection of Cigarette with single camera: The hardest part turns out to be finding the cigarettes. Since most cigarettes are white in color, it becomes challenging to match their RGB values for identification. The detecting procedure becomes more challenging when many sections of the same size and RGB values are present. Still, the system performs almost as well when detecting items with a single camera as it does when detecting other objects.

Detection of Cigarette with Multiple cameras at the same time: When recognizing objects with many cameras, the system shows a modest decline in accuracy. Occasionally, in test circumstances, it detects items or tiny regions that have RGB values comparable to cigarettes, which might cause some detection errors.

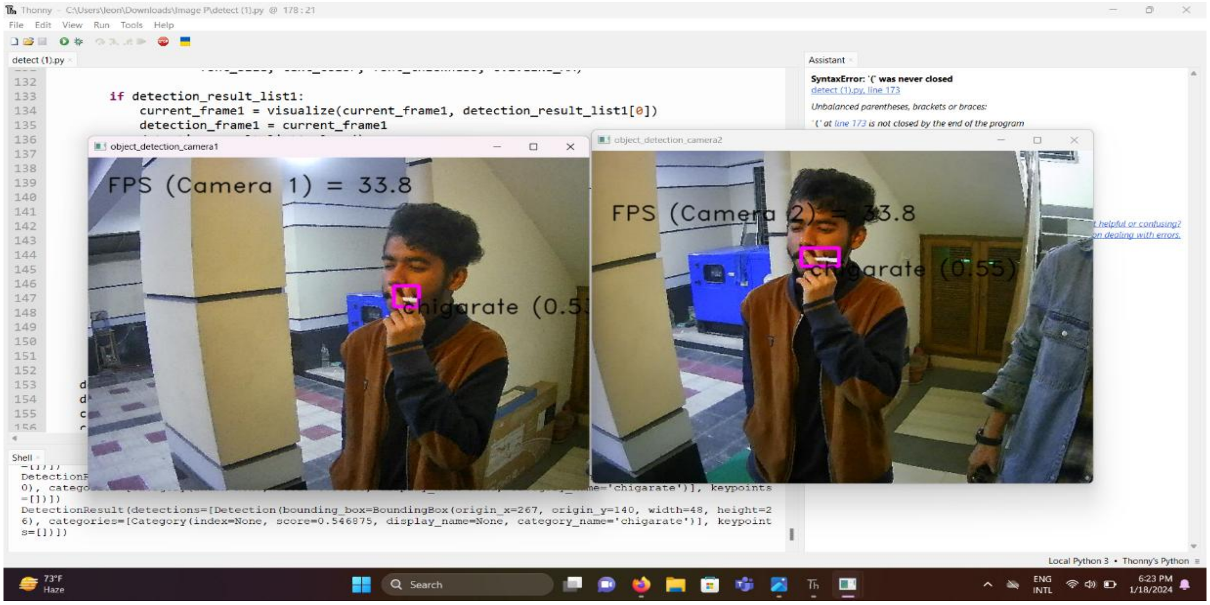


Figure 5.9: Detection of Cigarette with Multiple cameras in front of lift

Detecting Multiple Object same time with Different Cameras: As the number of cameras increases, the volume of input data also rises, leading to a substantial increase in computational workload and a slight delay.

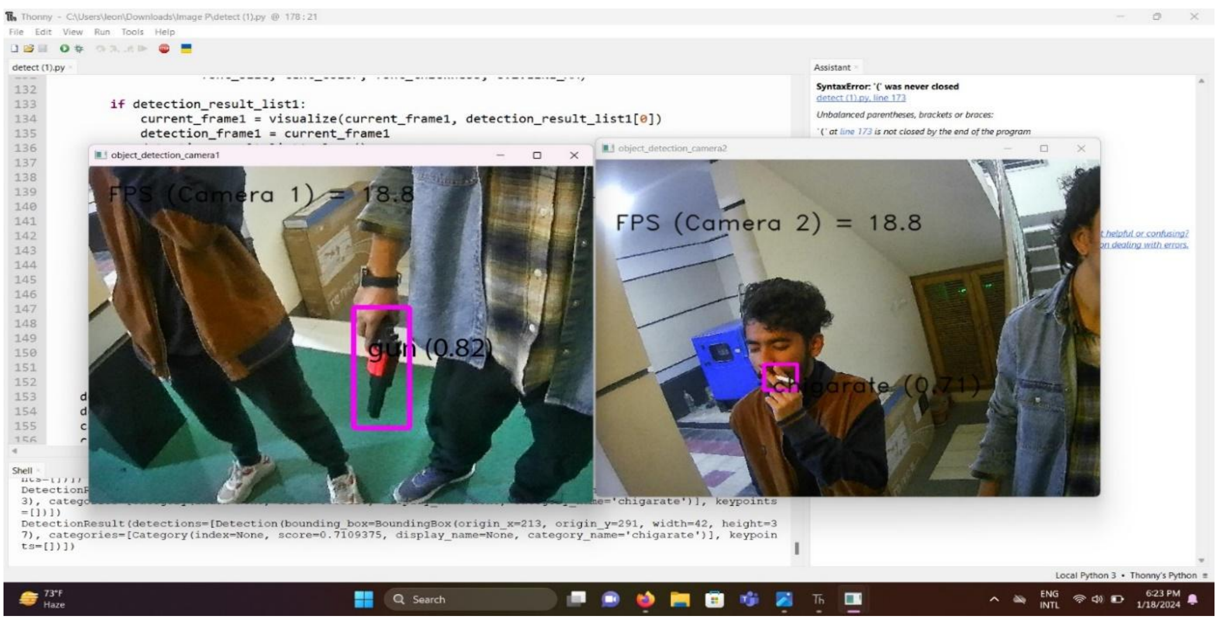


Figure 5.10: Detecting Multiple Object same time with Different Cameras in front of lift

