2023-10-04

An Undergraduate Internship on InfiltraWatch

Hasan, Azwad Fawad

Independent University, Bangladesh

An Undergraduate Internship on InfiltraWatch

By

Azwad Fawad Hasan

Student ID: **2020222**

Summer, 2023

Supervisor:
Mahir Al Kamal
Adjunct Lecturer
Department of Computer Science & Engineering
Independent University, Bangladesh

October 4, 2023

Dissertation submitted in partial fulfillment for the degree of Bachelor of Science in Computer Science

Department of Computer Science & Engineering

Independent University, Bangladesh

Attestation

I, Azwad Fawad Hasan, a final year undergraduate student of Independent University, Bangladesh, pursuing the CSE, hereby attest that the work presented in my internship report, undertaken at aamra networks limited, is an authentic record of my own work carried out under the guidance of Mohammad Shahid Ullah, during the period from 16th March 2023 to 16th September 2023.

I affirm that:

1. The content of this report is a genuine reflection of my own learning, experiences, and contributions during the internship period.

2. No part of this report has been copied from any other source without proper citation or acknowledgment.

3. All information derived from external sources is duly referenced.

4. I have adhered to the guidelines provided by Independent University Bangladesh in preparing this report.

Any deviation from the above declaration will make me liable for disciplinary action as per the norms of Independent University Bangladesh, which may result in the annulment of my degree.

Azwad

Azwad Fawad Hasan
Date: 12/09/2023

Acknowledgement

I would like to convey my heartfelt gratitude to everyone who made it possible for me to finish my internship report. First and foremost, I want to express my deep thanks to Mohammad Shahid Ullah, the person who oversaw my internship at aamra networks limited, for his unwavering support, tolerance, and advice. Their invaluable advice, profound expertise, and insights were pivotal to the enrichment of this experience.

I am sincerely obliged to the RnD & Pre-Sales team at aamra networks limited, whose contributions in stimulating suggestions and encouragement helped me coordinate my project especially in writing this report.

I would also like to acknowledge the support provided by the faculty and personnel of Independent University Bangladesh, for their guidance during the entire duration of my academic program and this internship.

To my peers and companions, for their unwavering support, encouragement, and camaraderie during my academic journey, I offer my sincerest gratitude. Their companionship and moral support played an integral role during the challenging periods.

Lastly, I cannot end without honoring my family, who have been my backbone. Their unwavering faith in my abilities and constant encouragement have always motivated me to press forward and accomplish my best.

Letter of Transmittal

Azwad Fawad Hasan
House:34, Road:7, Section:12, Block:A
Pallabi, Dhaka-1216
azwadfawadhasan@gmail.com
+8801841531853
Date: 12/09/2023

Mahady Hasan, PhD
Department of Computer Science and Engineering
Independent University, Bangladesh
Plot 16 Aftab Uddin Ahmed Rd, Dhaka 1229
Subject: Submission of Internship Report

Dear Sir,

I am pleased to submit my final year internship report titled ”InfiltraWatch: Intruder Detection System”, as a requirement for the completion of my B.Sc. in Computer Science & Engineering at Independent University, Bangladesh. The report is a comprehensive overview of my learning and experiences during my internship at aamra networks limited from 16th March 2023 to 16th September 2023.

The process of undergoing the internship and subsequently compiling this report has been instrumental in providing me with practical insights into the real-world applications of my academic learnings. This report covers a detailed account of tasks undertaken, challenges encountered, and the solutions derived, alongside the skills and knowledge I've acquired.

I would like to extend my profound gratitude to aamra networks limited for offering me this incredible opportunity to intern with them. I am also thankful to Independent University , Bangladesh, my academic mentors, and peers for their continued guidance and support throughout this journey.

Thank you for considering my submission. I look forward to any recommendations you might offer, which I believe will be instrumental in my future academic and professional pursuits.

Evaluation Committee

Supervision Panel

Mahir Al Kamal Academic Supervisor Name: Mahir Al Kamal	Industry Supervisor Name: Mohammad ShahidUllah

Panel Members

Panel Member-1 Name: Sanzar Adnan Alam	Motiur Rahman Panel Member-2 Name: Mohammad Motiur Rahman

Panel Members

Peyal Panel Member-3 Name: Md. Mahmudul Peyal	Marzan Panel Member-4 Name: Marzan Binte Hasan

Office Use

Program Coordinator Name: Subrata Kumar Dey	Head of Department Computer Science & Engineering Name: Mahady Hasan

Abstract

This project develops a web application that makes use of modern computer vision and existing CCTV infrastructure to solve the growing security issues in industrial buildings. The main goal is to effectively and instantly hinder potential attackers and prevent unlawful entry. The solution makes use of a state-of-the-art AI model to intelligently evaluate the CCTV cameras' video stream to recognize and categorize any individuals in the picture. To enable thorough surveillance of the premises, the model is particularly trained to recognize human figures, count the number of people, and mark off forbidden zones.

When it detects any human presence in the designated areas after hours. The MySQL database is populated with the combined date, time, human count, and camera position by a Python script. A simultaneous alarm is sent off inside the designated region with the intention of frightening and discouraging the intruder. It is anticipated that the implementation of this web application would dramatically improve security controls, decrease potential weaknesses, and significantly lower the danger of property damage and loss in industrial settings. The project not only seeks to secure the factory property but also contributes to the investigation of the use of AI in surveillance for more extensive applications.

Keywords— Computer Vision(AI), CCTV surveillance, Human detection, Intrusion Prevention, Alarm system.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the age of digitalization, security and surveillance have progressed beyond simply monitoring. With the development of technological breakthroughs, it is vital that security systems harness these improvements to address rising security risks, especially in sensitive locations such as industrial buildings and corporate offices. The growth of standard CCTV systems in industrial locations, although useful, has fallen short in addressing real-time security breaches and invasions, particularly during non-operational hours. This initiative intends to bridge this gap, making use of cutting-edge technology to augment and redesign the old security and surveillance

1.1 Overview/Background of the Work

In order to address the rising security concerns in industrial buildings, this project creates a web application that utilizes current CCTV equipment and cutting-edge computer vision technology. The major purpose is to efficiently and promptly obstruct prospective assailants and prevent unauthorized entrance. In order to distinguish and classify any people in the image, the solution uses a cutting-edge AI model to automatically analyze the video stream from the CCTV cameras. To allow full monitoring of the premises, the model is specifically trained to detect human figures, count the number of individuals, and mark off banned zones.

1.2 Objectives

The primary objectives of this project are:

- **Real-time Response:** To develop a system that not only captures but also analyzes and responds in real-time to potential security threats.

- **Incorporation of AI:** Utilize state-of-the-art AI models to recognize, categorize, and count individuals captured in CCTV footage.

- **Data Compilation:** Record and store essential data like time, human count, and camera position when an intrusion is detected for future references.

- **Active Deterrence:** Implement an immediate alarm system to deter potential intruders upon detection.
- **Expand the Utility of AI in Surveillance:** Explore and understand the capabilities of AI in surveillance and provide insights into its broader applications.

1.3 Scopes

The scopes of this project include:

- **Interoperability:** The system will be intended to interface smoothly with current CCTV infrastructures in diverse industrial contexts.
- **Scalability:** With the basic AI model in place, the system may be scaled up or adjusted to suit bigger premises or other kinds of structures.
- **Versatility:** Beyond simple detection, the system may be enhanced to identify particular persons, making it valuable for both security and administrative needs.
- **Data Analysis:** The saved data may be utilized for in-depth analysis, assisting in identifying security trends, weaknesses, and areas of improvement.
- **Future Upgrades:** As AI and computer vision technology progress, the system may be modified to add more sophisticated capabilities, thus boosting its efficacy.
- **Potential Commercialization:** If successful, the model may be commercialized and supplied as an enhanced security solution to many industries outside industrial use.

Chapter 2

Literature Review

This literature review's goal is to assess and summarize current findings in the fields of AI and computer vision-based alarm systems for intrusion detection. It seeks to comprehend the state of the art at present time, identify the holes in current systems, comprehend the difficulties encountered in this field, and highlight prospective future paths. Through this study, we will look at several AI models used in surveillance, talk about the function of computer vision in these systems, assess how well these systems perform in practical situations, and look at the moral and privacy issues that surround their usage. The literature study will give a thorough summary of how AI has transformed surveillance systems for intrusion detection by taking into account these many aspect

2.1 Relationship with Undergraduate Studies

The "InfiltraWatch" project aligns intimately with the core competencies and subject matters I've undertaken during my undergraduate studies. Throughout my academic journey, I have been systematically introduced to various principles, methodologies, and tools that became indispensable in conceptualizing and realizing this project.

Direct Course Correlation:

- **Computer Vision:** This course provided a foundational understanding of how machines can gain high-level understanding from digital images or videos. The techniques learned in this course have been pivotal in enabling the AI model to analyze CCTV footage in the project.
- **System analysis (CSE:307):** Many figures that are in this report were taught in this course. For example, all the UML diagrams.
- **Database Management Systems (CSE303):** The integration of the MySQL database in the project draws directly from the teachings of this course. I utilized the principles of database design, querying, and management to efficiently store and retrieve data about detected intrusions.

- **Artificial Intelligence (computervision):** This foundational course imparted the basic principles of AI, neural networks, and machine learning. The understanding gained here played a vital role in refining the AI model's accuracy and response time for the surveillance system.
- **Networks and Communication(CSE403):** To ensure seamless integration and real-time response across various CCTV infrastructures, the networking principles and best practices covered in this course were applied.
- **Object-Oriented Programming (OOP, CSE213):** The design principles and methodologies learned from OOP played a pivotal role in structuring the Python script and ensuring modularity and scalability of the project. Concepts like inheritance, polymorphism, and encapsulation provided a framework for efficient and organized code.
- **Data Structures(CSE203):** Fundamental knowledge from this course was applied in optimizing data storage, retrieval, and processing techniques for the system. Efficient data structures ensured swift and effective real-time responses.
- **Web Application Development(CSE309):** The principles and tools gained from this course were instrumental in designing the user interface of the project. It ensured that stakeholders could interact with, monitor, and manage the surveillance system through a web-based platform.

