VIGILANCE 360
AN INTERNSHIP REPORT

Submitted by

Payal Rajput - 200103061007
Dhruv Gor - 200103062014
Diya Patel - 200103062021
Kavisha Patel – 210133061004
Gaurav Sharma -200103062029
Riya Mishra – 210133061003
Rahul Kothari – 210133061002
Shruti Kharate – 200103062016
Nish Shah - 210133062011

BACHELOR OF TECHNOLOGY

in

COMPUTER ENGINEERING WITH ML-AI

College of Technology
Silver Oak College of Engineering & Technology

Silver Oak University, Ahmedabad

April, 2024

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Payal Rajput** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25

A/ Prof. Sanket Shah
Internal Guide

Dr. Satvik Khara
Head of the Department

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Dhruv Gor** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25

A/ Prof. Sanket Shah	**Dr. Satvik Khara**
Internal Guide	**Head of the Department**

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Shruti Kharate** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25.

A/ Prof. Sanket Shah **Internal Guide**	**DR. Satvik Khara** **Head of the Department**

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Vigilance 360** has been carried out by **Gaurav Sharma** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25.

A/ Prof. Sanket Shah	**DR. Satvik Khara**
Internal Guide	**Head of the Department**

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Diya Patel** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25

A/ Prof. Sanket Shah
Internal Guide

DR. Satvik Khara
Head of the Department

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Rahul Kothari** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2022-23.

A/ Prof. Sanket Shah	**DR. Satvik Khara**
Internal Guide	**Head of the Department**

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Riya Mishra** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25

A/ Prof. Sanket Shah
Internal Guide

DR. Satvik Khara
Head of the Department

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Kavisha Patel** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25

A/ Prof. Sanket Shah
Internal Guide

DR. Satvik Khara
Head of the Department

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

CERTIFICATE

This is to certify that the Internship report submitted along with the Internship entitled **Python with AI Intern** has been carried out by **Nish Shah** under my guidance in partial fulfillment for the Bachelor of Technology in Computer Engineering (MLAI), 8th Semester of Silver Oak University, Ahmedabad during the academic year 2024-25

A/ Prof. Sanket Shah
Internal Guide

DR. Satvik Khara
Head of the Department

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axisray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Payal Rajput

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axisray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Dhruv Gor

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axisray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student	**Sign of student**
Diya Patel	

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axisray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Kavisha Patel

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axisray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student's reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Gaurav Sharma

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axisray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Riya Mishra

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axiray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student's reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Rahul Kothari

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axiray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Shruti Kharate

Silver Oak College of Engineering & Technology

Opp. Bhagwat Vidhyapith, S.G. Highway, Ahmedabad-382481

DECLARATION

We hereby declare that the Internship report submitted along with the Internship entitled **Python with AI Intern** submitted in partial fulfillment for the **Bachelor of Technology in Computer Engineering (MLAI)** to Silver Oak University, Ahmedabad, is a Bonafede record of original project work carried out by me at **Axiray** under the supervision of **Mr. Asit Pandit** and that no part of this report has been directly copied from any student‘s reports or taken from any other source, without providing due

Name of the Student **Sign of student**

Nish Shah

ACKNOWLEDGEMENT

I wish to express my heartfelt appreciation to all those who have contributed to this project, both explicitly and implicitly, without the co-operation of whom, it would not have been possible to complete this project. I would like to thank our H.O.D Dr. Satvik Khara as well as (Internal Guide) Mr. Sanket Shah for constantly guiding and showing us the correct path to reach towards our desired goal. Also, I thank them for sharing their experience, knowledge, and valuable time with me and showing their concern for my project to make it better. I also thank all the other faculties who directly or indirectly supported me in making my project successful by sharing their ideas and knowledge.

Abstract

Vigilance 360 is an enhanced safety system that combines object detection and facial recognition technology. Utilizing Mediapipe for facial recognition and YOLOv8 for object detection, the system provides extensive surveillance coverage, allowing for real-time pre-incident detection. It can follow people inside the ATM area, identify between faces that are covered and those that are not, and detect firearms. The technology offers proactive security monitoring and quick response to possible threats, setting a new benchmark for safety in ATM environments.

List of Figures

List of Tables

Abbreviations

ATM: Automated Teller Machine

UAT: User Acceptance Testing

SQL: Structured Query Language

MYSQL: MySQL Database Management System

GUI: Graphical User Interface

AI: Artificial Intelligence

CCTV: Closed-Circuit Television

ROI: Region of Interest

API: Application Programming Interface

IT: Information Technology

YOLO: You Only Look Once

Table of Contents

CHAPTER 1: OVERVIEW OF THE COMPANY

1.1 HISTORY

Axisray, founded by seasoned entrepreneurs, aimed to transform India's R&D and Product Engineering landscape. With guiding principles of collaboration, client-centricity, and innovation, Axisray delivers cutting-edge solutions across diverse industries like Healthcare, E-commerce, and Construction. Embracing AI, Big Data, and IoT, Axisray empowers startups and drives progress in the digital age. Positioned as a catalyst for transformative change, Axisray remains committed to pushing the boundaries of possibility and driving innovation, cementing its reputation as a trusted partner in navigating the complexities of the modern technological landscape.

1.2 SCOPE OF WORK

- **Cloud Services:** It offers comprehensive cloud solutions tailored to meet the scalability, security, and performance needs of businesses, enabling seamless migration, management, and optimization of cloud environments.
- **Big Data and Business Intelligence:** Leveraging advanced analytics and data visualization techniques, It empowers organizations to derive actionable insights from vast volumes of data, driving informed decision-making and enhancing operational efficiency.
- **Artificial Intelligence:** It develops AI-powered solutions that automate tasks, personalize customer experiences, and unlock new opportunities for innovation across various industries, harnessing the transformative potential of machine learning and natural language processing.
- **Internet of Things (IoT):** By integrating IoT technologies into existing systems and processes, It enables real-time monitoring, predictive maintenance, and data-driven decision-making, paving the way for smarter, more connected ecosystems.

- **Enterprise Solution Development:** It specializes in the design, development, and implementation of scalable enterprise solutions that streamline workflows, improve collaboration, and drive digital transformation initiatives.
- **Chatbots and Voice Solutions:** It creates intelligent chatbots and voice-enabled applications that enhance customer engagement, automate support processes, and deliver personalized experiences through natural language interfaces.
- **Video Streaming Services:** It delivers end-to-end video streaming solutions that enable seamless content delivery, live event broadcasting, and interactive multimedia experiences, leveraging advanced encoding, transcoding, and streaming technologies.

1.3 INFRASTRUCTURE CAPACITY

There are 51-200 employees in the company.

CHAPTER 2: OVERVIEW OF DIFFERENT DEPARTMENTS OF THE ORGANIZATION

2.1 THE WORK BEING CARRIED OUT IN EACH DEPARTMENT

- **Development/Engineering:** This department is responsible for designing, developing, and maintaining software applications, websites, or other digital products. It may include roles such as software engineers, web developers, mobile app developers, etc.
- **Quality Assurance (QA) / Testing:** QA engineers are responsible for ensuring the quality and reliability of software products by testing them thoroughly. This department conducts various types of testing, including functional testing, performance testing, and security testing.
- **Project Management:** Project managers oversee the planning, execution, and delivery of IT projects. They coordinate with different teams to ensure that projects are completed on time and within budget.
- **Human Resources (HR):** The HR department manages recruitment, employee relations, training, and other personnel-related matters. It ensures that the company's workforce is skilled, motivated, and compliant with relevant regulations.
- **Finance/Accounting:** The finance and accounting department handles financial transactions, budgeting, payroll, taxes, and financial reporting. It ensures that the company's financial operations are accurate, efficient, and compliant.
- **Research and Development (R&D):** The R&D department focuses on innovation and the development of new technologies, products, or solutions. It conducts research, experiments, and prototyping to drive the company's future growth.