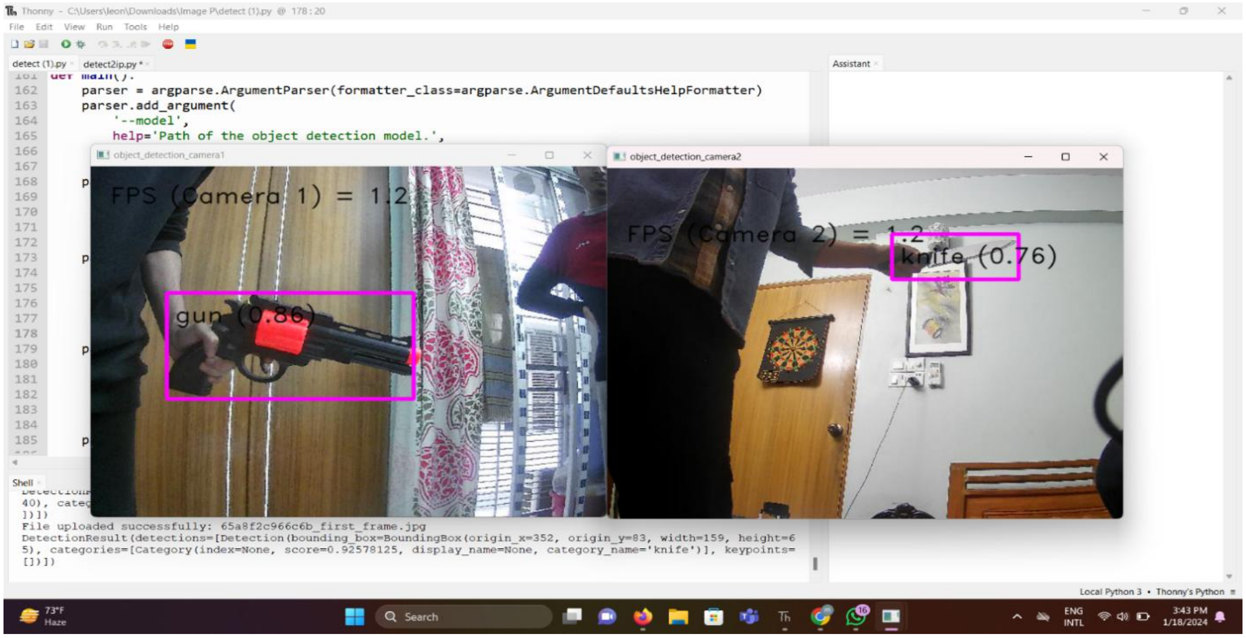


Figure 5.11: Detecting multiple object same time with Different cameras at room

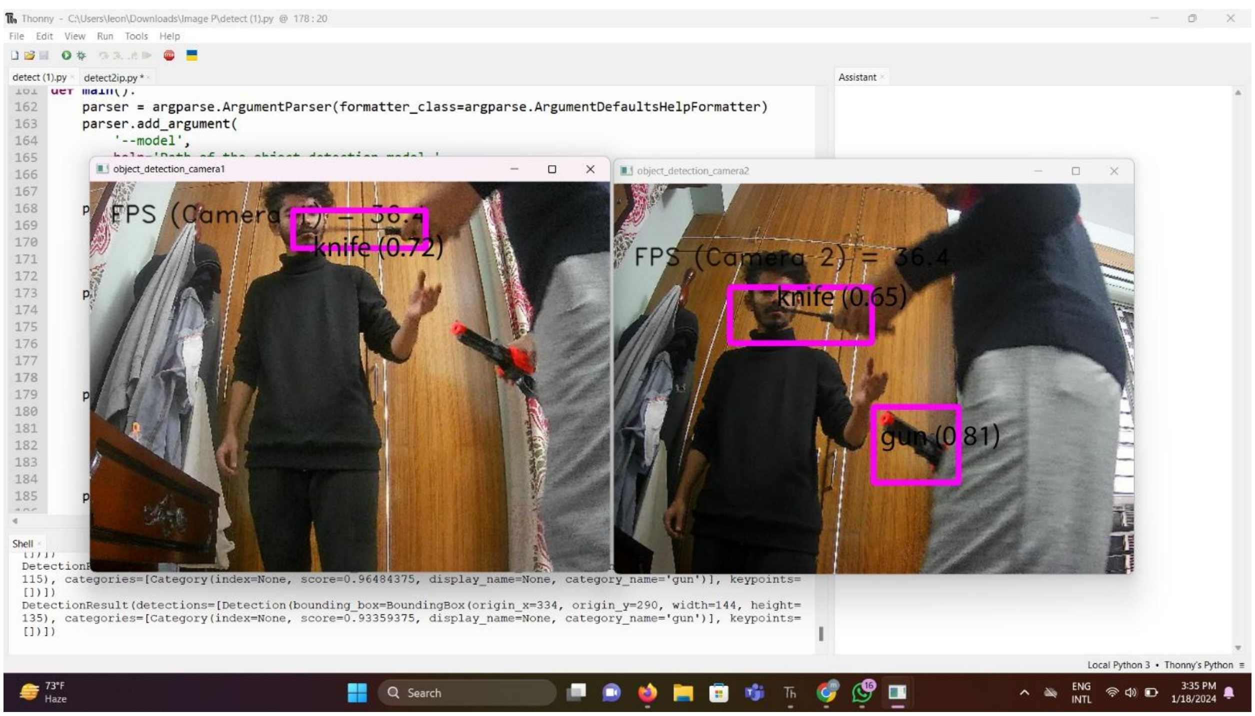


Figure 5.12: Detecting multiple objects in same frame at the same time with Different cameras at room

Web Server:

The surveillance system has the capability to identify instances of gun, knife, and smoking activities. It then sends the recorded data to a pre-designated website as soon as it detects such behaviors. The pertinent data is immediately sent to the internet for storage and retrieval as soon as the system detects any of these behaviors using the cameras. By taking a proactive stance, possible safety issues or security threats are quickly reported to the appropriate platform. The website's storage of this data facilitates effective categorization and analysis, allowing for prompt notifications to relevant parties. Visitors to the website can remain updated about detected activity, which promotes increased security and makes it possible to react quickly to possible threats. The smooth connection between web-based notification and detection improves the system's overall efficacy in delivering alerts in real-time.