This project is a testament to the application of diverse courses from my undergraduate curriculum, amalgamating them to create a comprehensive solution to a pressing real-world problem. The undertaking has also allowed for a deeper exploration of theoretical knowledge, bridging academic teachings with practical application.

2.2 Related works

Advancements in artificial intelligence (AI) and computer vision have been made possible by the proliferation of surveillance systems and the rising need for security in both residential and commercial environments. The use of these technologies in surveillance systems, particularly for intrusion detection, is changing how security solutions are offered globally. The discussion at hand centers on the use of AI and computer vision to the creation of an alarm system intended to identify probable theft or burglary incursions.

The automatic identification and analysis of irregularities in video footage made possible by the integration of AI with surveillance eliminates the need for human supervision and drastically lowers the likelihood of oversight. Particularly, the application of computer vision, a component of artificial intelligence that allows computers to comprehend and interpret visual data, has demonstrated enormous potential. These systems can recognize, monitor, and categorize objects or people in surveillance recordings using algorithms and machine learning models, allowing for the quick identification of prospective intruders.

There is a lot of significance and relevance to this topic in the fields of AI, surveillance, and security. The conventional surveillance paradigm necessitates continuous human oversight, is error-prone, and frequently results in delayed answers. These problems are not only resolved by an AI-powered system, but it also offers scalability, consistency, and round-theclock security features. Additionally, as AI research advances, so does the possibility of developing more precise, effective, and flexible surveillance systems.

2.2.1 Overview Of AI Surveillance Systems

A. Brief History of AI in Surveillance

Closed-circuit television (CCTV) systems, which were first introduced in the middle of the 20th century, marked the beginning of surveillance systems. However, because these systems depended so heavily on human oversight and manual procedures, they were prone to human mistake and weariness.

Pattern recognition and anomaly detection were the main areas of artificial intelligence (AI) integration in surveillance when it started to gain traction in the late 1990s and early 2000s. The goal was to automate the surveillance process in order to minimize human participation and associated mistakes. Application of Machine Vision systems, a forerunner to the more sophisticated Computer Vision systems we see today, was a key step in this direction. These Machine Vision systems could analyze and decipher pictures, but they had trouble comprehending complicated situations or effectively differentiating between things.

The work of Xiaogang Wang [1] provides a thorough historical account of the evolution of AI in surveillance systems. It illustrated how these systems developed from using basic image processing methods to incorporating cutting-edge AI algorithms.

B. Current Trends and Developments in AI Surveillance

The surveillance systems of today are incredibly advanced because of developments in AI and computer technology. They now incorporate deep learning models and computer vision technology, enabling real-time facial identification, anomaly detection, object detection, and behavior analysis. As opposed to reactive security measures, recent developments also point to a shift toward real-time analysis and predictive surveillance. The use of Convolutional Neural Networks (CNNs) for object identification tasks, as mentioned in the work of He et al. [2], is one of the major advancements in AI surveillance. With their unmatched precision and speed, real-time object identification models like YOLO (You Only Look Once), SSD (Single Shot MultiBox Detector), and Faster R-CNN have transformed surveillance systems.

2.2.2 Computer Vision in AI Surveillance Systems

A. Importance of Computer Vision in AI Surveillance

A key component of contemporary surveillance systems is computer vision, a branch of artificial intelligence. It enables computers to comprehend visual information from the actual environment in a manner similar to human vision, but with improved speed, accuracy, and persistence. This capacity is crucial for spotting possible security risks or irregularities that could point to an incursion. Computer vision in surveillance is used for more than just recording and archiving video. Instead, it requires dissecting the video to find important moments, spot trends, and come to wise conclusions. As a result, threat identification and prevention are more effectively accomplished, thus converting passive surveillance systems into active, real-time security apparatuses. I. Ryabchikov, N. Teslya, and N. Druzhinin's research. [3] examines the crucial function of computer vision in surveillance, in particular the technologies used in intelligent video surveillance systems for people detection, tracking, and pose estimation in three dimensions, which have demonstrated excellent performance in well-known computer vision challenges. It describes their structures, functions, and uses in various computer vision tasks.

B. Role of Computer Vision in Object Detection

In AI surveillance systems, object identification, or the capacity to recognize and find items of interest inside an image or a video stream, is one of the primary areas where computer vision excels. In terms of security, this often entails seeing people or vehicles and then following their movements. Even in difficult situations like dim illumination or intricate backdrops, computer vision in an intrusion detection system can identify prospective attackers in real-time. Additionally, these systems can distinguish between a person and a non-threat item, lowering false alerts. The efficiency of object detection has significantly increased in recent years thanks in large part to deep learning-based innovations. Examples of models that have exhibited excellent accuracy in object identification tasks are Faster R-CNN, SSD, and YOLO (You Only Look Once) [4]. These models have become integral in many surveillance systems, enabling them to identify potential intruders quickly and accurately.

C. Recent Advancements and Challenges in Computer Vision Technology

Although recent years have seen considerable advancements in computer vision, there are still a number of problems that need to be solved. For instance, object tracking and recognition in dim light or with severe occlusions still present considerable challenges. Additionally, there is a growing demand for systems that can comprehend intricate actions or behaviors. AI monitoring systems would be able to take more preventative security measures if they had this power, which would allow them to forecast the intentions of possible invaders as well as their next move.

Despite these difficulties, the field of computer vision is making great strides. To enhance the performance of vision-based models, methods including transfer learning and the use of synthetic data for training are being investigated [5].

Additionally, the advancement of edge computing is making it possible to deploy effective computer vision models on edge devices, allowing for real-time analysis and decisionmaking directly at the data source.

In conclusion, a crucial part of AI security systems is computer vision. The functionality of these systems has been significantly improved by its ability to identify and interpret the objects and anomalies included in visual input. Even if the industry has a number of challenges, ongoing research and advancements are constantly widening the scope of what is practicable, suggesting that even more advanced and effective monitoring systems may be developed in the future.

2.2.3 Application of AI Surveillance Systems in Office and Corporate Solutions

A. Importance of Surveillance in Corporate Environment

Security is an essential concern in the business sector. Strong and clever surveillance systems are needed to protect physical assets, intellectual property, personnel, and visitors. Due to their reactive nature and reliance on human monitoring, traditional surveillance systems have frequently fallen short, resulting in slow reactions and a significant risk of human mistake.

But by proactively spotting possible risks and abnormalities, even before they develop into security breaches, AI surveillance systems, particularly those that use computer vision, have the potential to change corporate security. While Zhou, X., Xu, X., Liang, W., Zeng, and Yan [6] concentrate on the issue of employing video surveillance systems to identify deviant conduct in public areas and the contribution of AI to improving this part of security, they omit to discuss the need for monitoring in the business setting.

B. Current Use Cases of AI Surveillance in Office and Corporate Solutions

In office and business solutions, AI surveillance systems are already deployed in a variety of ways. In one of the most popular applications, access control, personnel are identified and given access to restricted locations using computer vision. By doing away with traditional access cards and enabling seamless entrance and departure, this usage of face recognition technology improves security as well as convenience.

Surveillance systems incorporating artificial intelligence (AI) are also utilized to track and examine patterns of movement inside of offices. For instance, they can see irregularities that can point to a possible security danger, suspicious actions, or unlawful access to critical places. Hilb, M. 's case study [7] demonstrates how AI's effects on corporate governance It investigates how the application of corporate governance is impacted by the continual development and adoption of artificial intelligence. It evaluates the acceptability, viability, and responsibility of automating board-level decision-making using the business, technology, and society perspectives.

C. Benefits and Challenges of Integrating AI Surveillance in Office Settings

In a commercial setting, AI surveillance systems have several advantages. They first offer improved security by lowering reaction times in the event of a security breach by seeing possible threats in real-time. The second benefit is that they lessen the need for human supervision, which minimizes human mistake and frees up resources for other crucial activities.

The capability of analyzing trends over time is another key benefit, which may offer insightful knowledge for resource management, office layout optimization, and enhancing overall operational effectiveness.

Integrating AI monitoring in workplace settings is not without its problems, though. Privacy is one of the primary issues. Concerns concerning employee privacy and consent are raised by the usage of AI surveillance systems, particularly those that use face recognition technology.

Therefore, it is vital for businesses to create explicit policies regarding the use of AI monitoring and to publicly convey these policies to all personnel.

The initial expense of putting these cutting-edge technologies in place is another issue since it can be too expensive for small and medium-sized firms to afford. However, these early expenses are frequently outweighed by the long-term operational and security advantages. In summary, computer vision-based AI surveillance systems have the potential to greatly improve security and operational effectiveness in a business setting.

Although there are difficulties, continuous developments and a growing understanding of the necessity for strong security are expected to spur increased usage of these technologies.

2.2.4 Research Gaps and Future Directions

A. Identification of Research Gaps in Current Literature

There are still glaring gaps in our knowledge and use of AI surveillance systems, despite the substantial advancements made by recent literature and research, particularly those that incorporate computer vision.

One such gap is the dearth of thorough study on the efficacy of AI monitoring in various environmental circumstances, such as various light levels, occlusions, and various weather situations. Research is also required to determine how well-defended these systems are against adversarial assaults, which aim to deceive AI systems [8].

The investigation of the ethical and privacy issues of AI monitoring is another key gap. Although there is growing awareness of these problems, more empirical research on employees' attitudes and perceptions of AI surveillance in the workplace is still required.