2.2 TECHNICAL SPECIPICATION OF MAJOR EQUIPMENT USED IN EACH DEPARTMENT

- **Development/Engineering:** High-performance desktop computers with powerful processors, ample RAM and dedicated graphics cards. Development software and tools such as Integrated Development Environments (IDEs), code editors, version control systems and debugging tools. Virtualization software and platforms for testing and deployment, such as Docker, Kubernetes, or virtual machines. Test devices for compatibility testing, such as smartphones, tablets, and different web browsers.

Quality Assurance (QA) / Testing: Testing machines or devices with various operating systems and configurations for compatibility testing. Automated testing tools and frameworks for test automation.

- Load testing tools for performance testing. Security testing tools for vulnerability assessment and penetration testing.
- **Project Management:** Project management software and tools for task management, scheduling, and collaboration. Communication and collaboration tools such as Microsoft Teams for team meetings, discussions, and file sharing. Cloud-based project management platforms for remote access and scalability.
- **Human Resources (HR):** Human resource management systems for employee records, payroll, benefits administration, and performance management. Recruitment and applicant tracking systems for job postings, candidate sourcing, and hiring processes. Learning management systems for employee training, onboarding, and skills development.
- **Finance/Accounting:** Accounting software or enterprise resource planning (ERP) systems for financial transactions, budgeting, and financial reporting. Payroll processing software for managing employee compensation, taxes, and deductions. Expense management tools for tracking business expenses, reimbursements, and approvals.
- **Research and Development (R&D):** Research tools and databases for gathering information, academic papers, patents, and industry trends (e.g., IEEE Xplore, Google Scholar). Prototyping and development platforms for experimenting with new technologies, frameworks, and programming languages. Collaboration tools for sharing research findings, brainstorming ideas, and coordinating R&D projects.

2.3 SCHEMETIC LAYOUT FOR SEQUENCE OF OPERATIONS

2.3.1 Development Phase:

Department: Development/Engineering

Equipment: High-performance desktop or laptop computers, integrated development environments (IDEs), version control systems (e.g., Git) Sequence of Operation: Developers receive project requirements and specifications. They use IDEs and version control systems to write and manage code. Code changes are reviewed, tested, and committed to the version control system. Continuous integration and automated testing processes are triggered.

2.3.2 Quality Assurance Phase:

Department: Quality Assurance (QA) / Testing

Equipment: Testing devices, automated testing tools (e.g., Selenium), bug tracking software Sequence of Operation: Testers receive builds or code changes from the development team. They perform manual and automated testing to identify bugs and verify functionality. Bug reports are logged in the bug tracking software, and issues are prioritized. Test results and bug reports are communicated to the development team for resolution.

2.3.3 Deployment Phase:

Department: Infrastructure/Operations

Equipment: Servers, networking equipment, monitoring tools Sequence of Operation: Operations team receives approved code changes from the development team. They deploy the application or updates to staging or production servers. Monitoring tools are used to ensure the health and performance of deployed applications. Any issues or alerts are addressed promptly to minimize downtime.

2.3.4 Maintenance Phase:

Department: Infrastructure/Operations

Equipment: Configuration management tools, monitoring and alerting systems Sequence of Operation: Operations team performs routine maintenance tasks on servers and network infrastructure. They apply security patches, update software, and perform backups as needed. Monitoring systems alert for any anomalies or potential issues. Proactive measures are taken to prevent system failures and ensure uptime.

2.3.5 Continuous Improvement Phase:

Department: Research and Development (R&D)

Equipment: High-performance computing resources, collaboration platforms Sequence of Operation: R&D team analyzes data and metrics from development, testing, and deployment phases. They identify areas for improvement in processes, tools, and product features. Prototypes and experiments are conducted to test new ideas and technologies. Findings and recommendations are shared with relevant departments for implementation.

2.4 EXPLAIN IN DETAIL ABOUT EACH STAGE OF PRODUCTION

2.4.1 Development Phase:

- Requirement Analysis: Understanding client needs and project specifications.
- Coding: Writing source code using programming languages and integrated development environments (IDEs).
- Version Control: Managing code changes and collaboration using version control systems like Git.
- Code Review: Reviewing code changes by peers to ensure quality and adherence to coding standards.

2.4.2 Quality Assurance Phase:

- Manual Testing: Testers execute test cases manually to validate software functionality.
- Automated Testing: Writing and executing automated test scripts using tools like Selenium for regression testing.
- Bug Tracking: Logging and tracking defects using bug tracking software like Jira.
- Test Reporting: Generating reports on test coverage, pass/fail rates, and defect metrics.

2.4.3 Deployment Phase:

- Continuous Integration/Deployment (CI/CD): Automating the process of building, testing, and deploying software changes using CI/CD pipelines.
- Server Configuration: Setting up servers and configuring software environments for deployment.
- Deployment Planning: Planning and scheduling deployment activities to minimize downtime and disruption.
- Rollback Strategy: Establishing procedures for rolling back changes in case of deployment failures or issues.

2.4.4 Maintenance Phase:

- Patch Management: Applying security patches and updates to software components to address vulnerabilities and bugs.
- Performance Monitoring: Monitoring system performance and resource utilization to identify and address bottlenecks or issues.
- Backup and Recovery: Implementing regular data backups and recovery procedures to prevent data loss. Capacity
- Planning: Planning and provisioning resources to accommodate growth and demand.

2.4.5 Continuous Improvement Phase:

- Data Analysis: Analyzing data and metrics from various stages of the software development lifecycle to identify trends, patterns, and areas for improvement.
- Research and Development: Exploring new technologies, tools, and methodologies to enhance product features and capabilities.
- Feedback Collection: Soliciting feedback from stakeholders, end-users, and internal teams to gather insights for improvement.
- Experimentation: Conducting experiments and pilots to test hypotheses and validate ideas for potential implementation

Chapter 3: Introduction to Project

3.1 Project Summary

The "Vigilance 360" project is a comprehensive solution aimed at enhancing security measures in Automated Teller Machines (ATMs) by implementing pre-incident detection systems. Using dual-camera surveillance, it identifies individuals attempting entry with covered faces and stores relevant data in the database. The system also detects and stores data about individuals carrying harmful tools or heavy metals. The project provides occupancy monitoring for maintaining a safe environment and implements a user-specific session duration to enhance operational efficiency, ensuring a secure and protected ATM environment.

3.2 Purpose

The purpose of the project is to develop a robust security solution for ATMs that proactively detects and addresses potential security threats before they escalate. By integrating advanced surveillance technology and database storage mechanisms, the system aims to minimize the risk of security breaches and ensure the safety of ATM users and assets.

3.3 Objective

- The main objective of the project is to design and implement a pre-incident detection system for ATMs that:
- Identifies individuals attempting entry with covered faces.
- Detects and stores data about individuals carrying harmful tools or heavy metals.
- Provides occupancy monitoring to maintain a safe environment.
- Enhances operational efficiency through user-specific session duration.

3.4 Scope

- The project can Detect unauthorized entry into ATM premises through dual-camera surveillance.
- Identify individuals with covered faces and store relevant data in the database.
- Detect and store data about individuals carrying harmful tools or heavy metals.
- Monitor occupancy levels to ensure a safe environment.
- Implement user-specific session duration to optimize operational efficiency.

The project cannot:

- Guarantee complete elimination of security threats.
- Provide physical intervention in case of security breaches.
- Replace the need for human security personnel entirely.

3.5 Technology and Literature Review

The project incorporates state-of-the-art surveillance technology, including YOLOv8 for person tracking and object detection. The use of YOLOv8 enables efficient real-time detection of covered faces and potential threats like weapons. Additionally, the project utilizes MYSQL database using SQLyog tool for database connectivity, ensuring efficient storage and retrieval of relevant data.

3.6 Project Planning

3.6.1 Project Development Approach and Justification

The development approach for the "Vigilance 360" project follows an iterative and collaborative process. This approach allows for continuous feedback and refinement, ensuring that the final solution meets the requirements effectively. Justification for this approach lies in its flexibility to adapt to evolving project needs and incorporate stakeholder feedback throughout the development lifecycle. Additionally, the iterative nature of the approach facilitates early detection and resolution of potential issues, leading to a more robust and reliable system.