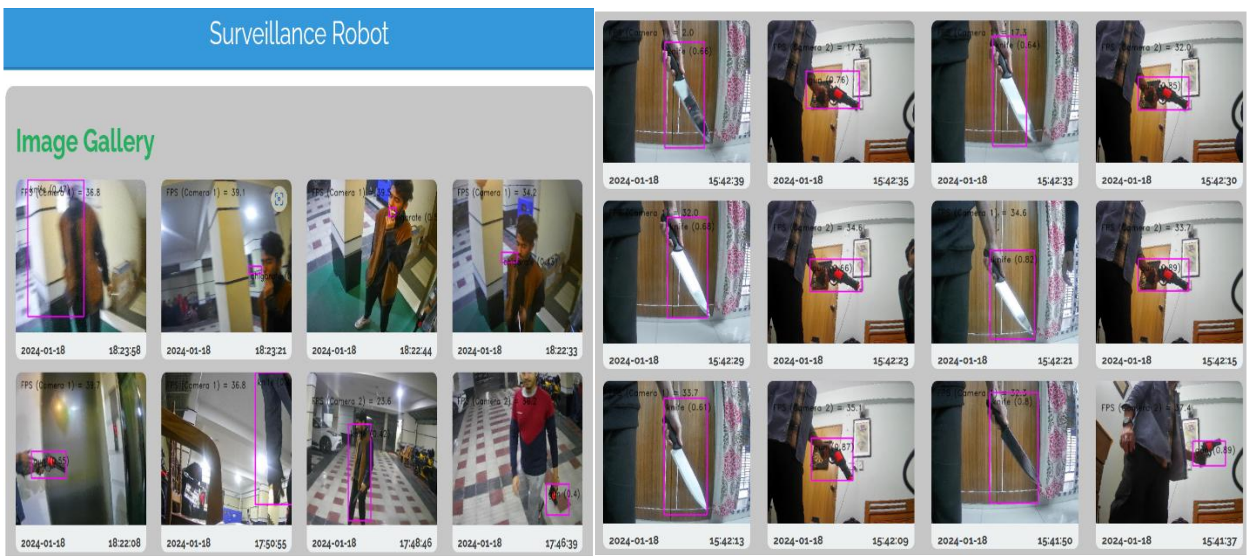


Figure 5.13: Web server gallery

5.2.2. Hardware Result

The autonomous rover served as the primary hardware component in this project, and its implementation was highly successful. The rover successfully embodies the anticipated functionality, operating in accordance with the plan that was envisioned throughout the project's planning phase.

The rover utilizes LiDAR technology to generate a virtual map and assess the presence of obstacles in its path. The rover moves ahead in the event that it detects no obstructions. The rover, however, alters course if an obstruction is detected 20 cm ahead of it. The rover performs almost flawlessly in our testing, identifying objects and changing its trajectory accordingly.

Detection of knife with the rover: When identifying knives with the rover camera, the system has some difficulties that cause the accuracy of knife recognition to slightly drop when compared to other circumstances.

Figure 5.14: Detection of Knife with the rover at room

Detection of Gun with the Rover: The data obtained from the camera installed on the rover is dynamic by nature, as it is a mobile instrument. In spite of this difficult circumstance, the system has good success rates in identifying firearms and completes the work in the least amount of time.

Figure 5.15: Detection of Gun with the rover at garage

Detection of Smoking with the Rover: The rover's camera, driven by an improved algorithm, had an astonishing capacity to detect even small objects, as seen by its accurate recognition of cigarettes during smoking episodes. The complicated color gradient patterns associated with such things made the task even more difficult. Despite its complexity, the revised algorithm demonstrated extraordinary competency, allowing the system to detect and reliably identify tiny, finely patterned items such as cigarettes.

Autonomous Navigation Ability:

Our rover can detect obstacles by using the 2D LiDAR. LiDAR plays a crucial role in autonomous vehicles for obstacle detection and navigation. LiDAR systems emit laser pulses and measure the time it takes for the light to return after bouncing off objects. In our rover, if the 2D LiDAR finds any obstacles in the 25cm range it will go its left side as it’s first priority.

5.3. Comparison of Results

The project's success depends on a careful comparison of its results with those of current systems, demonstrating the superiority of the created solution. Our assessment concentrated on the ability to identify dangerous things while providing benchmark data. Our system's accuracy was evaluated in relation to the number of cameras used, proving its effectiveness when configured optimally. Furthermore, the system's real-time capabilities which are critical for security applications were highlighted by comparing detection times as a means of assessing responsiveness. In addition, we evaluated the system's adaptability by determining the greatest detection range that maintains accuracy. These comparisons demonstrated how consistently our system outperformed its competitors, demonstrating how important it is to advance security measures in commercial infrastructures. These thorough assessments were taken into consideration in this section.

Distance Comparison with anomalous objects:

Table 5.1: Gun Detection Distance Coverage by Cameras

Distance Coverage (Meters)	**Computer-integrated CCTV camera**	**Rover Camera**	**Mobile IP Camera**
0.1	Instant Detection	Instant Detection	Instant Detection
0.5	Instant Detection	Instant Detection	Instant Detection
1	Instant Detection	Instant Detection	Instant Detection
1.5	Instant Detection	Instant Detection	Instant Detection
2	Instant Detection	Instant Detection	Instant Detection
2.5	Instant Detection	Instant Detection	Almost instant Detection
3	Instant Detection	Instant Detection	Almost instant Detection
3.5	Instant Detection	Almost instant Detection	Slight delay Detection
4	Almost Instant Detection	Slight delay Detection	Delay Detection
4.5	Slight Delay Detection	Delay Detection	Delay Detection
5	Delay Detection	Delay Detection	No Detection

The variation in detection speed among cameras is likely due to differences in their resolutions. Short distances allow for clearer details, enabling instant recognition, while longer ranges may require more processing time for accurate analysis. The rover excels at close-range detection, suggesting superior optics and the IP camera's swift detection within 2.5m indicates high-resolution capabilities. Achieving a balance between detection speed and accuracy involves optimizing algorithms to accommodate the specific specifications of each camera in the system.

Table 5.2: Knife Detection Distance Coverage by Cameras

Distance Coverage (Meters)	**Computer-integrated CCTV camera**	**Rover Camera**	**Mobile IP Camera**
0.5	Instant Detection	Instant Detection	Instant Detection
1	Instant Detection	Instant Detection	Instant Detection
2	Instant Detection	Instant Detection	Instant Detection
3	Instant Detection	Almost instant Detection	Delay Detection
4	Almost instant Detection	Slight delay Detection	Hardly Detect
5	Delay Detection	Delay Detection	No Detection

Resolution and focal length discrepancies could be the cause of the discrepancy in detecting ability between cameras. Due to the clarity of details, knives can be instantly detected at close range. When the CCTV camera is farther away than 4 meters, it lags, probably because of decreased clarity. The rover performs really well at 3 meters, suggesting excellent optics, while the IP camera detects objects quickly at 4 meters, suggesting excellent resolution. The difficulties presented by differing distances and camera capabilities in surveillance systems must be addressed in order to optimize algorithms to take each camera's specs into account and strike a balance between accuracy and speed.