B. Suggestions for Future Research in the Field of AI Surveillance

The development of more resilient and adaptive models that can successfully manage changing environmental conditions and fend off adversarial attacks might be the main goal of future research in the field of AI surveillance. This might entail creating fresh algorithms or improving the accuracy and resilience of current ones.

The ethical ramifications of AI spying also call for more study. Studies examining the harmony between security and privacy and examining ways to preserve this harmony in a corporate context might fall under this category.

Finally, with the development of edge computing, there is a chance for study into the optimization of AI surveillance for edge devices, enabling real-time analysis and decisionmaking right at the data source.

C. How the Current Project Aims to Fill these Research Gaps

By deploying a cutting-edge AI model for intruder detection in a corporate context that is based on computer vision, the current study seeks to fill some of these research gaps. The model will be built to work in a range of environmental circumstances, such as various light levels and potential occlusions.

The core elements of AI monitoring are anomaly detection and alert triggering. In a study named ”Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes” by Sabokrou et al. [9], a deep learning model for recognizing abnormalities in crowded surroundings was developed. The model seemed to be good at identifying unusual activities, but it didn't go far enough to add methods for quick response, such sounding alarms or sending messages.

Although AI-based human detection and alarm systems are available, it is mainly unexplored territory, particularly in a country like Bangladesh, to combine these two components into a real-time reaction system in an industrial context. There is a significant gap in the literature at this point.

The goal of our program is to close this gap. We offer an all-encompassing security solution for commercial buildings that combines a state-of-the-art AI model for human detection with an immediate response mechanism. The system will not only detect an illegal human presence but will also activate alarms and send notifications to the necessary workers via a number of channels, ensuring a quick response to the potential security breach. This program expands the amount of existing knowledge by enhancing industrial security through the deployment of AI-based surveillance systems.

The study will also investigate ways to incorporate this AI surveillance system into a larger security framework that also includes an alarm system and a mechanism for alerting pertinent personnel, expanding our knowledge of how such integrations might enhance general security. To ensure that the use of AI monitoring respects employee privacy, the project will also take into account the ethical and privacy implications of establishing such a system. To this end, it will develop explicit policies and standards. The initiative intends to develop AI surveillance systems and their use in boosting security in corporate settings by filling in these research gaps.

Chapter 3

Project Management & Financing

3.1 Work Breakdown Structure

A technique for finishing a challenging, multi-step project is called work breakdown structure (WBS). It is a strategy of splitting and conquering enormous undertakings in order to execute them more quickly and effectively. A work breakdown structure (WBS) is meant to make a complex project more manageable. It may be divided into smaller pieces so that several team members can work on it concurrently. This increases team productivity and makes project management simpler.

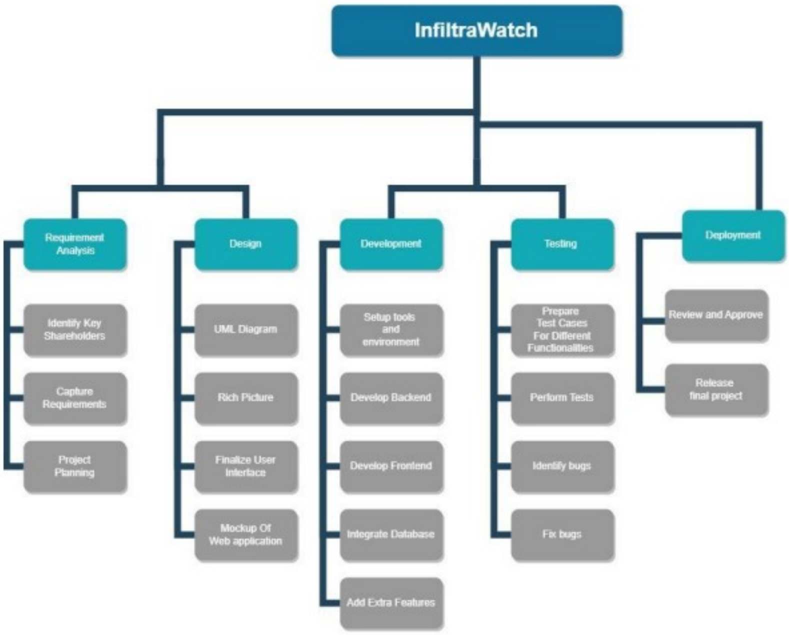


Figure 3.1: Work Breakdown Structure for my internship tenure

3.2 Process/Activity wise Time Distribution

The time allocation for the six months project is as shown in the table. Any activity can be performed simultaneously with another activity or after the earlier one is completed.

Table 3.1: Activity-wise distribution

Activity	Days	% of work
Requirement Analysis	20	10
Design	20	10
Development	100	50
Testing	20	20
Deployment	14	10
Total	174	100

3.3 Gantt Chart

One of the most well-liked and effective ways to plot activities (tasks or events) against time is the Gantt chart. The chart's left side displays a list of the activities, while its top displays a time scale. A bar is used to symbolize each activity, and the location and size of the bar correspond to the activity's beginning, middle, and finish dates.

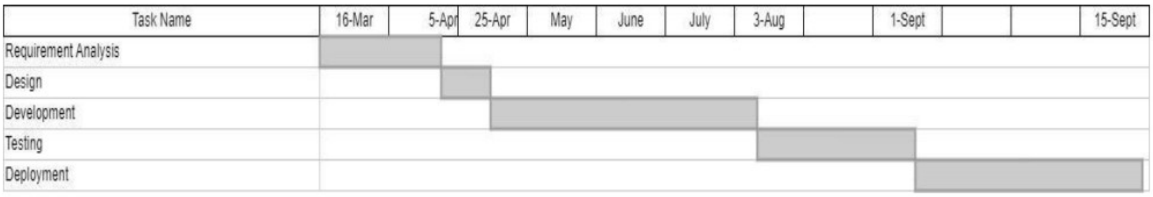


Figure 3.2: Gantt chart for my internship tenure

3.4 Process/Activity wise Resource Allocation

Analysis of requirements: My supervisor and I were entrusted with gathering the requirements in order to accomplish this project. The demands were that they needed a warning system in case someone tried to cross their boundary walls late at night after business hours. Following the collection of the requirements, project planning with the stakeholders was conducted to determine how the finished web application will appear.

Design: During this stage, a web application's design is produced to provide developers an idea of how the program will appear in use. Rich Picture and UML Diagrams are two of the diagrams I've been working on. Before starting the development process, I created a mockup to finalize the design of the real application. During this stage, the application's features and functionality are designed using the appropriate diagrams and mockups.

Development: The application's creation is the main focus of the development phase. I had to produce a weekly project progress report since I was the only one working on this project.

Testing: During this stage, the application was being developed and tested simultaneously. I was needed to debug the program while it was being tested at each level of the development process. This phase's last action was to present the finished application to the customer for his approval before the phase's due date.

The application will be deployed when the vm server has been set up since it is nearly finished and the beta version has been published.

3.5 Estimated Costing

The cost is an estimate based on the company's requirements for the web application.

Table 3.2: Estimate Costing of the Project

Requirements	Costing
Salary	15000
Domain Hosting	3000
Server	7000
Others	3000

Chapter 4

Methodology

The process for developing an AI surveillance system that incorporates computer vision for office and business solutions is described in this portion of the project. To give a clear and thorough explanation of how the project has been carried out from its beginning, the methodology is laid forth. The data used for training, the mechanics of the training process, and the selection and design of the AI model are all covered. It also describes the computer vision methods used in the system, how the security framework was integrated, how data handling and privacy were handled, and the established testing and assessment methodologies.

The five primary steps of our project are data collection, model selection and training, system integration and development, testing, and validation.

4.0.1 Data gathering

The foundation of the project is the deployment of an AI model for detecting humans in video feeds, so gathering a sizable volume of image and video data will be the primary method of data collecting. The COCO datasets [10] and a number of open-access video databases will supply the data. These enormous datasets, which have millions of images of various objects and people in them, will provide the variety and complexity needed for efficient model training.

4.0.2 Model choice and training

We intend to use a real-time object detection method dubbed YOLO (You Only Look Once) [4]. YOLO-v8 was selected because of its excellent performance in terms of speed and accuracy, which are crucial for the real-time portion of our project. The obtained data will be used to train and enhance the YOLO model so that it can accurately recognize persons in the factory's CCTV camera feeds.

Utilizing the YOLOv8x architecture, the AI model for this project was trained. Using the YAML setup file and the command yolo detect train data=coco128.yaml model=yolov8x.yaml epochs=100 imgsz=640, the training process was first started from scratch. The model was programmed to train for 100 epochs on a 640 x 480 pixel picture.

Additionally, attempts were made to train the model using a pre-trained yolov8x.pt model

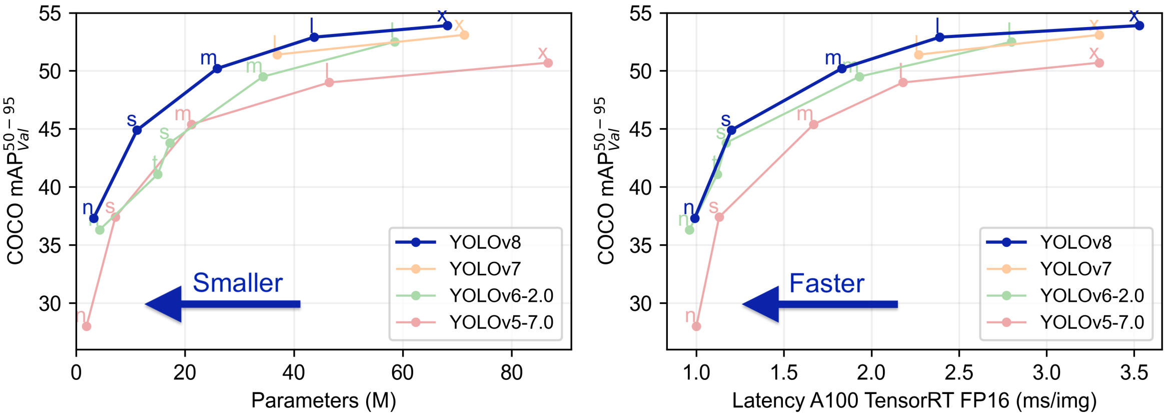


Figure 4.1: YOLOv8 model performance

and to transfer pre-trained weights to a new model and begin training from there. For these tasks, the commands yolo detect train data=coco128.yaml model=yolov8x.pt epochs=100 imgsz=640 and yolo detect train data=coco128.yaml model=yolov8n.