3.6.2 Project Effort and Time, Cost Estimation

Effort and time estimation for the project are based on the complexity of implementing various features such as dual-camera surveillance, object detection, and database integration. Cost estimation includes expenses related to hardware procurement, software development, testing, and deployment. The project timeline is divided into distinct phases, each with specific deliverable and milestones. Effort and time estimates are regularly monitored and adjusted based on project progress and feedback from stakeholders.

3.6.3 Roles and Responsibilities

- Project Manager: Oversees the overall planning, execution, and delivery of the project. Responsible for coordinating team activities, managing resources, and ensuring adherence to project timelines and objectives.
- Software Developers: Responsible for designing, implementing, and testing the software components of the system, including surveillance algorithms, object detection, and database integration.
- Database Administrator: Manages the design, implementation, and maintenance of the project database, ensuring data integrity, security, and optimal performance.
- Quality Assurance Engineer: Conducts thorough testing of the system to identify and rectify any bugs or issues before deployment. Also responsible for ensuring compliance with quality standards and specifications.

3.6.4 Group Dependencies

- The success of the project relies on effective collaboration and communication among team members and external stakeholders. Key dependencies include:
- Timely availability of hardware components such as cameras and sensors for system integration.
- Access to relevant datasets for training and testing object detection algorithms.
- Coordination with security personnel for real-world testing and validation of the system.
- Collaboration with IT departments for network integration system within ATM environments

CHAPTER - 4 SYSTEM ANALYSIS

4.1 Study of Current System

Currently, many ATMs rely on basic surveillance systems that may not effectively detect or prevent security threats. These systems often lack sophisticated features such as real-time object detection and pre-incident alerts.

4.2 Problem and Weaknesses of Current System

- Limited surveillance capabilities: Current systems may only provide basic video monitoring without advanced features like object detection.
- Reactive approach to security: Without pre-incident detection, security personnel can only respond to security threats after they occur, increasing the risk of harm to individuals and damage to property.
- Lack of integration: Current systems may not integrate seamlessly with other security measures or databases, leading to disjointed security efforts.

4.3 Requirements of New System

- The new system should:
- Provide advanced surveillance capabilities, including real-time object detection and precise storage of relevant data in the database.
- Integrate seamlessly with existing security measures and databases.
- Be user-friendly and easily accessible for security personnel to monitor and manage.

4.4 System Feasibility

4.4.1 Does the System Contribute to the Overall Objectives of the Organization?

Yes, the system contributes to the overall objective of enhancing security measures in ATM environments by proactively detecting and addressing potential security threats.

4.4.2 Can the System be Implemented Using the Current Technology and Within the Given Cost and Schedule Constraints?

Yes, the system can be implemented using existing technologies such as YOLOv8 for object detection and MYSQL database using SQLyog tool for database connectivity. Efforts will be made to ensure that the project remains within the allocated budget and timeline.

4.4.3 Can the System be Integrated with Other Systems which are Already in Place?

Yes, the system is designed to be integrated seamlessly with existing security systems and databases, enhancing overall security measures in ATM environments.

4.5 Activity in New System

- Dual-camera surveillance for comprehensive coverage.
- Real-time object detection for identifying unauthorized entry and potential security threats.
- Database storage of relevant data with date and time information.
- Integration with existing security measures and databases.
- User-friendly interface for easy monitoring and management

4.6 Features of New System

- Dual-Camera Surveillance: The system incorporates dual-camera surveillance to provide comprehensive coverage of the ATM environment. This allows for monitoring both the inner and outer areas of the ATM, enhancing security measures.

- Real-Time Object Detection: Utilizing advanced object detection algorithms, the system can identify unauthorized entry, suspicious activities, and potential security threats in real-time. This feature enables security personnel to respond promptly to security incidents.

- Database Integration: The system seamlessly integrates with a MYSQL database using SQLyog tool for efficient storage and retrieval of surveillance data, detected anomalies, user sessions, and system logs. This enables security personnel to access and review relevant data for investigation and analysis.

- User-Friendly Interface: The system features a user-friendly interface that allows security personnel to easily navigate and interact with the system. The interface provides intuitive controls for initiating surveillance, accessing database information, and receiving real-time alerts.

- Anomaly Analysis and Reporting: The system analyzes detected anomalies and provides detailed reports to security personnel. These reports include information on the type and severity of anomalies detected, as well as recommendations for response and mitigation strategies.

- Integration with Existing Security Measures: The system is designed to seamlessly integrate with existing security measures and protocols in ATM environments. This enables security personnel to augment their existing security infrastructure with advanced surveillance and detection capabilities.

- Scalability and Flexibility: The system is scalable and flexible, allowing for easy expansion and adaptation to meet evolving security requirements. It can accommodate changes in ATM configurations, security protocols, and regulatory requirements without compromising performance or reliability.

4.7 List Main Modules

1. Surveillance Module: This module is responsible for capturing and monitoring the ATM environment using dual-camera surveillance. It includes functionalities for initiating surveillance, capturing footage, and streaming live feeds to security personnel.

2. Object Detection Module: The object detection module utilizes advanced algorithms to analyze surveillance footage in real-time and detect potential security threats or anomalies. It identifies objects such as covered faces, suspicious activities, or individuals carrying harmful tools, enabling prompt response by security personnel.

3. Database Storage Module: This module manages the storage and retrieval of surveillance data, detected anomalies, user sessions, and system logs in a MYSQL database using SQLyog tool. It ensures efficient organization and accessibility of data for further analysis and investigation.

4. Integration Module: The integration module facilitates seamless integration of various system components, including surveillance, object detection, and database management. It ensures smooth communication and collaboration between different modules to enhance overall system functionality.

5. User Interface Module: The user interface module provides a user-friendly interface for security personnel to interact with the system. It includes features such as dashboard navigation, surveillance mode selection, database access, and real-time alerts/notification display, ensuring ease of use and effective monitoring of ATM security.