Table 5.3: Smoking Detection Distance Coverage by Cameras

Distance Coverage (Meters)	**Computer-integrated CCTV camera**	**Rover Camera**	**Mobile IP Camera**
0.5	Instant Detection	Instant Detection	Instant Detection
1	Instant Detection	Instant Detection	Instant Detection
2	Instant Detection	Instant Detection	Almost instant Detection

3	Almost instant Detection	Almost instant Detection	Delay Detection
4	Delay Detection	Hardly Detect	No Detection
5	No Detection	No Detection	No Detection

The CCTV camera excels within 3 meters for instant smoking detection but experiences delays beyond that range due to potential reductions in clarity. The rover's swift 2m gun detection showcases superior optics, while the IP camera detects guns within 4m without delay, indicating high-resolution capabilities. To address the issue, optimizing algorithms for varying distances and adjusting parameters based on camera specifications can enhance overall performance. Balancing the trade-off between accuracy and speed ensures effective surveillance for smoking and gun detection in diverse scenarios within your system.

Light Intensity performance comparison:

Table 5.4: Impact of Light for Anomalous Object Detection

Luminance Intensity	**Computer-integrated CCTV camera**	**Rover Camera**	**Mobile IP Camera**
High	Instant Detection	Instant Detection	Instant Detection
Medium	Instant Detection	Instant Detection	Instant Detection
Low	Almost instant Detection	Delay Detection	Delay Detection
No Light	No Detection	No Detection	No Detection

The system excels in detecting anomalous activity in well-lit conditions, showcasing reliable performance. In medium-light environments, there's a marginal variation in its effectiveness, indicating some adaptability to varying lighting conditions. However, the system faces significant challenges in low-light scenarios, where its performance notably degrades. In these conditions, the detection accuracy becomes quite poor, posing a limitation to the system's overall efficacy. Furthermore, in the complete absence of light, the system's performance reaches zero, suggesting a critical vulnerability in handling scenarios with no illumination. To address this issue, exploring low-light optimization techniques or incorporating infrared technology could be beneficial. Improving the system's ability to function in diverse lighting conditions is essential for maintaining reliable surveillance and ensuring effective anomaly detection across a broader range of operational environments.

Multiple anomalous object detection comparison:

Table 5.5: Success Rate of Different Systems Detecting Multiple Anomalous Objects

Numbers Of Anomalous Objects	**Computer-integrated CCTV camera**	**Rover Camera**	**Mobile IP Camera**
One	100%	100%	100%
Two	100%	100%	66.67%
Three	100%	66.67%	33.33%

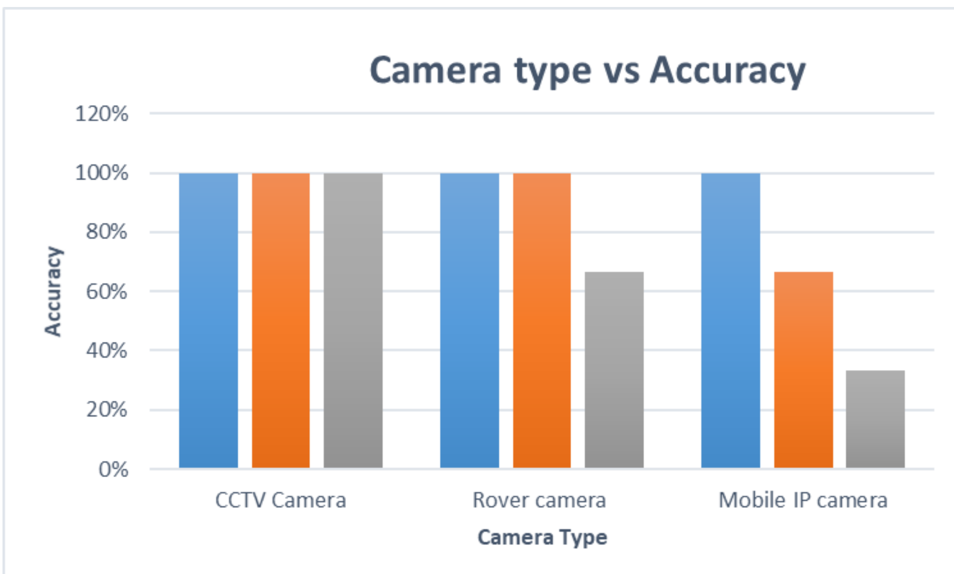


Figure 5.18: Multiple anomalous object detection Graph

Accuracy comparison:

Table 5.6: Comparison of Object Detection Accuracy

System	**No of Test**	**Detected**	**Failed**	**Accuracy (%)**
Computer-integrated CCTV camera	50	48	2	96%
Rover Camera	50	45	4	90%

Mobile IP Camera	50	43	7	86%

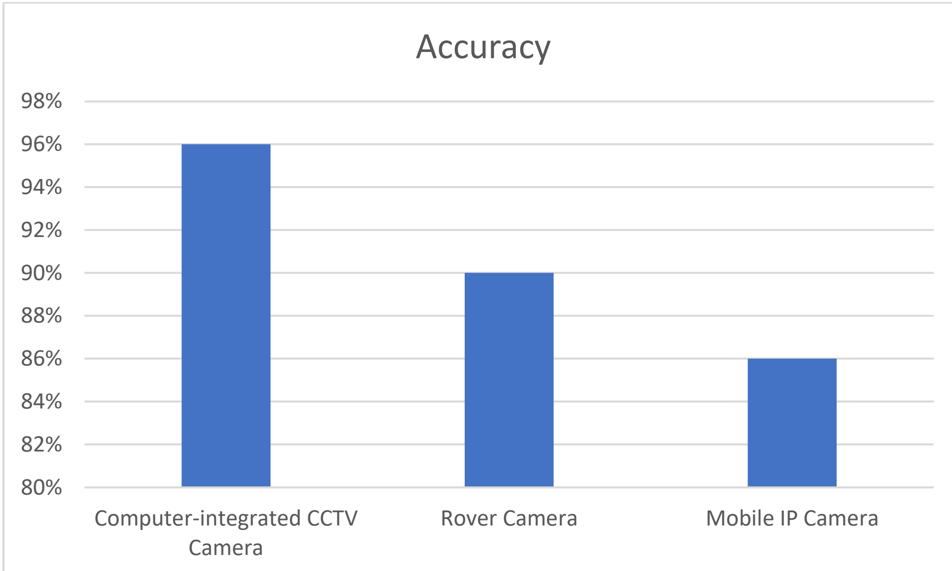


Figure 5.19: Accuracy comparison Graph

Comparison with conventional Security Guard:

The efficiency of security systems is dependent on continuous observation, which requires constant vigilance. Traditional techniques depending on human guards are vulnerable to gaps because guards may become preoccupied with activities such as napping or mobile phone use. Such mistakes create weaknesses, allowing possible suspects carrying unusual goods to enter unnoticed.