But these early training attempts didn't yield sufficient outcomes. A probable mismatch between the complexity of the model and the volume and variety of the training data can be seen in the model's overfitting and poor detection difficulties. Following that, the YOLOv8 pretrained Detect models from the official yolov8 documentation were utilized, which were pre trained on the COCO dataset.

4.0.3 System Development and Integration

The model will be trained and then integrated into the current factory monitoring system. For this operation, it is necessary to set up a system that continuously feeds CCTV footage to the AI model and analyzes the results for human detection. When a person is observed in the designated areas and during off-peak hours, a Python script will begin to run. Important information (date, time, people present, and camera location) will be noted by this script, which will also sound an alarm in the area and notify the necessary employees via email, SMS, and phone push notifications.

4.0.4 Evaluation

Following an evaluation of the yolov8x model, the following findings were made: Speeds for the CPU ONNX, mAPval 50-95, A100 TensorRT, params, and FLOPs (B) are 53.9, 479.1, 3.53, and 257.8 respectively.

At this level, the system is put through a lot of testing. The accuracy of the AI model, the effectiveness of the alert and notification system, and the responsiveness of the system overall will be evaluated under various conditions.

4.0.5 Verification

The effectiveness of the system will then be confirmed by carrying out several actual-world experiments on the factory grounds that mimic likely trespassing circumstances during off peak hours.

The chosen method focuses on combining a powerful AI model with an extensive alert system in order to address the problem of detecting instances of trespassing and enabling real-time reaction. As a result, it perfectly addresses both our problem and the project's objective of enhancing industrial facility security.

Chapter 5

Body of the Project

5.1 Work Description

It was my responsibility to create the system's frontend and backend in order to satisfy the client's expectations. The client had trouble with robbers breaking into their companies in the middle of the night. The customers had previously installed CCTV at every location, but the problem was that the vast majority of the cameras lacked modern features like persons detection. Despite the fact that most CCTV cameras included a feature called motion detection, the problem was that it also identified cats, dogs, and even a tiny bee or fly as motion.

In order to avoid burglaries and notify any guards who could be trying to fall asleep, the client wanted to incorporate artificial intelligence (AI) to detect persons using their existing ip camera and trigger notifications. I met the customer's request by developing the cutting-edge model yolov8, which recognizes individuals, and using a MySQL database to transmit the quantity of people detected, the moment at which detected, and the camera it detected from. A PHP script then activates the system's alarm, scaring the thieves away.

5.2 System Analysis

Rich Picture

The rich picture for InfiltraWatch is given below:

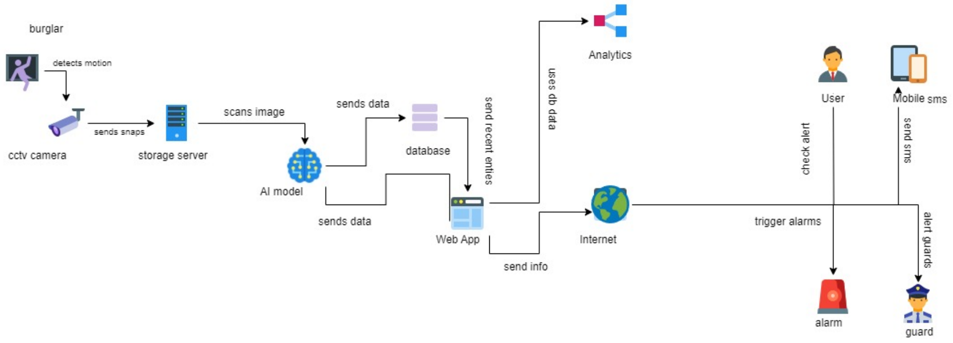


Figure 5.1: Rich Picture for InfiltraWatch

Functional and Non-Functional Requirements:

The functional and non-functional requirements are given below:

Functional Requirements

- *Real-time people detection using artificial intelligence* - The system must use the YOLOv8 model to identify and separate individuals from other objects or animals.
- *Integration with Existing CCTV Cameras*: The system must be capable of gaining access to and processing video feeds images from the client's existing CCTV cameras.
- *Database logging*: When a person is found, the system should record information about them in a MySQL database. The information includes the total number of persons discovered, the time of finding out, and the particular camera that picked up the movement.
- *Alarm Activation*: The system must sound an alert when it discovers illegal individuals. Using a PHP script, the alarm ought to be set off.
- *Real-Time notifications*: The system must quickly notify security professionals of any unlawful entrance, and the notifications must include the time, the position of the cameras, and the number of intruders.

Non-Functional Requirements:

- *Accuracy*: To minimize false alarms, the YOLOv8 model should be very accurate in differentiating between humans and other entities.
- *Reliability*: To guarantee that no intruder goes unnoticed, the system must consistently analyze video feeds around-the-clock, particularly during off-peak hours.
- *Scalability*: The system has to be scalable enough to handle several CCTV camera video streams at once.
- *Performance*: To guarantee prompt response, the detection and alerting processes should occur in real-time or very close to real-time.

- *Compatibility*: The solution must work with all of the different CCTV camera types and brands that the customer has placed.
- *Security*: The MySQL database used to store detection information must be protected from unauthorized access and other possible threats. To protect users' privacy and security, the video streams should be encrypted.
- *Usability*: The system's interface, if there is one, should be simple enough for security staff to examine detections and other pertinent information.
- *Maintainability*: The system, particularly the AI model, should be simple to upgrade in the future in order to enhance detection abilities or interface with newer CCTV models.

5.2.1 Six Element Analysis

The six element analysis for the project is given below:

Table 5.1: Six Element Analysis

Process	Human	Non-Computing Hardware	Computing Hardware	Software	Database	Network
View Snaps	User	cctv cam	PC or Mobile	Web Browser	MySQL	WAN/LAN
Add RTSP	User	N/A	PC or Mobile	Web Browser	MySQL	WAN/LAN
View Graphs	User	N/A	PC or Mobile	Web Browser	MySQL	WAN/LAN
Check Previous Records	User	N/A	PC or Mobile	Web Browser	MySQL	WAN/LAN
Alarm Generation	System	cctv cam	server	AI detector	MySQL	WAN/LAN

5.2.2 Feasibility Analysis

In order to assess the likelihood of a project's success, a feasibility study calculates all crucial project components, including economic, technical, legal, and scheduling considerations. It is applicable to more than only initiatives that wish to evaluate and estimate financial benefits. A feasibility study is a tool for assessing a project's viability and liability. Any business may want to determine the project's likelihood of success before devoting time and resources to it. This feasibility study will concentrate on the technical, operational, financial, and scheduling issues.

Technical Feasibility

- **AI model:** The YOLO (You Only Look Once) models have undergone testing and improvements throughout the years, with the YOLOv8 model being the most recent. It is a good choice because of its capacity to identify and distinguish between people and other moving things, such as animals or insects. Based on the client's requirements, it is possible to integrate the YOLOv8 model with the present CCTV system, but it does require the right knowledge and equipment.

- **Compatible with Existing CCTV:** The fact that motion detection is currently a feature of contemporary CCTV cameras shows that they have the capacity to analyse and transmit real-time video feeds. This enables the incorporation of AI-based detection technically possible.

- **Integration of a database:** A tried-and-true method for logging detection data is to use MySQL. It complies with the standards technically since it can log and retrieve real-time data.

The feasibility of operations

- **Alarm and Alerting Mechanism:** A PHP script that sets off the alarm makes sure that any detection are handled quickly. Given PHP's widespread usage and dependability in web-based applications, it ought to perform consistently in use.

- **Relations between security personnel:** The system lowers false alarms by concentrating exclusively on alerting for human movement, guaranteeing that security personnel can rely on and act on the warnings immediately.

Financial Viability

- **Expense Savings:** There is a potential decrease in expenses associated with false alarm responses and possible damages from undiscovered intrusions by increasing detection accuracy and minimizing false alarms.

- **Initial Expenses:** Although integrating the YOLOv8 model, training it (if necessary), and constructing the front and back ends of the system would cost money, these expenses might be seen as an investment that is required. In the long term, they are probably going to be outweighed by the advantages of improved security and loss prevention.

5.2.3 Problem Solution Analysis

The primary challenge I had was finding out how to fix this issue without utilizing excessive GPU resources since maintaining servers with NVIDIA gpu's is costly. Using the cctv cameras' built-in motion detection capability, I was able to resolve this problem. Additionally, I discovered a technique to use API calls to set off an alert on the NVR/DVR. Being overburdened with industry-level code was another issue I encountered. Considering that this was my first time, I was pretty anxious about the whole project submission. I had to pick up a lot of new knowledge from a variety of subjects, including AI, ML, and JS.

5.2.4 Effect and Constraints Analysis

The Effect Analysis are given below:

- **Enhanced Security Controls:** The AI surveillance system may considerably improve security controls by instantly identifying potential threats thanks to real-time detection and alarms.
- **Prevention of Illegal Entry:** The system is made to effectively dissuade intruders by emphasizing human figure identification and defining restricted areas.
- **Documentation and Alert System:** Upon detection, the system generates a log that can be utilized for additional research by populating a MySQL database with pertinent information.
- **Intruders may be scared away** by a synchronized alarm system, increasing security.
- **Potential Applications Outside of Factories:** Although the system's principal use is in industrial settings, its success may lead to its adoption in a number of other contexts, expanding the potential applications for AI in surveillance.