4.8 Selection of Hardware, Software, Algorithms, Methodology, Techniques and Approaches

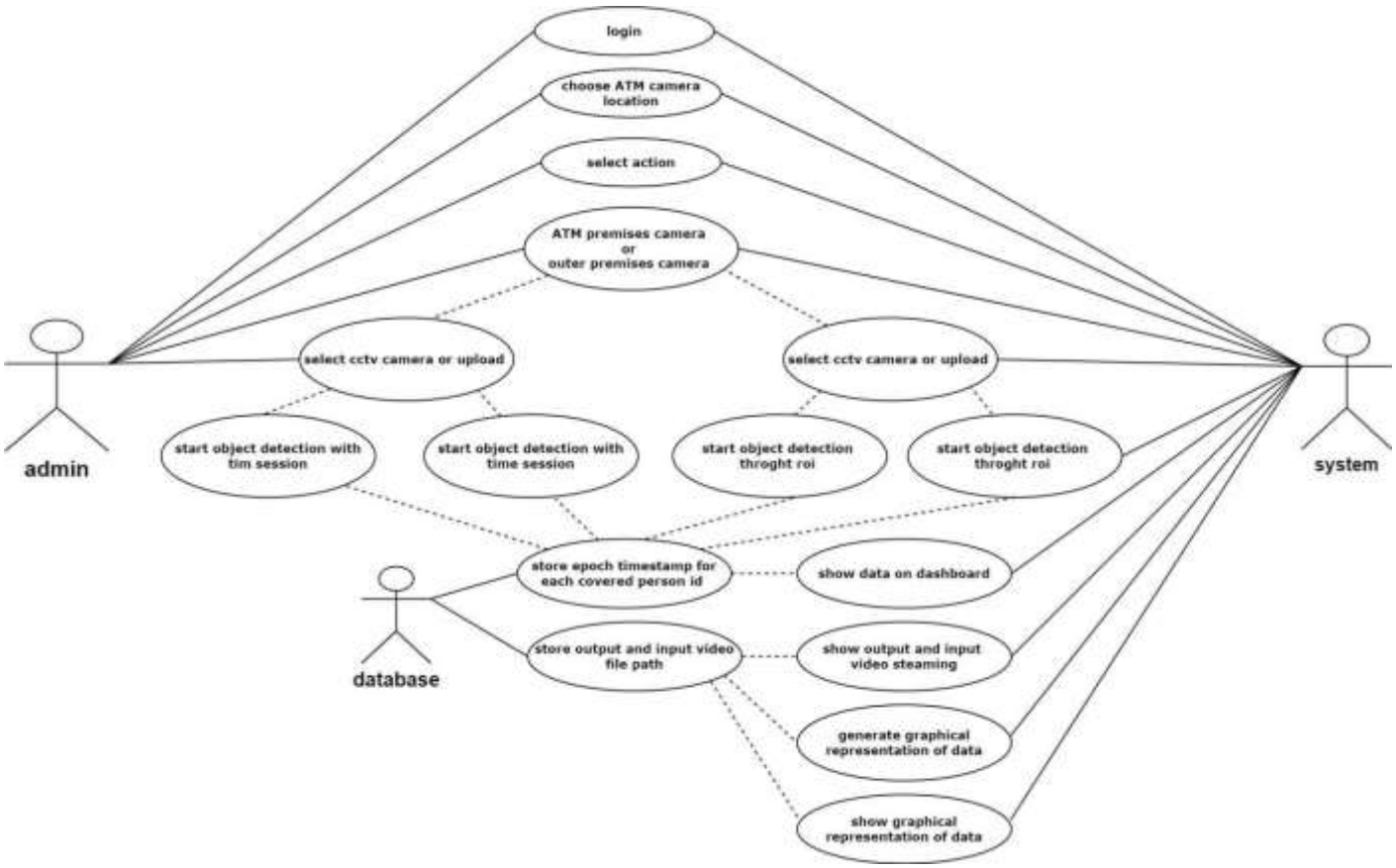
- Hardware: High-resolution cameras for optimal surveillance coverage.
- Software: YOLOv8 for real-time object detection, MYSQL database using SQLyog tool for database connectivity.
- Algorithms: Object detection algorithms for identifying potential security threats.
- Methodology: Iterative development approach for continuous improvement and refinement.
- Techniques: Dual-camera surveillance for comprehensive coverage and accuracy.
- Approaches: Integration of existing technologies and systems for seamless operation.

CHAPTER 5 - SYSTEM DESIGN

5.1 System Design & Methodology

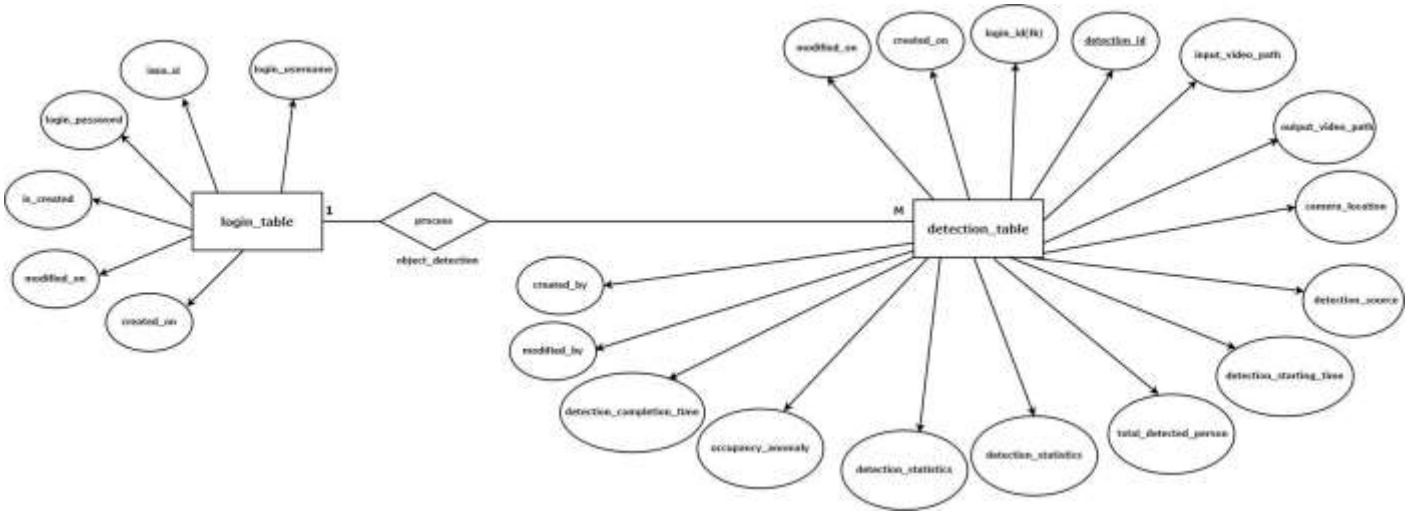
The system design for Vigilance 360 follows a modular and scalable approach. The methodology employed includes iterative development cycles to continuously refine and improve system functionalities. Each module is designed to handle specific tasks, such as surveillance, object detection, database integration, and user interface, allowing for easier maintenance and future enhancements

Fig 5.1.1 USE CASE DIAGRAM



- The USE case outlines the process by which users interact with the Vigilance 360 platform to enhance security measures in Automated Teller Machines (ATMs). The primary actor in this scenario is the security personnel, who access the platform and utilize its functionalities to monitor and manage security threats.
- Once logged in, the security personnel navigate to the surveillance interface and initiate dual-camera surveillance.
- Security personnel have access to the Vigilance 360 platform and can monitor surveillance feeds from both inner and outer cameras.
- After initiating surveillance, security personnel can detect unauthorized entry or suspicious activities by analyzing the surveillance feeds.
- The system analyzes the surveillance footage and detects any anomalies, such as covered faces or individuals carrying harmful tools or heavy metals.
- Upon detecting anomalies, the system alerts security personnel and stores relevant data in the database.
- Security personnel can access the database to view stored data and review detected anomalies.