Figure 5.20: Failure of conventional security system (Gun)

Our novel approach fills this essential security gap. Figure 5.20 represents a scenario in which a security guard is asleep, unaware that a suspect is approaching the garage with a pistol. Fortunately, our smart technology immediately detects the suspect and easily transmits the information to the server.

Figure 5.21: Failure of conventional security system (Smoking)

Figure 5.21 demonstrates another security breakdown in which a suspect is spotted smoking in front of a lift, which is a forbidden behavior within the facility. Once again, the security guard is unable to catch the breach since he is sleeping. However, our clever technology takes the lead, swiftly recording the criminal activities and immediately communicating both the film and facts to the server.

Table 5.7: Comparison with Conventional Security System

System	No of Test	Detected	Failed	Accuracy (%)
Our System	50	46	4	92%
Security Guard	50	41	9	82%

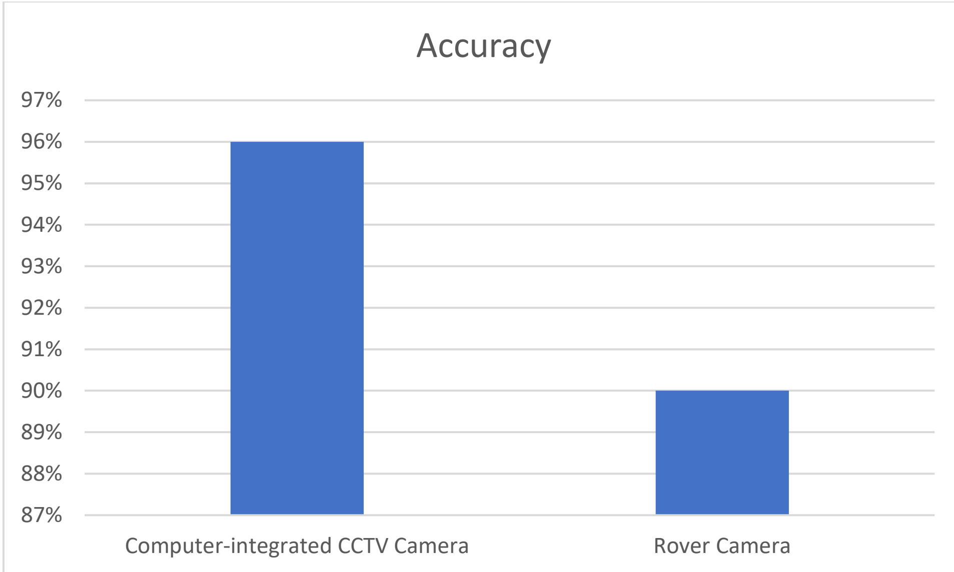


Figure 5.22: Graph of Comparison with conventional Security

According to our evaluation, the system did a good job of recognizing unusual activity, correctly identifying 46 out of 50 samples with a 92% accuracy rate. On security guard data, on the other hand, the system's accuracy was 82%, identifying 41 out of 50 samples. Despite its effectiveness, there were times when detections went unnoticed, highlighting the necessity of further improvement. These findings demonstrate the system's ability to detect anomalies, and further development is necessary to increase the system's accuracy, especially when it comes to the security guard data category. 5.7

5.4. Summary

In "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures," the Results Analysis and Critical Design Review phase serves as essential for evaluating the system's efficacy and dependability. Thorough testing and analysis revealed insights into the system's functioning. The results show that the three types of cameras work together to complete the system. The web cameras function as CCTV cameras when paired with a PC or laptop, while the rover webcam and mobile camera are converted to IP cameras with IP URL addresses. The CCTV camera system outperforms the other two varieties, although the rover camera works satisfactorily.

The research considers factors such as accuracy, response speed, and the system's capacity to effectively identify possible dangers. Furthermore, the Critical Design Review investigates the complexities of the system's architecture and design, determining if it fulfills engineering standards and safety criteria. This step requires a thorough analysis of the system's components, sensors, control algorithms, and overall technological integration. Finally, the Results Analysis and Critical Design Review give useful information about the system's strengths and limitations. It serves as the foundation for fine-tuning the design, improving performance, and guaranteeing that the "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" is a reliable and resilient solution that advances railway safety and efficiency.

Chapter 6

CONCLUSION

6.1. Summary of Findings

Any civilization that functions must prioritize security and safety, especially in commercial infrastructures where breaches may have serious dangers and repercussions. Security threats may take many different forms, from theft and illegal access to more serious situations including violence or terrorism. Finding possible weak points is essential to putting in place strong security measures.

To neutralize and minimize these threats this project develops an anomalous event detection system. An autonomous robot with the ability to navigate and keep an eye on certain locations is used in the implementation. To identify irregularities and possible dangers and also to navigate autonomous way the robot is outfitted with sophisticated sensors and imaging equipment. With a very high success rate, the system developed here is able to recognize dangerous items like knives and fire arms as well as other forbidden items like cigarettes. The system has effectively identified risks in several test scenarios and promptly warned the user. The rover can accurately identify items in front of it and change direction to travel freely, which makes the autonomous tracking system function very well.

Despite the project's effective execution, there are still certain problems. The system grows somewhat slower as the amount of input data increases and so does the calculation time. The system's inability to detect knives with 100% precision is the second issue that was encountered. It's challenging to correctly recognize the knife because of its dazzling appearance.

In summary, our idea presents a fresh approach to enhancing security and safety in commercial buildings. We've been successful in achieving our goal of making these spaces safer for individuals. In order to safeguard society as a whole and stay ahead of constantly evolving dangers, modern security systems must make use of this cutting-edge technology.

6.2. Novelty of the Work

The “Anomalous Event Detection for Enhanced Security for Commercial Infrastructures” reveals an innovative approach to security and surveillance systems that is centered on the early detection and mitigation of anomalous events. The strategy outlined in this project is notable for its pioneering and creative approach in the domain of security and surveillance. Its distinctiveness is evident through various unique facets:

Integration of Real-Time Supervision: This system provides a comprehensive approach to anomalous event detection by integrating real-time video footage, with the analysis of anomalous object outlines.

Decision-Making: The CNN model, trained to identify unusual activity, examines the incoming video streams. The system can make decisions, analyze sensor data quickly, and notify the server right away.

Safety Procedures: The developed system promptly responds to emergencies or safety concerns by offering real-time monitoring capabilities, thereby avoiding potential damages or losses. Our system is also used to increase security in workplaces, offices, and universities. Unlike other systems, it doesn't require any additional time or labor because it alerts the server right away.

Scholarly Work: The project makes use of scholarly publications that highlight the significance of abnormal activity detection and draws from current security systems research.