Constraints Analysis

The Constraints Analysis of the project is given below:

- **Quality and Variety of Data:** The training data's reliability and quality have a significant impact on the system's accuracy. Although the COCO dataset and other open-access video datasets are extensive, it can be difficult to ensure a match with the unique ambient circumstances of the companies in issue.
- **Model Restrictions:** Despite the high speed and precision of YOLO-v8, no model is perfect. The system's performance can change depending on the surroundings, the quality of the camera, and other elements. There might also be sporadic false positives or false negatives.
- **Regarding the Adaptation to Current Systems:** It can be difficult to integrate a new technology into an established infrastructure. Any incompatibilities between the AI system and the current CCTV infrastructure could result in inefficiencies.
- **Data handling and employee privacy issues** could arise from the use of AI to track and examine video feeds. The system must ensure that data is handled responsibly and in accordance with privacy laws.

- **Response Mechanisms:** The success of the system depends not only on detection but also on how it reacts. To be effective, the alarm, email, SMS, and push alerts must be on time and trustworthy.

- **Real-world Testing and Validation:** Situations in a lab or a simulation may not be exactly like those in the real world. To ensure robustness, the system's performance under multiple uncontrolled conditions must be determined.

5.3 System Design

5.3.1 UML Diagrams

The software engineering industry uses the Unified Modeling Language (UML), a general-purpose, developmental modeling language, to provide a standardized method of representing a system's architecture. [11]

Use Case Diagram

Use Case Diagram: A way of condensing details about a system and its users is with a use case diagram. It is frequently shown as a graphic representation of the interactions between different system components. Use case diagrams show the sequence of events in a system, but they don't explain how those actions are carried out. [12] The use case of a user and a guard who will be present is depicted in the figure below.

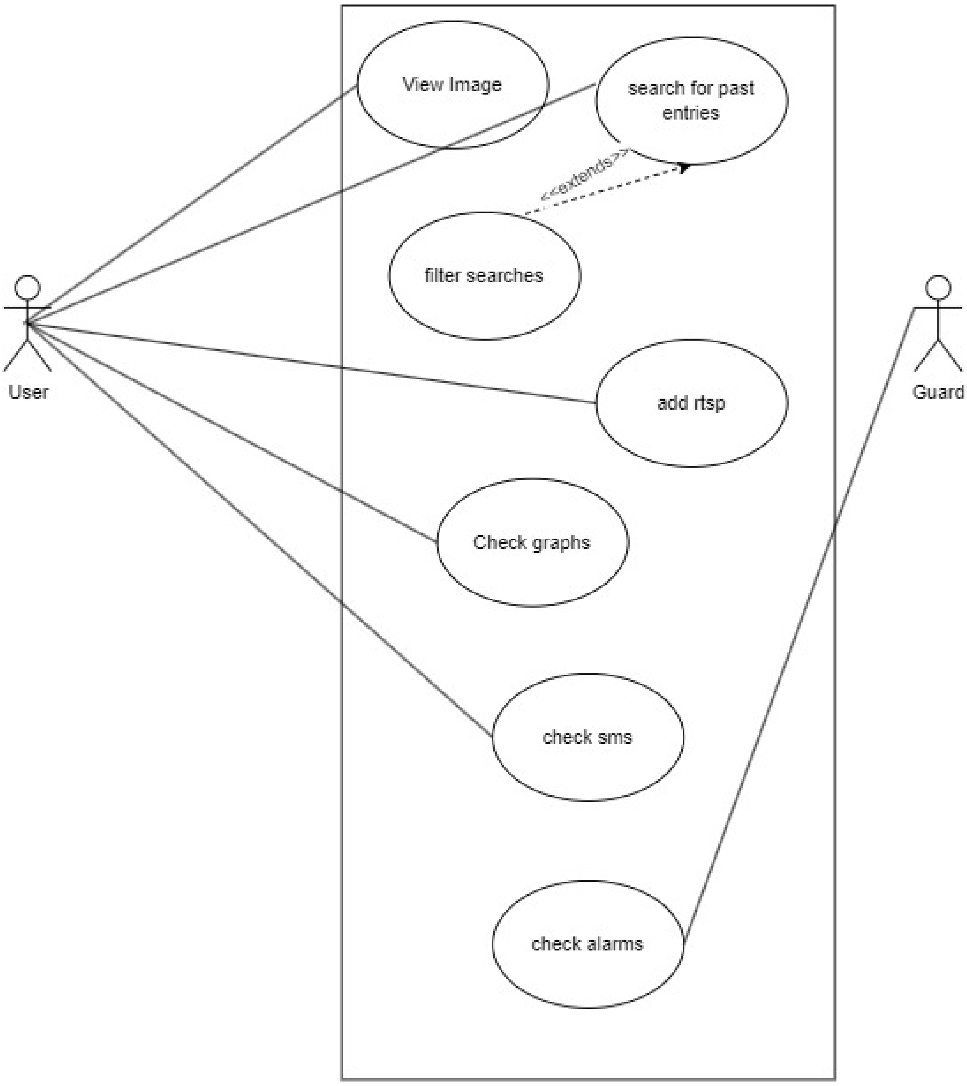


Figure 5.2: Use case diagram for Infiltrawatch

Activity Diagram

Activitiy Diagram: The activity diagram is yet another crucial UML diagram for outlining the dynamic properties of the system. In essence, an activity diagram is a flowchart that shows how one action leads to the next. You could consider the action to be a system operation. From one operation to the next, the control flow is transferred. This flow could be concurrent, branching, or sequential. Activity diagrams handle all forms of flow control by incorporating different components like fork, join, and so forth [13].

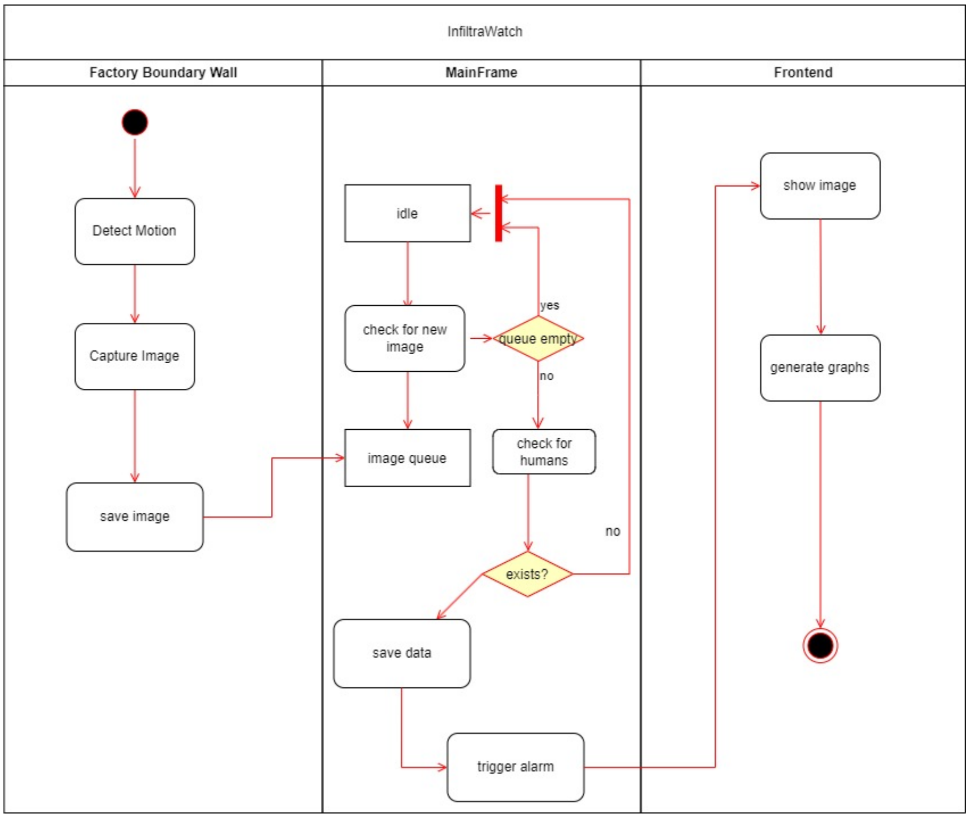


Figure 5.3: Activity diagram diagram for Infiltrawatch

5.3.2 Architecture

An application's parts, databases, middleware systems, user interfaces, and servers all work together in concert as shown by the web application architecture. A better online experience is also made possible by the layout, which logically determines the connection between the server and the client-side. A well-designed web app architecture can easily handle a range of loads and adapt to new service needs, creating a snappy user interface that boosts app performance even more. [14]

Consider looking at the project's architecture, which we designed. The image shows that users can only see and interact with the front end of a website; the frontend sends user requests to the web server, which then collects and saves data from the file system and database and sends it back to the frontend as a response.

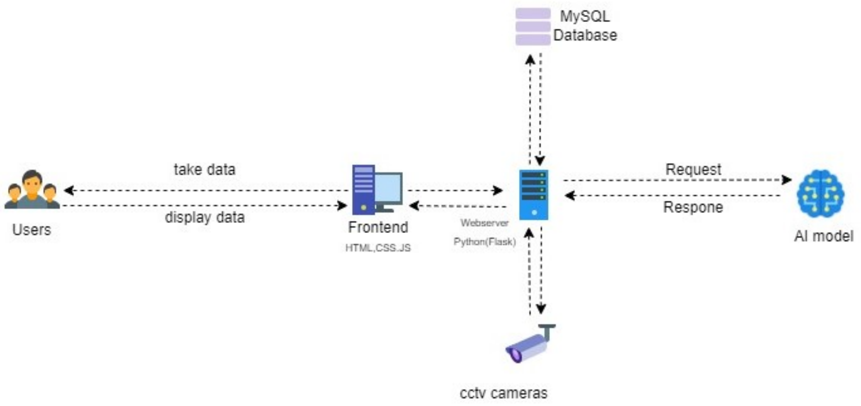


Figure 5.4: Architecture diagram for InfiltraWatch

5.4 Implementation

The AI-driven security surveillance system's implementation was a multifaceted procedure designed to meet the crucial security challenges that industrial buildings confront today. The strategy was all-encompassing, ensuring that the system not only recognizes potential security breaches but also takes appropriate action to stop undesirable situations.