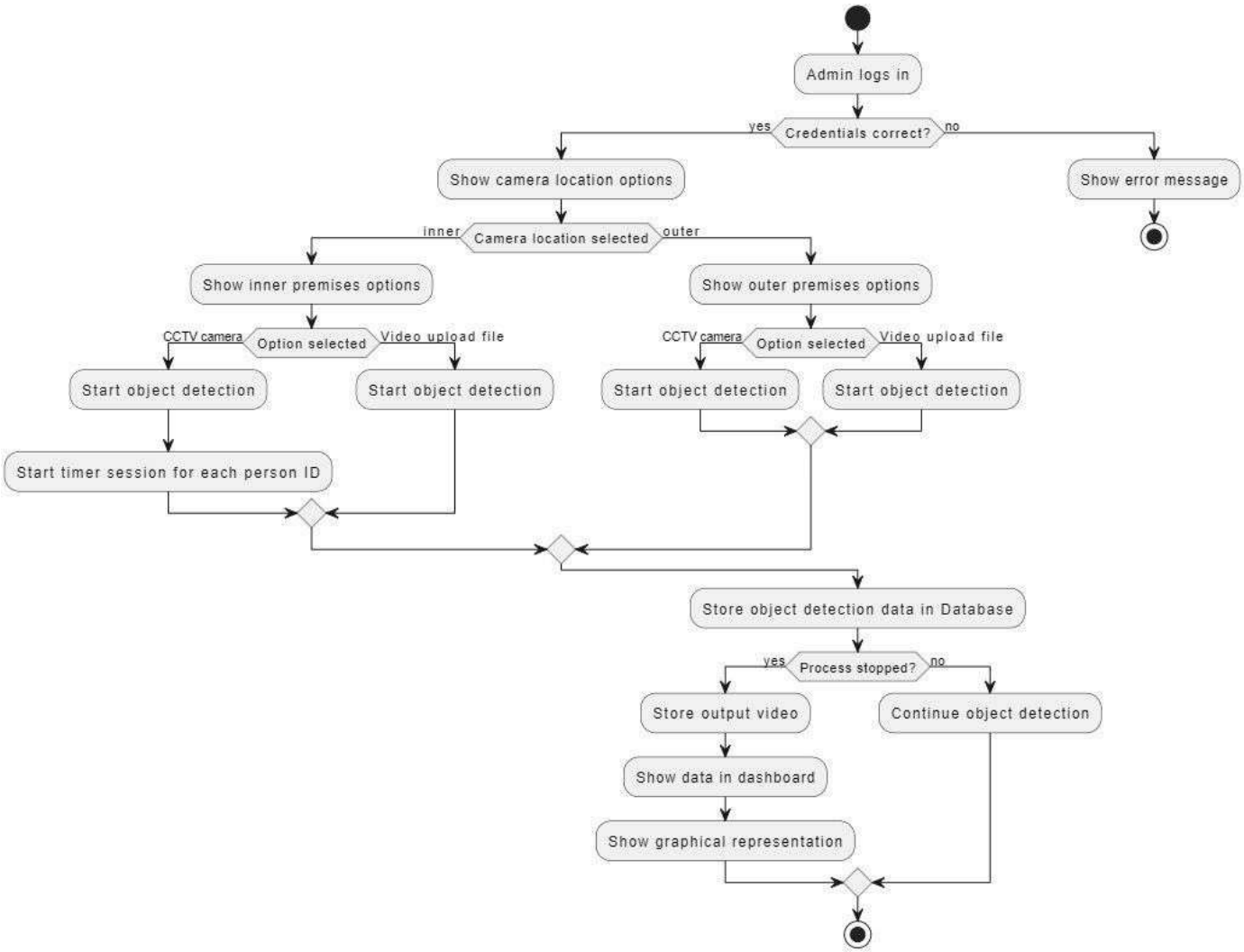
Fig 5.1.2 ER DIAGRAM



The relationships in the E-R diagram indicate how entities are related to each other within the Vigilance 360 system:

- Users interact with the system by accessing the dashboard and monitoring surveillance feeds.
- Surveillance feeds are associated with users and can be analyzed for security threats.
- Detected anomalies, such as covered faces or individuals carrying harmful tools, are related to surveillance feeds and provide additional information for security personnel.
- Security personnel can upload documents containing relevant information about security protocols or incidents.
- Documents are managed by the system and can be accessed by security personnel for reference.
- Administrators have specific permissions to modify system settings, view surveillance data, and manage user access within the system.

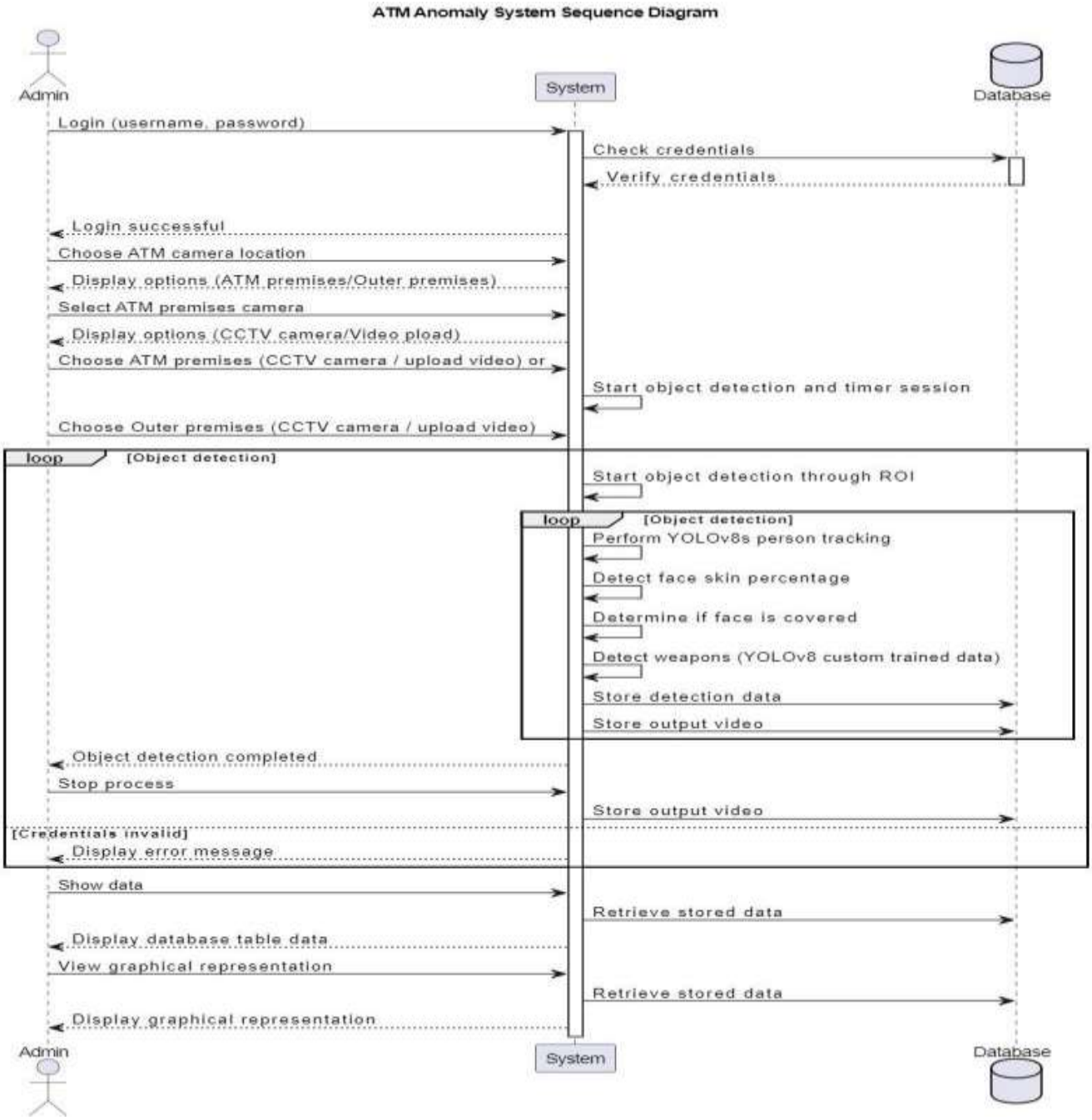
Fig 5.1.3 ACTIVITY DIAGRAM



- The activity diagram illustrates the workflow within the Vigilance 360 system, detailing the sequence of actions performed by users and the system itself:
- Security personnel initiate the system by logging in and accessing the dashboard.
- Upon accessing the dashboard, security personnel have the option to select the surveillance mode (inner or outer camera).