Safety and Efficiency Gains: The project entails creating a highly sophisticated security and surveillance system that uses auto navigating rover and Deep Learning to monitor the designated area for any unusual activity. These strange objects' outlines will be compared to an already-existing database of objects that are known to be safe.

Cost-effectiveness: Because of its lower hardware costs, ability to utilize pre-existing infrastructure, reduced maintenance costs, scalability, and automation of security operations—all of which lead to long-term cost savings—the security system is affordable.

6.3. Cultural and Societal Factors and Impacts

During the design phase of "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" cultural and societal factors were carefully taken into consideration as well.

These are important because they can have a big impact on how well-received and successful engineering solutions are, especially when it comes to risks and public safety.

While some communities prioritize security measures more highly than others, others could be concerned about unwanted surveillance. In order to manage these differences, conducting stakeholder engagement and community meetings can help assess public mood and resolve any cultural or sociological reservations.

Cultural values and ethical frameworks should be integrated into system development to guarantee that the algorithms and models eliminate bias and discrimination, function openly, and allow for inspection. Cultural sensitivity is another essential component of security system design and implementation. Considering cultural variation, practices, and norms when developing the system's rules, behaviors, and reaction mechanisms helps prevent assumptions that might not fit with particular cultural contexts and guarantees that the system respects cultural sensitivity. Similarly, the security system needs to be inclusive and accessible, accounting for linguistic obstacles, cultural diversity, and physical restrictions. Including components such as user-friendly designs, multilingual interfaces, and human considerations.

The main goal was to make sure that the system's implementation blends in well with the social and cultural landscape of the areas it serves. By taking these things into account, the initiative aimed to improve safety, convenience, and quality of life while also making a good impact on the environment and communities. This thorough examination and incorporation of social and cultural aspects represents an ethical and comprehensive method to engineering design, in which technology is used to enhance people's lives while honoring and balancing regional norms and expectations.

6.4. Engineering Solution in accordance with professional practices

The development and execution of the "Anomalous Event Detection for Enhanced Security in Commercial Infrastructure" showcase a steadfast dedication to engineering solutions by following professional practices with precision. This initiative not only exhibits a determination to address complex challenges but also maintains fundamental principles such as safety, security, ethics, and societal welfare, which are firmly embedded in the realm of engineering.

The accomplishment of this project lies in the meticulous application of engineering precepts in the formulation of inventive resolutions. By integrating cutting edge technology, sophisticated data analytic methodologies, and precisely calibrated detection algorithms, this intricately engineered system is architected to furnish real-time security surveillance for commercial infrastructures. The deliberate deployment of an autonomously navigating robotic entity, equipped with surveillance cameras across the infrastructural expanse, denotes a judicious engineering decision, thereby constituting a vigilant network that incessantly inspects real-time conditions and expeditiously identifies potential security threats or aberrant activities. The automated discernment of such anomalies underscores the project's unwavering commitment to prioritizing safety, thereby exemplifying the quintessence of this engineering endeavor.

This effort demonstrates a profound understanding of the significant influence that engineers have on society, in addition to their technical proficiency. Ethical considerations and a profound sense of professional responsibility for public safety take precedence. The anomalous event detection system embodies these principles by vigilantly securing commercial infrastructures, aligning seamlessly with engineering ethics to proactively prevent security breaches and potential risks.

This project also acknowledges the wider socioeconomic consequences of engineering endeavors. It recognizes the cultural relevance of a safe and dependable infrastructure and the economic and social benefits of maximizing security measures for commercial places. The automation of the system considerably lowers the requirement for ongoing human intervention in the pursuit of increased security and risk mitigation, improving operational efficiency and lowering security vulnerabilities which is a concrete example of engineering's commitment to societal well-being.

In essence, the idea and execution of the "Anomalous Event Detection for Advanced Security in Commercial Infrastructure" demonstrate a keen interest in engineering solutions as well as a meticulous respect to industry standards. Acting as a model, it demonstrates the use of cutting-edge technology and sophisticated data analysis to tackle complex problems while unequivocally respecting moral principles and taking into account societal concerns. Above all, this program is a powerful example of how engineering can be used to improve security, operational effectiveness, and social welfare in the context of commercial infrastructures, and it represents the highest standard of professional competence in the industry.

6.5. Limitations of the Work

In concluding the "Anomalous Event Detection for Enhanced Security for Commercial Infrastructures," it is critical to acknowledge the limits that were associated with the project's scope. While this unique technology represents a substantial development in commercial infrastructures, it is important to emphasize a few limitations.

Firstly, our innovative surveillance system, which uses cameras on both the rover and the monitoring station, has advanced capabilities, it has a significant disadvantage when confronted with severe weather conditions, notably dense fog. The atmospheric interference generated by dense fog can dramatically reduce camera vision and, as a result, their ability to detect and identify items of interest. In instances with restricted visibility owing to foggy weather, the system may struggle to maintain optimal performance. The system's overall accuracy and reliability in identifying anomalous objects may be hampered as a result of compromised visual data acquisition.

Secondly, a considerable limitation in the execution of our surveillance project stems from budgetary constraints. There is the possibility of improving system performance by using high-end, more expensive cameras and cutting-edge hardware components. Unfortunately, budgetary constraints force us to make sacrifices in our choosing, opting for less expensive alternatives. This tradeoff may result in trade-offs, compromising the system's capacity to attain optimal detection accuracy and responsiveness. While we aim to optimize capabilities within our financial limits, it is critical to recognize that resource constraints may impair the project's complete potential.

Thirdly. when faced with the responsibility of monitoring a CCTV monitoring room with 9-10 real-time TV footage at the same time, an inherent restriction in our surveillance system becomes apparent. While the system is capable of handling 2-3 footages, increasing the number poses computational issues. The additional data influx may tax the system's processing capabilities, resulting in slower reaction times and decreased overall monitoring efficiency. Our surveillance system has a fundamental disadvantage in that it struggles to detect anything concealed beneath pockets, coats, or shirts, where full visibility is reduced. In such cases, ordinary cameras are insufficient, necessitating the incorporation of infrared (IR) cameras. To address this constraint, the inclusion of IR technology becomes critical, allowing the system to bypass visual boundaries and identify concealed things that would otherwise go unreported.

In short, if we point out the limitations:

- Budgetary constraints.
- Not immune to severe weather conditions.
- The detection range of CCTV footage was not significantly vast.
- Unavailability of IR cameras causes a struggle in detecting not fully visible objects.

6.6. Future Scope

The "Anomalous Event Detection for Enhanced Security for Commercial Infrastructures" project has achieved significant milestones in improving security through innovative surveillance technology. Considering the recognized constraints, it is essential to articulate the future possibilities of the project to ensure further improvements and increased efficiency.