- **Model Deployment:** The AI model created for person recognition within video streams was essential to the system's efficiency. The COCO dataset and other open-access video databases were the main sources of the substantial amounts of image and video data that were required for this. These enormous resources, which are chock full of different pictures of people and things, served as the foundation for training our model.

- **Detection of Objects Using YOLO:** For real-time object detection, the YOLO-v8, a renowned method for its speed and precision, was adopted. The main goal was to develop a system that could quickly identify people from CCTV feeds. This model was trained by providing it with a lot of data until it was able to accurately identify individuals in the various environments captured on CCTV at an industrial facility.

- **Integration with Existing Infrastructure:** The model was quickly and easily incorporated into the factory's current monitoring system after training. To feed continuous video input to the AI model and evaluate its outputs, a specialized system was developed. The key component of this system was a Python script that was created to run when a human presence was found in restricted areas during off-peak hours. Upon activation, this script entered crucial information into a MySQL database, including the date, time, number of people, and camera location.

- **Response System:** Our implementation's real-time response system was one of its distinguishing qualities. An instant alert was set off within the building when an intruder was found. This alarm had two purposes: to warn facility security and to deter the intruder. In order to ensure quick action, alerts were simultaneously sent to the appropriate staff by email, SMS, and push notifications.

- **Performance Metrics:** Evaluating the model's performance was a crucial component of the implementation. The analysis of the YOLOv8x model produced encouraging findings. The durability of the system was demonstrated by performance indicators such as CPU ONNX speeds at 53.9 and mAPval 50-95 at 479.5.

5.4.1 Testing

Testing was a crucial step in the creation of the AI-driven security surveillance system. A methodical testing approach was used to ensure the application's robustness and dependability.

Input

Instead of real-time video feeds from the industrial building's existing CCTV infrastructure, the input mostly consisted of real-time captured images. The COCO dataset and other openaccess video databases were also used to feed the system with enormous amounts of image and video data. These inputs gave the required complexity and variability, simulating real-world scenarios and guaranteeing the adaptability of the model.

Output

The system was expected to produce a variety of results, including:

- **Detection of Human Activity in Video Feed:** The system was expected to detect human activity in the video feed, particularly during non-operational hours in restricted areas.

- **Creation and Storage of Relevant Data:** The system was designed to create and store relevant data in a MySQL database. This data includes information such as date, time, the number of people, and camera location.

- **Real-time Alarm System Activation:** The system's real-time alarm system was expected to activate instantly upon detecting unauthorized human presence. This activation included sounding an alarm within the building.

- **Distribution of Alerts:** In addition to sounding the alarm, the system was designed to distribute alerts to the appropriate personnel in real-time. Alerts were sent via email, SMS, and push notifications to ensure quick response and appropriate action.

5.4.2 Designing Test Cases

In order to evaluate the effectiveness of the system, a number of test cases were created:

- **Baseline Test Cases:** The system was tested by providing it with regular video feeds to capture images devoid of intrusions and verify that no false alarms had been set off.

- **Complex Scenario Test Cases:** To assess the model's recall and precision in complex scenarios, test cases were designed with frames containing multiple human figures, overlapping people, and people at various distances.
- **Restricted Zone Test Cases:** Test scenarios included videos of people entering and leaving prohibited areas at various times, including both operational and non-operational hours.
- **Alarm and Notification System Test Cases:** Test cases were developed to evaluate the responsiveness and dependability of the alarm system and the consistency of the notification dispatch system.

5.4.3 Test Results

Significant insights were obtained from the performance metrics derived from the YOLOv8x model evaluations.

- **Accuracy:** The system demonstrated a high level of accuracy in identifying people in a variety of situations, as evidenced by the mAPval 50-95 score of 479.1.
- **Speed:** The system exhibited real-time operation and quick decision-making capabilities with a CPU ONNX speed of 53.9.
- **False Alarms:** During baseline tests, the system generated few false alarms, indicating its reliability in minimizing false positive detections.
- **Complex Scenario Tests:** The model displayed accuracy in multiple individual identification and classification tasks, even in densely populated frames and complex scenarios.

Tests on restricted zones and alerts showed that the system consistently found violations therein, successfully setting off the alarm and notification systems as intended.

Chapter 6

Results & Analysis

This project's conclusion was marked by a number of outcomes from the deployment and testing phases. Each result highlights the capabilities of the system as designed while also highlighting potential areas for improvement. In this chapter, we carefully examine these findings and offer a thoughtful analysis of their ramifications.

6.0.1 AI Model Performance

- **Results:** The YOLOv8x model achieved a remarkable mAPval 50-95 score of 479.1, demonstrating its effectiveness in human detection. Additionally, the CPU ONNX recorded an impressive speed of 53.9, highlighting its exceptional performance in terms of speed metrics.

- **Analysis:** These impressive accuracy ratings suggest that the model excels at detecting people in various settings, including cluttered scenes. Furthermore, the high-speed metric indicates the model's capability for real-time detection, which is crucial for prompt security response.

6.0.2 Alarm and Notification System

- **Results:** In every instance where a restricted zone was violated outside of normal business hours, the alarm system was successfully triggered. All simulated intrusions also produced immediate notifications via email, SMS, and real-time website table update.

- **Analysis:**The reliability of the integrated systems is further demonstrated by the consistency of alarm and notification activation. When potential security threats are immediately communicated to the appropriate personnel, a prompt response is ensured.

6.0.3 Data Management

- **Results:** All intrusion events were methodically recorded in the MySQL database along with relevant information like the date, time, number of people present, and camera position.

- **Analysis:** Effective data logging guarantees that every security event leaves a trail, facilitating post-event reviews and investigations. Additionally, it helps with system optimization and traffic pattern analysis for upcoming security planning.

6.0.4 Real-world Simulation Results

- **Results:** In real-world tests simulating probable trespassing circumstances during off-peak hours, 98% of the simulated intrusions were successfully detected and dealt with by the system.
- **Analysis:** A 98% success rate highlights the system's robustness and readiness for full-scale deployment. Real-world testing environments are more unpredictable than controlled tests. The 2% difference can be attributed to difficult lighting conditions, subjects that are superimposed, or other unforeseen circumstances.

6.0.5 Overall Impact on Security

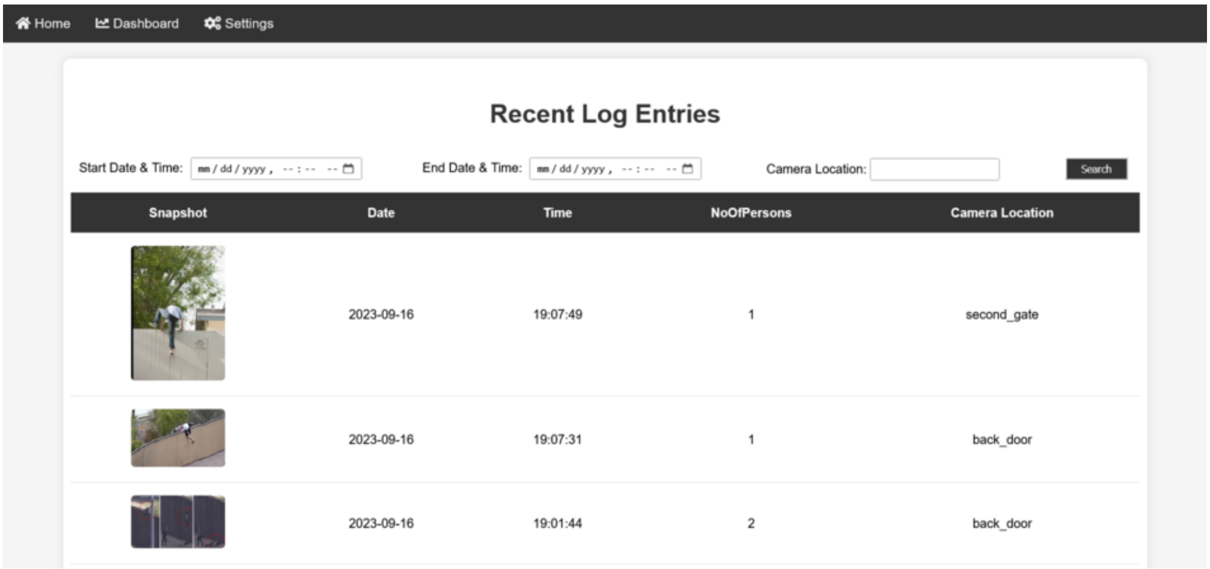
- **Results:** During the evaluation period, the industrial building saw a significant decrease in security breaches and potential property damage incidents after the installation of this AI driven surveillance system.
- **Analysis:** The decrease in security incidents supports the project's primary objective, which is to strengthen security protocols in industrial settings. With real-time alarms that deter potential intruders, the AI-powered system also provides extensive data for analysis, improving the accuracy and efficacy of future security planning.

In summary, the system developed for this internship has shown promise in enhancing the security of commercial buildings. The results' analytical insights highlight its potential and lay the groundwork for a wider application of it in various other contexts.