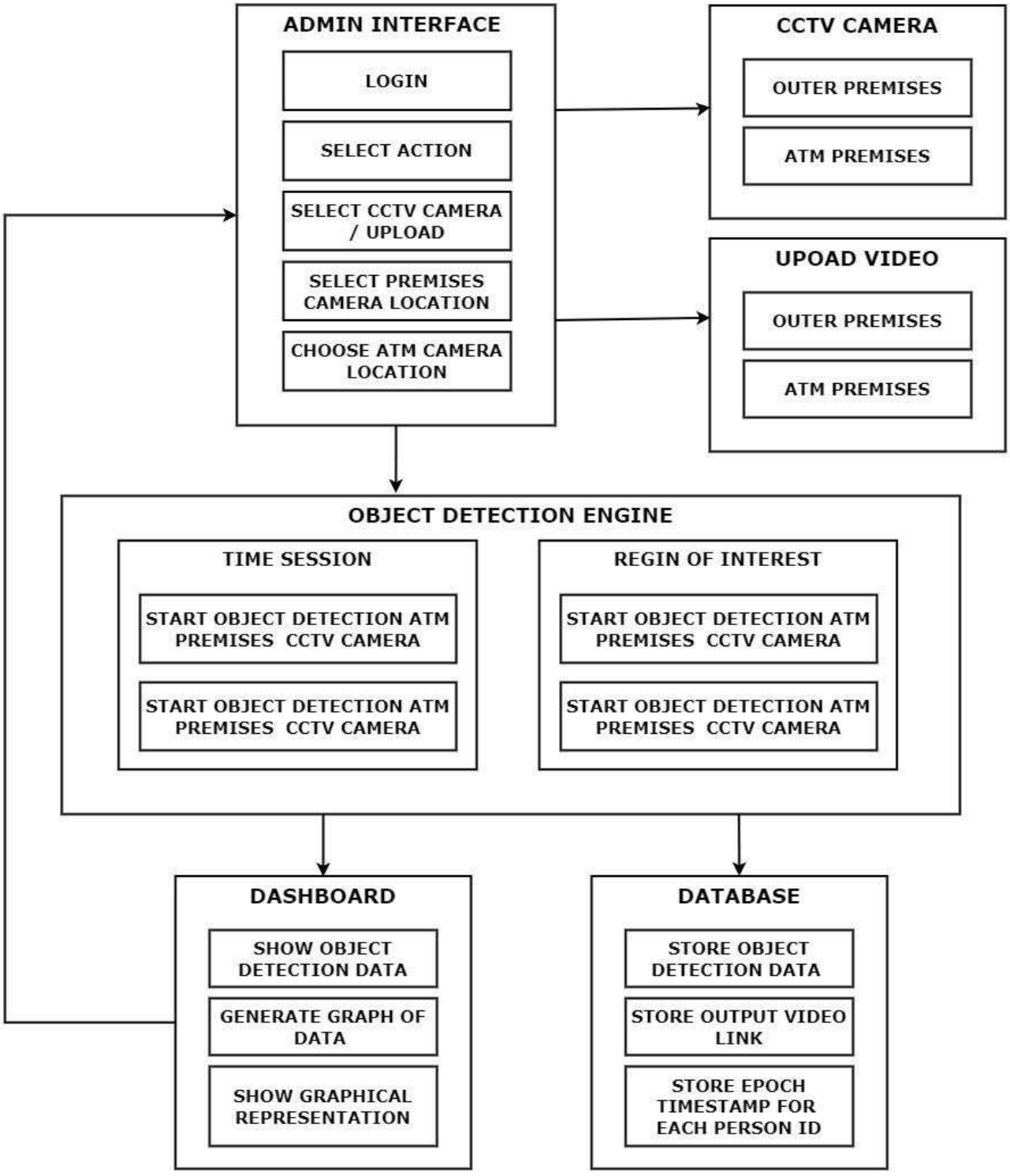
- If inner camera mode is selected, the system initiates dual-camera surveillance and begins monitoring for security threats.
- If outer camera mode is selected, the system activates the web camera and initiates surveillance of the ATM surroundings.
- As surveillance is ongoing, the system continuously analyzes the footage for anomalies, such as covered faces or suspicious activities.
- Upon detecting anomalies, the system alerts security personnel and stores relevant data in the database for further analysis.
- Security personnel can access the database to review stored data and investigate detected anomalies.
- The activity diagram provides a visual representation of the workflow within the Vigilance 360 system, highlighting the sequence of actions and interactions between users and the system components.

Fig 5.1.4 SEQUENCE DIAGRAM



- The sequence diagram illustrates the interactions between different components of the Vigilance 360 system during the process of detecting and responding to security threats.
- Security personnel initiate the system by logging in and accessing the dashboard.
- Upon accessing the dashboard, security personnel select the surveillance mode (inner or outer camera).
- The system validates the user's credentials and grants access to the selected surveillance mode.
- If inner camera mode is selected, the system activates dual-camera surveillance and begins monitoring for security threats.
- If outer camera mode is selected, the system activates the web camera and initiates surveillance of the ATM surroundings.
- As surveillance is ongoing, the system continuously analyzes the footage for anomalies, such as covered faces or suspicious activities.
- Upon detecting anomalies, the system triggers an alert notification to security personnel and stores relevant data in the database.
- Security personnel receive the alert notification and access the database to review stored data and investigate detected anomalies.
- The sequence diagram provides a detailed view of the interactions between users and system components, illustrating the flow of actions and messages exchanged during the detection and response process.

Fig 5.1.5 BLOCK DIAGRAM



- The block diagram provides a high-level overview of the Vigilance 360 system architecture, illustrating the key components and their interactions.
- The system consists of multiple components, including the user interface, surveillance module, anomaly detection module, database management system, and alert notification system.
- Security personnel interact with the system through the user interface, accessing functionalities such as surveillance mode selection and database review.
- The surveillance module initiates dual-camera surveillance or web camera activation based on user selection, capturing footage of the ATM environment.
- The anomaly detection module analyzes the surveillance footage in real-time, identifying anomalies such as covered faces or individuals carrying harmful tools.
- Upon detecting anomalies, the system triggers an alert notification to security personnel and stores relevant data in the database for further analysis.
- The database management system manages the storage and retrieval of surveillance data, detected anomalies, and user information.
- The alert notification system sends real-time alerts to security personnel, ensuring prompt response to security threats.
- The block diagram provides a simplified representation of the Vigilance 360 system architecture, highlighting the interconnections between its various components and their roles in enhancing ATM security.

5.2 Database Design

The database design for Vigilance 360 utilizes MYSQL database management system with SQLyog tool for connectivity. The database structure includes tables to store data related to surveillance, detected anomalies, user sessions, and system logs. Relationships between tables are established to ensure data integrity and efficient retrieval. The design also incorporates mechanisms for data backup and security to protect sensitive information.

Table 5.2.1 Design of Login Database Table

Field Name	Data Type	Length	Constraints
login_id	Integer	-	Primary Key
login_username	String	100	Unique, Not Null
login_password	String	100	Not Null
created_on	Integer	-	Default (current timestamp)
modified_on	Integer	-	On Update (current timestamp)

Table 5.2.2 Design of Detection Database Table

Field name	Datatype	Length	Constraints
detection_source	String	100	-
detection_starting_time	Integer	-	-
total_detected_person	Integer	-	-
detection_statistics	String	1000	-
occupancy_anomaly	String	1000	-
detection_completion_time	Integer	-	-
graph_path	String	255	-
created_on	Integer	-	-
modified_on	Integer	-	-
created_by	String	100	ForeignKey('login_table.login_id')
modified_by	String	100	ForeignKey('login_table.login_id')

CHAPTER 6 - IMPLEMENTATION

6.1 Implementation Platform

- The implementation of Vigilance 360 is carried out on a robust platform/environment consisting of:
- Operating System: Windows/Linux
- Programming Language: Python
- Development Environment: Anaconda/Jupyter Notebook
- Database Management System: MYSQL
- Tools: YOLOv8 for object detection, SQLyog for database connectivity

6.2 Process of Implementation

- Surveillance Module:
  1. Utilizes dual-camera setup for comprehensive coverage.
  2. Implements YOLOv8 for real-time object detection.
- Database Integration:
  1. Utilizes MYSQL database with SQLyog tool for efficient data storage and retrieval.
  2. Implements database schema to store surveillance data, detected anomalies, user sessions, and system logs.
- User Interface:
  1. Provides a user-friendly interface for security personnel to monitor and manage the system.
  2. Allows for easy navigation and interaction with surveillance feeds, alerts, and reports.

6.3 Results and Outcomes

During the implementation phase of Vigilance 360, the following findings, results, and outcomes were observed:

- Successful integration of dual-camera surveillance with real-time object detection using YOLOv8.
- Efficient storage and retrieval of surveillance data in the MYSQL database using SQLyog tool.
- User-friendly interface design facilitating easy monitoring and management of the system by security personnel.