The Future scope for this surveillance system includes a strong expansion plan to smoothly monitor over 20 cameras at once, guaranteeing scalability, efficiency, and adaptability to various business infrastructures. The combination of distributed computing architecture with parallel processing emerges as a pivotal solution to the challenge of monitoring an increasing number of cameras. As the camera count rises, the system's ability to manage the additional computational burden is optimized by distributing tasks across multiple processing units or servers. This not only ensures efficient handling of the workload but also maintains optimal performance, addressing concerns related to computational challenges.

Simultaneously, the strategic incorporation of edge computing adds a tactical advantage to the surveillance system. Placing computing work closer to the cameras enhances real-time processing capabilities and reduces latency. This proves crucial in dynamic environments such as airports and train stations, where quick reactions are imperative for maintaining security.

In addition to the comprehensive strategy outlined for the future development of the human activity detection algorithm in surveillance, a critical scope involves the incorporation of infrared (IR) cameras to enhance security measures. By introducing IR technology into the surveillance system, there is a strategic focus on disclosing harmful objects that may be concealed under layers of clothing.

The integration of IR cameras brings a unique advantage to the surveillance infrastructure, particularly in scenarios where conventional cameras may struggle to provide full visibility, such as when items are hidden beneath pockets, coats, or shirts. IR cameras can effectively penetrate visual barriers, enabling the system to detect and identify objects that would otherwise remain hidden from standard camera views.

In conclusion, a comprehensive strategy incorporating edge computing, distributed architecture, parallel processing, and cloud integration and the involvement of IR cameras are required for the future development of the human activity recognition algorithm in surveillance. By overcoming the existing constraints, this all-encompassing approach seeks to create a surveillance system that is extremely scalable, efficient, and adaptive, able to monitor multiple cameras at once in intricate commercial infrastructures.

6.7. Social, Economic, Cultural and Environmental Aspects

6.7.1. Sustainability

The project "Anomalous Event Detection for Enhanced Security for Commercial Infrastructures" concludes by addressing not just technological concerns but also larger social, economic, cultural, and environmental elements. One important consideration is sustainability, which is in line with the United Nations Sustainable Development Goals (SDGs).

The project contributes significantly to SDGs, particularly Goal 9 (Industry, Innovation, and Infrastructure) and Goal 11 (Sustainable Cities and Communities). By developing a system able to detect anomalous events and objects, the system satisfies the goal of making cities and human settlements inclusive, safe, resilient, and sustainable [12]. The system also helps to build resilient infrastructure promote inclusive and sustainable industrialization and foster innovation [12].

Security systems based on object and activity identification improve energy efficiency and reduce environmental impact. To begin, it is critical to select energy-efficient hardware components and design the system to reduce power consumption through the use of low-power CPUs, efficient algorithms, and power management approaches. Secondly, adopting cloud-based solutions for system hosting can benefit from energy-efficient architecture and resource optimization, lowering the environmental effect of physical server maintenance. Optimized data storage can also help with energy savings by applying appropriate data management methods, keeping just-needed object recognition data, and eliminating redundant storage. Continuous system improvement can enhance accuracy and efficiency while minimizing excessive resource usage through frequent upgrades and optimization of algorithms and software.

Finally, encouraging responsible usage and correct system handling among users and stakeholders, as well as increasing education and knowledge about the environmental advantages of object recognition systems, can help to reduce energy waste and maximize resource utilization. Object recognition systems may help to a more eco-friendly and ecologically conscientious operation by applying these sustainable practices.

6.7.2. Economic and Cultural Factors

The "Anomalous Event Detection for Enhanced Security for Commercial Infrastructures" project has taken into account the larger social, economic, cultural, and environmental implications.

Economic Factors:

To provide a low-cost security solution, the project makes use of open-source software and low-cost hardware components. This emphasis on cost has the potential to promote accessibility by making the system more accessible to persons or organizations with limited financial resources. Furthermore, the development, implementation, and maintenance of the security system may contribute to the creation of jobs in the technology and security industries. Skilled workers may be required for several occupations, including system design, coding, installation, and ongoing maintenance, stimulating job opportunities and supporting economic growth in these areas.

Cultural Factors:

The project's flexibility, which allows for customization and adaptation to distinct cultural conditions, is a significant cultural component. Different cultures may have different security requirements or preferences, and the ability to adjust the system to match those requirements helps to ensure cultural relevance and acceptance.

When surveillance technologies are applied, cultural norms and attitudes have a substantial impact on ethical issues about monitoring and privacy. To ensure that the project is done in a culturally acceptable manner, cultural sensitivity, respect for individual rights, and adherence to legal and ethical norms must all be considered. By taking these factors into account, organizations may handle the problems of monitoring in diverse cultural contexts while developing respect for privacy and preserving ethical norms.

6.8. Conclusion

In summary, the initiative "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" presents a revolutionary approach to security and surveillance. This pioneering project introduces a sophisticated system incorporating real-time video supervision, a decision-making Convolutional Neural Network (CNN) model, and safety protocols for the swift detection and mitigation of anomalous events.

However, challenges such as sensitivity to weather conditions, financial constraints, and limited camera range indicate the need for ongoing enhancements. The project envisions a promising future scope marked by scalability, edge computing, integration of IR cameras, and utilization of cloud-based solutions to overcome these limitations and elevate operational efficiency.

Ultimately, "Anomalous Event Detection for Enhanced Security in Commercial Infrastructures" makes a significant contribution to security systems through its innovative technology, emphasis on social responsibility, and commitment to continual development.The potential improvements in safety, efficiency, and sustainability across diverse commercial environments underscore its significance as a noteworthy advancement in the field of security.

REFERENCES

[1] “Unusual event detection via multi-camera video mining,” *IEEE Conference Publication | IEEE Xplore*, 2006. https://ieeexplore.ieee.org/abstract/document/1699732

[2] https://ieeexplore.ieee.org/document/6129539

[3] “Detecting unusual activity in video,” *IEEE Conference Publication | IEEE Xplore*, 2004. https://ieeexplore.ieee.org/document/1315249

[4] “Surveillance-Oriented event detection in video streams,” *IEEE Journals & Magazine | IEEE Xplore*, Jun. 01, 2011. https://ieeexplore.ieee.org/abstract/document/5445067

[5] Habib, Shabana, Altaf Hussain, Waleed Albattah, Muhammad Islam, Sheroz Khan, Rehan Ullah Khan, and Khalil Khan. "Abnormal activity recognition from surveillance videos using convolutional neural network." *Sensors* 21, no. 24 (2021): 8291.