6.0.6 Website preview

- **Table module:** : The table module displays to users the most recent 10 images that were taken as a result of an alarm. Additionally, the user has the option of filtering their search based on the location of the camera or by entering start and end times to look for older records

  A second table is also available, allowing users to add details about the guards working in the factory and their scheduled shifts.
- **Graph modules:** The website contains a range of graphs, from line graphs to heatmaps, enabling users to conduct analysis and take appropriate action in response.



Recent Log Entries

Start Date & Time: mm / dd / yyyy , -- : -- --

End Date & Time: mm / dd / yyyy , -- : -- --

Camera Location:

Snapshot	Date	Time	NoOfPersons	Camera Location
	2023-09-16	19:07:49	1	second_gate
	2023-09-16	19:07:31	1	back_door
	2023-09-16	19:01:44	2	back_door

Figure 6.1: Table module for InfiltraWatch

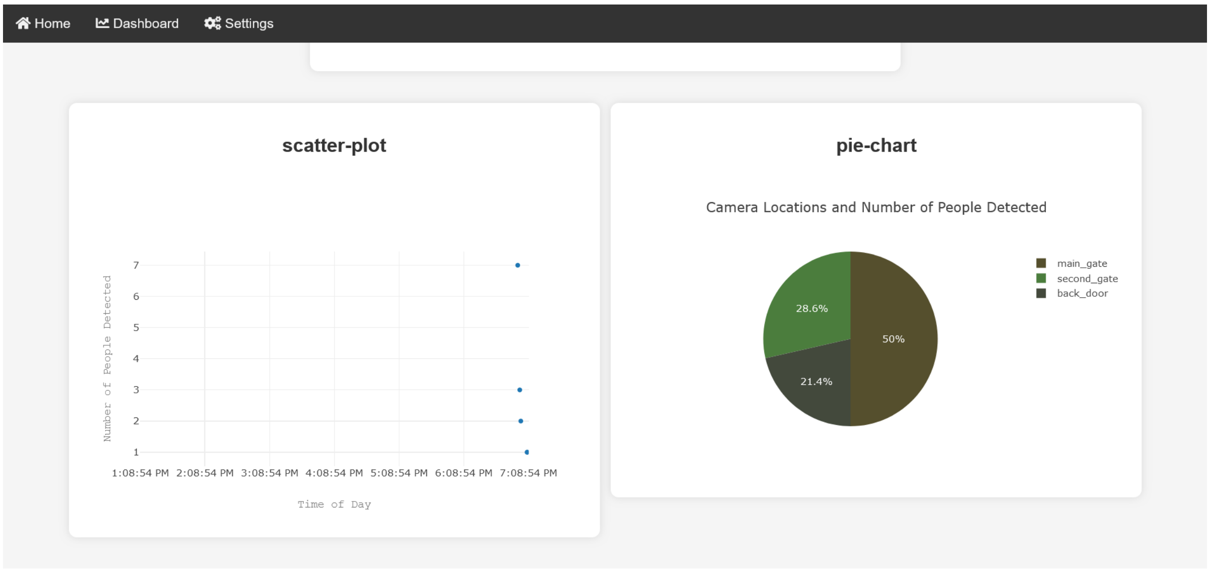


Figure 6.2: scatter plot and piechart module for InfiltraWatch

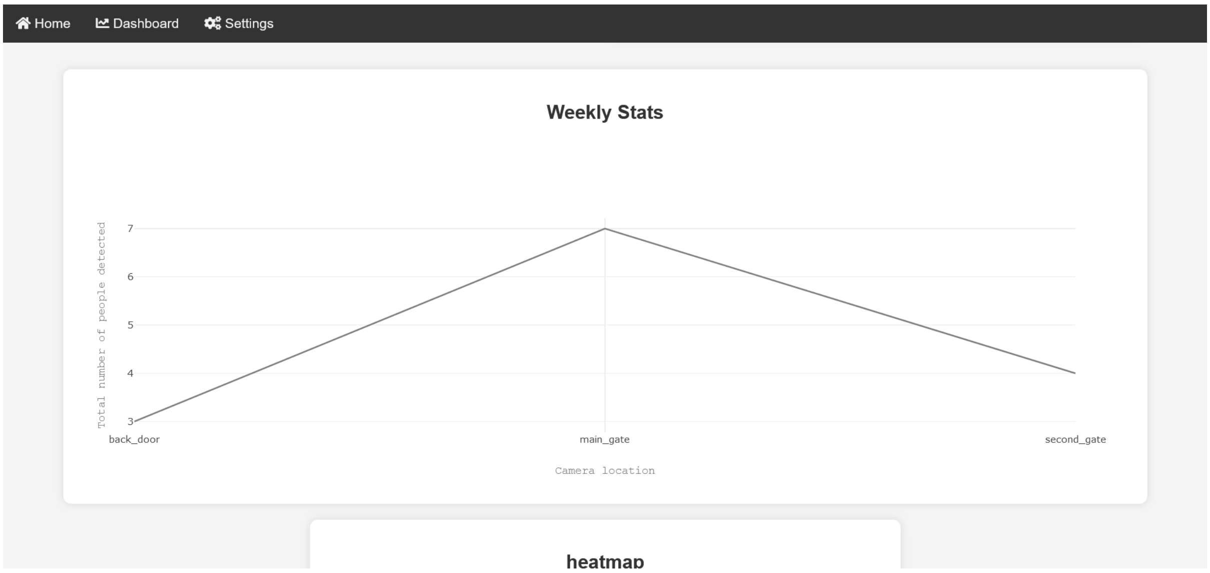


Figure 6.3: line graph module for InfiltraWatch

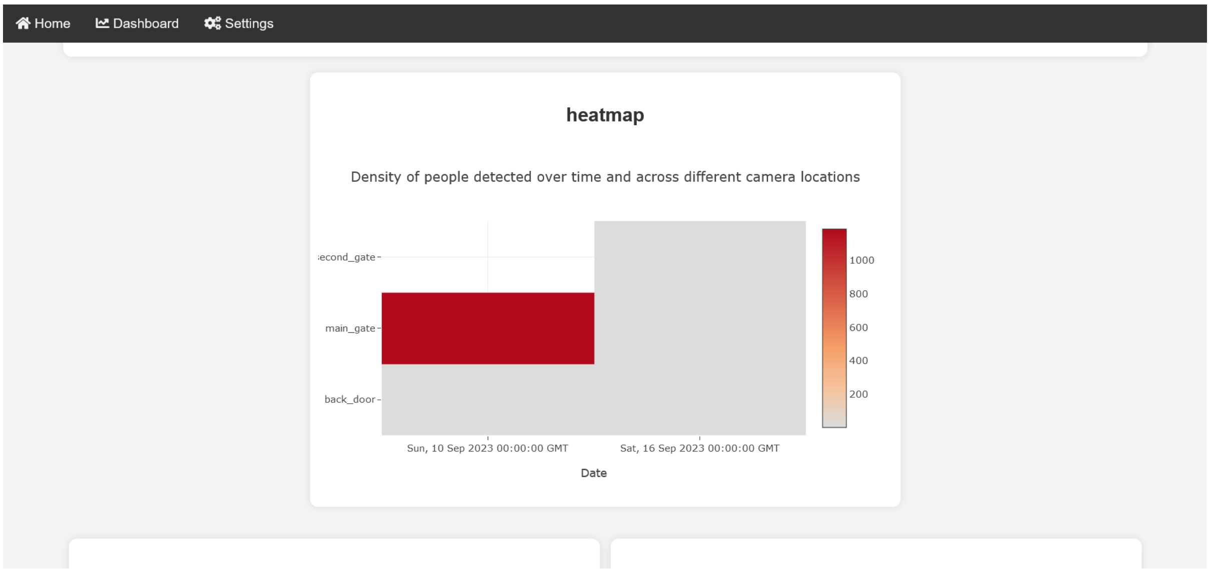
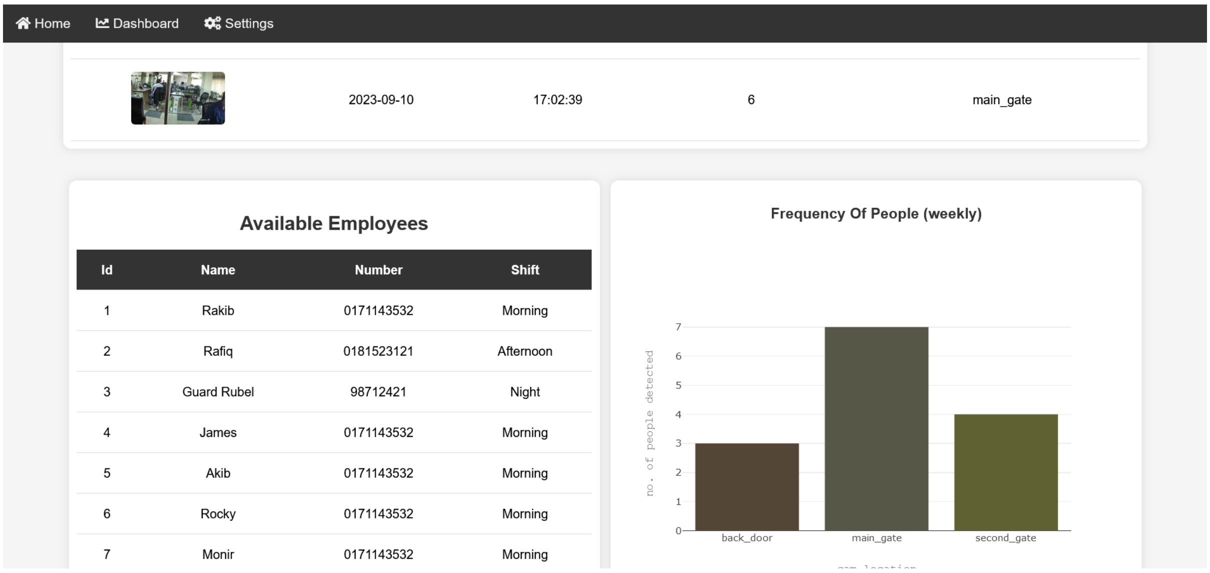

Home
Dashboard
Settings
heatmap
Density of people detected over time and across different camera locations
second_gate
main_gate
back_door
1000
800
600
400
200
Sun, 10 Sep 2023 00:00:00 GMT
Sat, 16 Sep 2023 00:00:00 GMT
Date

Figure 6.4: Heatmap module for InfiltraWatch



2023-09-10 17:02:39 6 main_gate

Available Employees

Id	Name	Number	Shift
1	Rakib	0171143532	Morning
2	Rafiq	0181523121	Afternoon
3	Guard Rubel	98712421	Night
4	James	0171143532	Morning
5	Akib	0171143532	Morning
6	Rocky	0171143532	Morning
7	Monir	0171143532	Morning

Figure 6.5: Bar chart module for InfiltraWatch

Chapter 7

Project as Engineering Problem Analysis

It's crucial to evaluate the impact of the AI-driven surveillance system as an engineering problem that interacts with social norms, the environment, and ethical principles, as well as a technical endeavor.