[6] Zhou, Joey Tianyi, Jiawei Du, Hongyuan Zhu, Xi Peng, Yong Liu, and Rick Siow Mong Goh. "Anomalynet: An anomaly detection network for video surveillance." *IEEE Transactions on Information Forensics and Security* 14, no. 10 (2019): 2537-2550.

[7] Huang, J. et al. (2018) Optical flow based real-time moving object detection in unconstrained scenes, arXiv.org. Available at: https://arxiv.org/abs/1807.04890 (Accessed: 26 June 2023).

[8] Zhang, J. et al. (2017) A real-time Chinese traffic sign detection algorithm based on modified yolov2, MDPI. Available at: https://www.mdpi.com/1999-4893/10/4/127 (Accessed: 18 October 2023).

[9] R. Kalsotra and S. Arora, "Background subtraction for moving object detection: explorations of recent developments and challenges," *The Visual Computer*, vol. 38, no. 12, pp. 4151–4178, Aug. 2021, doi: 10.1007/s00371-021-02286-0.

[10] https://www.investopedia.com/terms/p/pest-analysis.asp

[11] P. Miszczak, "AI Jobs Statistics 2023 [The Impact on The Job Market]," businessolution.org, Apr.02,2023.
https://businessolution.org/aijobsstatistics/#:~:text=According%20to%20the%20World%20Economic%20Forum%20AI%20is (accessed May 21, 2023).

[12] https://sdgs.un.org/goals

Appendix A

Datasheet of the ICs used

1. Raspberry Pi

PIN wise Specification:

Pin Number	Pin Number	Pin Number	Pin Number	Pin Number	Pin Number
1	3.3V	Power	21	GPIO9	SPI0 MISO
2	5V	Power	22	GPIO25	
3	GPIO2	I2C SDA	23	GPIO11	SPI0 SCLK
4	5V	Power	24	GPIO8	SPI0 CE0
5	GPIO3	I2C SCL	25	Ground	Ground
6	Ground	Ground	26	GPIO7	SPI0 CE1
7	GPIO4	GPCLK0	27	ID_SD	I2C ID EEPROM
8	GPIO14	UART0 TX	28	ID_SC	I2C ID EEPROM
9	Ground	Ground	29	GPIO5	
10	GPIO15	UART0 RX	30	Ground	Ground
11	GPIO17	SPI1 CE1	31	GPIO6	
12	GPIO18	SPI1 CE0	32	GPIO12	
13	GPIO27		33	GPIO13	
14	Ground	Ground	34	Ground	Ground
15	GPIO22		35	GPIO19	SPI1 MISO
16	GPIO23		36	GPIO16	SPI1 CE2
17	3.3V	Power	37	GPIO26	
18	GPIO24		38	GPIO20	SPI1 MOSI
19	GPIO10	SPI0 MOSI	39	Ground	Ground
20	Ground	Ground	40	GPIO21	SPI1 SCLK

Model Configuration:

Specification	Details
Processor	Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz1
Memory	4GB LPDDR4-3200 SDRAM1
Wireless	2.4 GHz and 5.0 GHz IEEE 802.11ac wireless1

Bluetooth	Bluetooth 5.0, BLE1
Ethernet	Gigabit Ethernet1
USB Ports	2 USB 3.0 ports; 2 USB 2.0 ports1
GPIO	Standard 40 pin GPIO header (fully backwards compatible with previous boards)1
HDMI Ports	2 × micro-HDMI® ports (up to 4kp60 supported)1
Display Port	2-lane MIPI DSI display port1
Camera Port	2-lane MIPI CSI camera port1
Audio	4-pole stereo audio and composite video port1
Video	H.265 (4kp60 decode), H264 (1080p60 decode, 1080p30 encode)1
Graphics	OpenGL ES 3.1, Vulkan 1.01
Storage	Micro-SD card slot for loading operating system and data storage1
Power	5V DC via USB-C connector (minimum 3A*), 5V DC via GPIO header (minimum 3A*), Power over Ethernet (PoE) enabled (requires separate PoE HAT)1
Operating Temperature	0 – 50 degrees C ambient1

2. ESP32

PIN wise Specification:

Pin	Function	Details
GPIO0 to GPIO33	General Purpose Input/Output (GPIO)	Can be used for various tasks like reading sensors, controlling LEDs, communicating with other devices, etc.
Vin	Input voltage (5V to 14V)	Supplies power to the ESP32 board.

3V3	3.3V output	Provides a stable 3.3V power supply for external devices.
GND	Ground	Connects the ESP32 board to ground for reference.
TXD0	Transmit data (Serial)	Used for transmitting serial data to other devices.
RXD0	Receive data (Serial)	Used for receiving serial data from other devices.
GPIO6 to GPIO11	SPI0 (typically used for SPI flash)	Used for communicating with SPI flash memory.
GPIO16 and GPIO17	SPI1	Used for communicating with other SPI devices.
Any GPIO pin	SDA (I2C)	Used for data transfer in I2C communication.
Any GPIO pin	SCL (I2C)	Used for clock synchronization in I2C communication.
GPIO32 to GPIO39	ADC (limited functionality)	Can be used for reading analog voltage levels, but with limited resolution compared to dedicated ADC pins.
GPIO32 to GPIO39, GPIO9 to GPIO15	RTC GPIO (low-power applications)	Can be used for low-power RTC (Real-Time Clock) functions.

3. LiDAR :

Pin configuration:

Pin Name	Description	Pin Name	Description
VCC	Power supply voltage	I2C_SCL	I2C clock line (if I2C interface is supported)
GND	Ground	I2C_SDA	I2C data line (if I2C interface is supported)
TX	Transmit data (for serial communication)	SPI_CLK	SPI clock line (if SPI interface is supported)
RX	Receive data (for serial communication)	SPI_MISO	SPI Master In Slave Out (if SPI interface is supported)
Enable/Disable	Enable or disable the LiDAR sensor	SPI_MOSI	SPI Master Out Slave In (if SPI interface is supported)

GPIO	General Purpose Input/Output for additional control	SPI_CS	SPI Chip Select (if SPI interface is supported)
PWM	Pulse Width Modulation for communication/measurement		

4. Webcam :

Specification :

Specification	Description	Specification	Description
Brand	Fantech LUMINOUS C30	Microphone	Yes
Model	Fantech	USB Type	USB 2.0
Sensor Resolution	4MP	Dimension (WxHxD)	73 x 26 x 33mm
Frame Rate	25FPS	Cable Length (Meter)	1.4 Meter
Field of View	106 Degree	Video Encoding Format	AVI with MPG/YUY2