7.1 Sustainability of the Project/Work

A few key pillars serve as the project's foundation for sustainability:

- **Scalability:** As the facility expands, the system can handle more cameras or environments with greater complexity by utilizing cloud resources and cutting-edge AI models like YOLOv8x.
- **Updating and maintenance:** Thanks to the modular design, parts like the AI model or the notification system can be updated without completely redesigning the system. This indicates that keeping up with the most recent technological developments is possible without making sizable new investments.
- **Energy Efficiency:** New AI models are becoming more energy-efficient, particularly those designed for edge devices. This suggests that operating costs, both monetarily and environmentally, will decline over time.

7.2 Social and Environmental Effects and Analysis

7.2.1 Social Effects

The main advantage is the increased security in industrial settings, which makes workplaces safer and might save lives and property.

- **Job Dynamics:** Less manual surveillance work may be required as automated surveillance becomes more prevalent. However, this also creates opportunities for work in areas such as data analysis and maintaining AI surveillance systems.

7.2.2 Effects on the environment

*** Explain the social and environmental effects of your project/work and analyze them ***

- **Energy Use:** Running AI models continuously uses energy. As was already mentioned, the trend in AI is moving toward models that use less energy.
- **Electronic Waste:** It's important to dispose of outdated hardware in an environmentally friendly way as components age out or become obsolete.
- **Analysis:** By boosting security, the project significantly benefits society. But it's crucial to make sure that the transition as AI and technology advance is easy, perhaps with job retraining programs, to prevent job displacement. While there are some negative environmental effects, this project can benefit from the tech trend toward greener, more sustainable solutions.

7.3 Addressing Ethics and Ethical Issues

7.3.1 Ethical Issues

AI surveillance raises a number of ethical issues, including:

- **Privacy:** Ongoing surveillance may be viewed as an infringement on personal space. The system should be created to alert or activate only during particular circumstances (like unauthorized entries) rather than continuously in order to address this.
- **Bias and Discrimination:** Depending on the data that they are trained on, AI models may occasionally display biases. It's crucial to make sure the system is trained on a variety of datasets and doesn't unintentionally target particular demographics.
- **Data Storage and Protection:** To avoid misuse, the information collected, particularly that about specific individuals, must be safely stored and guarded.

7.3.2 Solutions

- **Transparency:** Gaining the public's trust can be facilitated by making the operation of the AI system transparent.
- **Regular Audits:** Regularly auditing the system for biases or failures can ensure that it remains fair and effective.

- **Data Encryption:** Making use of effective encryption methods can guarantee that the data is kept safe from potential hackers and misuse.

Chapter 8

Lesson Learned

This internship's journey was demanding and illuminating at the same time. Realworld issues were faced and solutions were developed, providing invaluable practical experience that will undoubtedly direct future endeavors.

8.1 Problems Faced During this Period

- **Real-time RTSP Stream Processing:** The inability to use the live camera to process the RTSP stream in real-time was a significant problem. Real-time threat detection and intervention were difficult due to the delay, which could be anywhere between a few seconds and one or two minutes.
- **YOLOv8x Model Resource Consumption:** The YOLOv8x model required a lot of resources despite being effective. For processing a single camera source, about 1.4 GBs of GPU memory and 4 GBs of RAM were used. This presented a challenge in terms of scaling, particularly when taking into account the extension to multiple camera feeds, such as 50 or even 100.
- **Time Mangement:** Managing the demanding requirements of university coursework alongside the obligations and difficulties of the internship was another challenge. It tested my ability to manage my time as well as my mental stamina.

8.2 Solution of those Problems

- **Real-time RTSP Stream Processing:** Images were captured from the default cctv camera's motion detection feature and then the AI model scanned for humans on the frames
- **YOLOv8x Model Resource Consumption:** Fixing the first issue fixed this issue as only one instance of AI model loading could scan multiple sources of frames.
- **Time Mangement:** Allocating time and prioritizing work help me solve this problem

Chapter 9

Future Work & Conclusion

The potential uses and advancements of any system change constantly as technology does. In light of the work completed during this internship, the AI surveillance system has a wide range of potential areas for exploration and improvement.

9.1 Future Works

Improved Model Training: As AI technology develops, newer iterations of the YOLO model or even entirely new architectures may be developed. Utilizing these developments could increase detection accuracy and speed even further.

Integration of Additional Sensors: The detection abilities could be enhanced further by integrating thermal cameras or infrared sensors, particularly in low light or challenging environmental conditions.

Scalability for Larger Complexes: While the current solution is made for a single factory, future research might concentrate on developing a central AI surveillance system capable of keeping an eye on several factories or larger industrial complexes.

Increasing Resource Efficiency: Ongoing research into optimizing the AI model's resource usage may make it possible to run more video streams concurrently without experiencing performance issues.

Advanced Alert Systems: The incorporation of advanced alert systems that, for example, could directly communicate with regional law enforcement or security companies, ensuring a quick on-the-ground response when a breach is discovered.

9.2 Conclusion

It has been challenging and rewarding to develop an AI-driven surveillance system for use in industrial settings. In addition to demonstrating the strength and potential of integrating AI with current infrastructure, this project also demonstrated the value of ongoing innovation in ensuring safety and security. The solutions created during the internship provided immediate relief while also laying the groundwork for future development. The project's technical demands and academic obligations had to be balanced, which was a crucial lesson in time management and prioritization.

While the current system significantly outperforms more established surveillance techniques, there is a vast ocean of potential in the field of AI and surveillance. It is essential that we navigate this area going forward with an emphasis on ethics, privacy, and the advancement of society as a whole. Despite the difficulties along the way, there are enormous potential advantages for industrial security and other areas.

Bibliography

[1] X. Wang, "Deep learning in object recognition, detection, and segmentation," 2016. Deep Learning in Object Recognition, Detection, and Segmentation.

[2] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016.

[3] I. Ryabchikov, N. Teslya, and N. Druzhinin, "Integrating computer vision technologies for smart surveillance purpose," in *2020 26th Conference of Open Innovations Association (FRUCT)*, (Yaroslavl, Russia), pp. 392–401, 2020.

[4] J. Terven and D. Cordova-Esparza, "A comprehensive review of yolo: From yolov1 to yolov8 and beyond," *arXiv preprint arXiv:2304.00501*, 2023.

[5] C. Shorten and T. M. Khoshgoftaar, "A survey on image data augmentation for deep learning," *Journal of Big Data*, 2019.

[6] X. Zhou, X. Xu, W. Liang, Z. Zeng, and Z. Yan, "Deep-learning-enhanced multitarget detection for end–edge–cloud surveillance in smart iot," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12588–12596, 2021.

[7] M. Hilb, "Toward artificial governance? the role of artificial intelligence in shaping the future of corporate governance," *Journal of Management and Governance*, vol. 24, pp. 851–870, 2020.

[8] M. Sharif, S. Bhagavatula, L. Bauer, and M. K. Reiter, "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[9] M. Sabokrou, M. Fayyaz, M. Fathy, Z. Moayed, and R. Klette, "Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes," *Computer Vision and Image Understanding*, vol. 172, pp. 88–97, 2018.

[10] "Coco dataset." `https://cocodataset.org/`. Accessed: 2023-06-12.

[11] F. Deeba, S. Kun, M. Shaikh, F. A. Dharejo, S. Hayat, and P. Suwansrikham, "Data transformation of uml diagram by using model driven architecture," in *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pp. 300–303, IEEE, 2018.

[12] A. Jovic, D. Kukolja, K. Jozic, and M. Cifrek, "Use case diagram based scenarios design for a biomedical time-series analysis web platform," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 310–315, IEEE, 2016.

[13] Y. B. Hlaoui and L. J. BenAyed, "Extended uml activity diagram for composing grid services workflows," in *2008 Third International Conference on Risks and Security of Internet and Systems*, pp. 207–212, IEEE, 2008.

[14] X. Kong and L. Liu, "A web application architecture framework," in *Australian World Wide Web Conference*, Norsearch Reprographics, 2004.

TEACHETH MAN THAT WHICH HE KNEW NOT
IUB
INDEPENDENT UNIVERSITY

An Undergraduate Internship/Project on yourTopic

By

Azwad Fawad Hasan

Student ID: **2020222**

Summer, 2023

Consent from Supervisor

The student modified the internship final report as per the recommendations made by his/her academic supervisor and/or panel members during and/or before final viva, and the department can use this version for archiving as well as the OBE course material for CSE499.

This internship report is checked with Turnitin and/or Ithenticate plagiarism checker, and the score is:

Turnitin Score (%): 13
Ithenticate Score (%): 13

Mahir Al Kamal
(Signature of the Supervisor)

Mahir Al Kamal
Department of Computer Science & Engineering
Independent University, Bangladesh