Fig. 6.3.1 Login Page

Fig 6.3.2 Home Page (Camera Location)

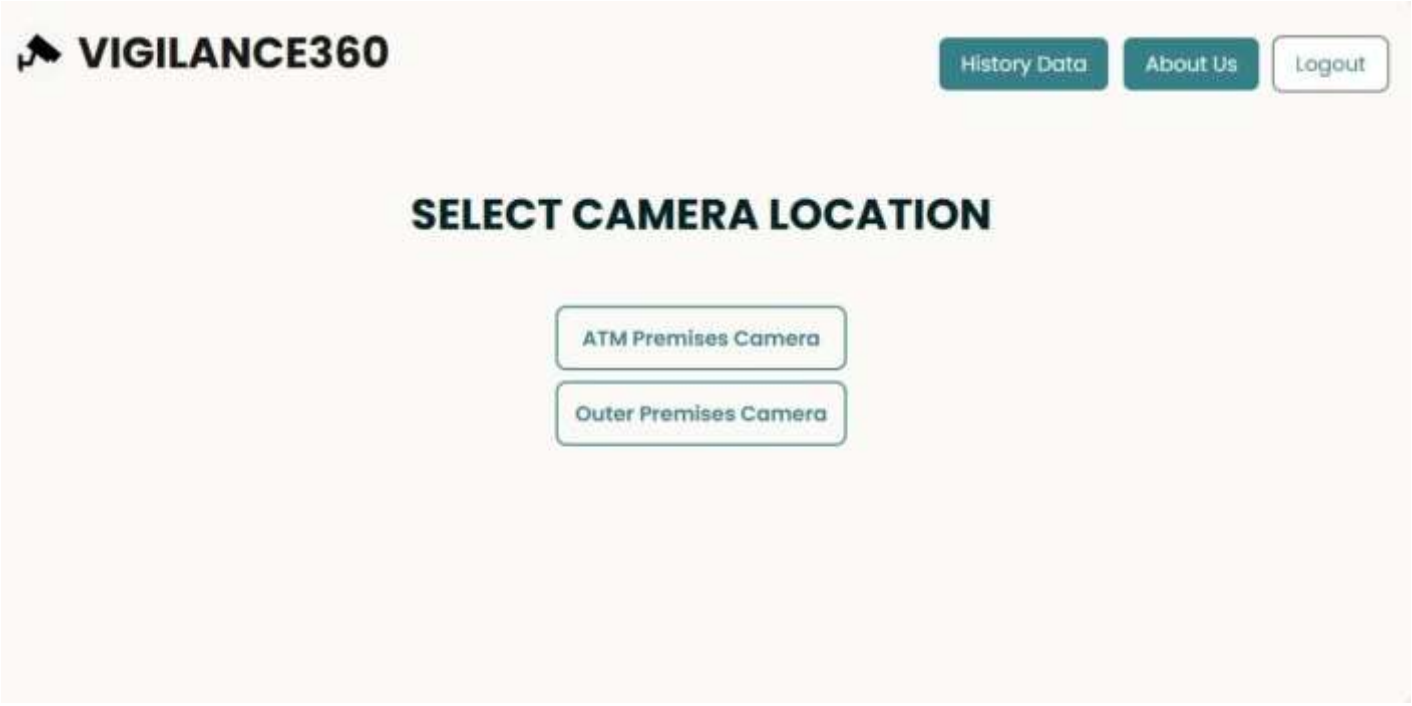


Fig 6.3.3 Select Source Page

Fig 6.3.4 Upload Page

Fig 6.3.5 CCTV Camera Page

Fig 6.3.6 Input Video Page

Fig 6.3.7 Output Video Page

Fig 6.3.8 Detection Table Page

Fig 6.3.6 Data Visualization Page

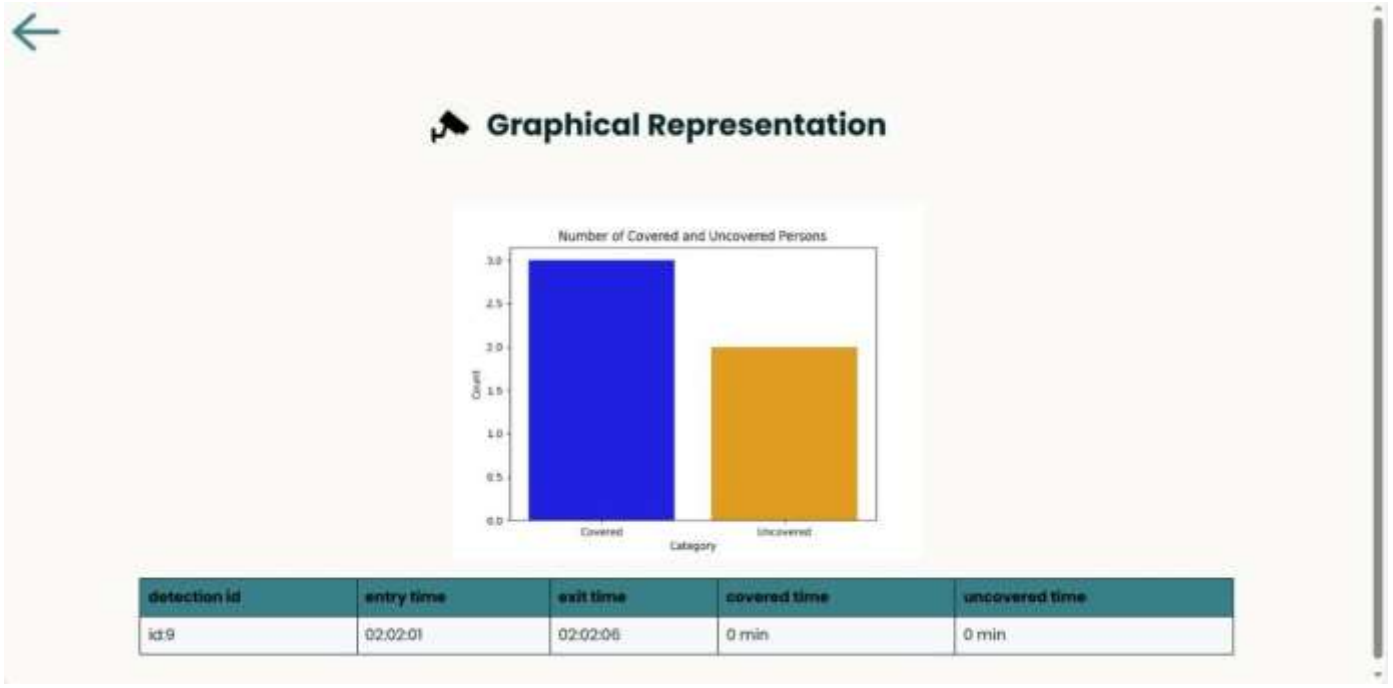


Fig 6.3.9 About Us Page

6.4 Result Analysis

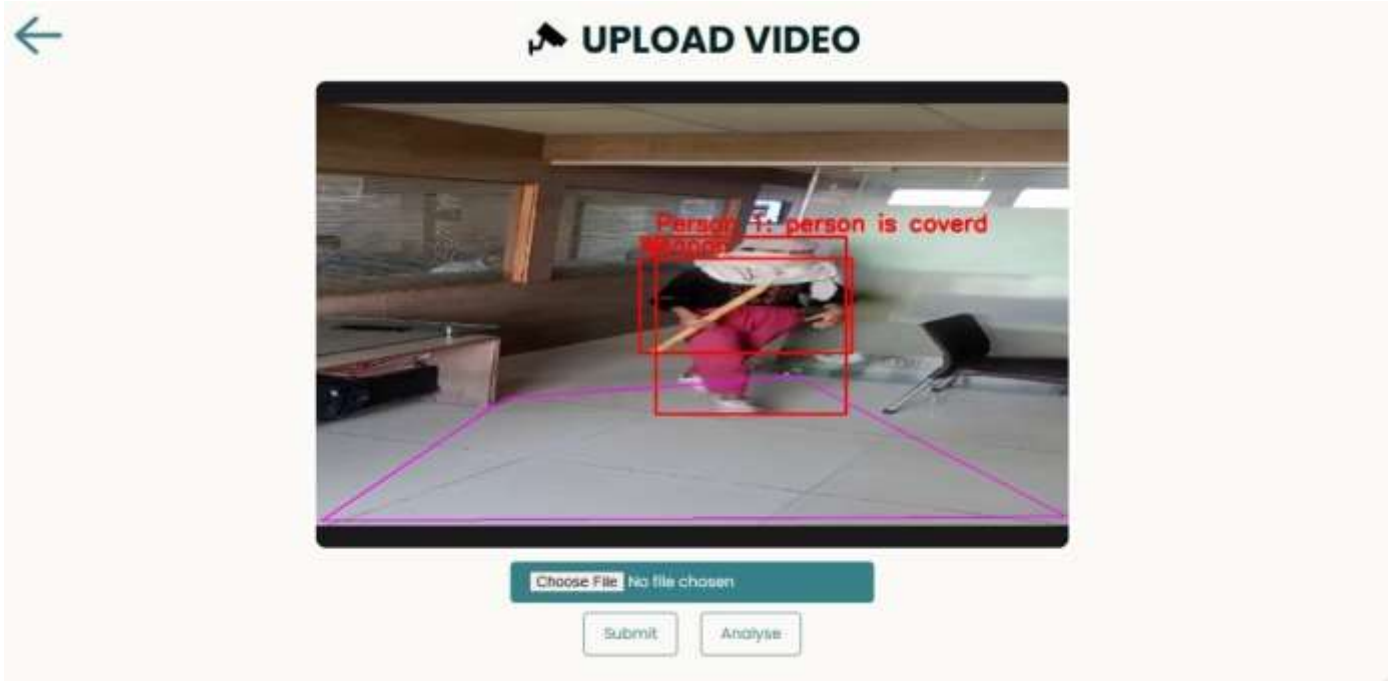
Upon analysis of the implementation results of Vigilance 360, the following conclusions can be drawn:

- The system demonstrates effective detection and monitoring capabilities, contributing to enhanced security measures in ATM environments.
- Comparison with existing surveillance systems highlights the superior performance and features of Vigilance 360, particularly in terms of real-time object detection and database integration.
- Deliberations regarding future enhancements may include implementing additional features such as automated alerts/notification systems and advanced analytics for anomaly detection.

Fig. 6.4.1 Result Analysis - Weapon Model Evaluation

A	B	C	D	E	F	G	H	I
epoch	train/box_loss	train/cls_loss	train/dfl_loss	metrics/precision(B)	metrics/recall(B)	val/box_loss	val/cls_loss	val/dfl_loss
1	1.4279	2.0252	1.4623	0.66434	0.41542	1.6633	3.9316	1.1024
2	1.4029	1.6858	1.4211	0.63806	0.33955	1.7643	3.1244	1.2532
3	1.4845	1.7042	1.4773	0.61784	0.35393	1.8631	2.3453	1.2582
4	1.4945	1.6874	1.4999	0.67551	0.39278	1.7758	1.8648	1.2259
5	1.4078	1.5544	1.4418	0.73438	0.40428	1.6897	1.7659	1.1536
6	1.3656	1.4844	1.4245	0.71366	0.44478	1.6164	1.7725	1.1123
7	1.3193	1.4169	1.3876	0.68834	0.4405	1.622	1.6128	1.1109
8	1.2901	1.3844	1.3744	0.72812	0.47507	1.5808	1.5349	1.089
9	1.2694	1.3449	1.3559	0.78508	0.47843	1.5665	1.4181	1.0628
10	1.2546	1.3167	1.3463	0.74117	0.50964	1.5341	1.5351	1.0473
11	1.2251	1.2718	1.3292	0.79383	0.50411	1.5121	1.3878	1.0317
12	1.2083	1.2469	1.3191	0.81265	0.5078	1.4723	1.3855	1.0145
13	1.1984	1.2377	1.3067	0.7861	0.52389	1.4926	1.3217	1.0133
14	1.1931	1.2143	1.3053	0.79126	0.5335	1.4575	1.3374	1.0015
15	1.1755	1.1951	1.2933	0.81029	0.53839	1.4513	1.3192	0.99443
16	1.1694	1.1762	1.2906	0.78762	0.55134	1.4264	1.2862	0.99009
17	1.1614	1.161	1.2802	0.80653	0.55217	1.4221	1.2695	0.98258
18	1.1551	1.1567	1.2782	0.80898	0.55858	1.4087	1.2606	0.97903
19	1.1413	1.1355	1.2661	0.79703	0.57661	1.3928	1.2688	0.96957
20	1.1338	1.1197	1.2615	0.79541	0.56868	1.3904	1.2431	0.96473

Fig 6.4.2 Sample Output Display on Dashboard



CHAPTER 7 – TESTING

7.1 Testing Plan

The testing plan/strategy for Vigilance 360 encompasses comprehensive testing methodologies to ensure the reliability and effectiveness of the system. The following testing phases are included:

- Unit Testing: Testing individual modules/components for functionality and correctness.
- Integration Testing: Testing the integration of modules/components to ensure seamless operation.
- System Testing: Testing the system to verify compliance with requirements and specifications.
- User Acceptance Testing (UAT): Involving end-users to validate the system against real-world scenarios and requirements.

7.2 Test Results and Analysis

Table 7.2.1 Test **C**ases **t**he **F**ollowing **T**est **C**ases **w**ere **E**xecuted **t**o **V**alidate **t**he **F**unctionality **a**nd **P**erformance **o**f **Vigilance 360**:

Test ID	Test Condition	Expected Output	Actual Output	Remark
TC-001	Dual-camera surveillance initiated	Surveillance feeds displayed	Surveillance feeds displayed	Pass
TC-002	Object detected in surveillance feed	Object highlighted	Object highlighted	Pass
TC-003	Data stored in database upon detection	Data stored in database	Data stored in database	Pass
TC-004	User login with correct credentials	Login successful	Login successful	Pass
TC-005	User login with incorrect credentials	Error message displayed	Error message displayed	Pass
TC-006	Integration of surveillance and database	Data synchronized	Data synchronized	Pass

CHAPTER 8: CONCLUSION AND DISCUSSION

8.1 Overall Analysis of Internship Vi-abilities

The overall analysis of the Vigilance 360 project demonstrates its viability as a comprehensive solution for enhancing security measures in Automated Teller Machines (ATM's). Through the integration of advanced surveillance technology, real-time object detection, and database management, Vigilance 360 offers a proactive approach to addressing security threats. The project has proven to be feasible, effective, and capable of meeting the objectives set forth during its development.

8.2 Photographs and Date of Surprise Visit by Institute Mentor

(Insert photographs and date of surprise visit by the institute mentor here, if applicable.)

8.3 Dates of Continuous Evaluation (Internal Review 1 & Review 2)

- Internal Review 1: - 21st February 2024
- Internal Review 2: - 13th April 2024

8.4 Problems Encountered and Possible Solutions

During the project, several challenges were encountered, including:

- Integration complexities between surveillance cameras and object detection algorithms.
- Database connectivity issues and data synchronization delays.
- User interface design iterations to meet usability requirements. To address these challenges, solutions such as dedicated troubleshooting sessions, enhanced documentation, and collaborative problem-solving approaches were implemented, resulting in successful resolution and progress of the project.
- Collaboration with industry partners for real-world testing and validation.

8.5 Summary of Project Work

The internship/project work on Vigilance 360 has been a rewarding experience, contributing to the development of a practical and innovative solution for enhancing ATM security. The project involved a systematic approach to problem-solving, collaborative teamwork, and continuous learning. Key accomplishments include the successful implementation of dual-camera surveillance, real-time object detection, and seamless database integration. The project has the potential to significantly improve security measures in ATM environments and has laid the foundation for further research and development in the field.

8.6 Limitations and Future Enhancements

8.6.1 Limitations

While Vigilance 360 offers significant advancements in ATM security, it is not without limitations. These include:

- Dependency on hardware and infrastructure availability.
- Potential false positives/negatives in object detection.
- Limited scalability in handling large volumes of surveillance data.

To address these limitations and further enhance the system, future enhancements may include:

- Integration of machine learning algorithms for improved object detection accuracy.
- Implementation of cloud-based storage solutions for enhanced scalabili

8.6.2 Future Enhancements

The model can be improved by training it on a larger and more diverse dataset of images. Additionally, the model can be extended to detect other types of empty shelves, such as shelves that are partially empty or shelves that are obscured by objects.

REFERENCES

[1] https://www.irjet.net/archives/V10/i4/IRJET-V10I4118.pdf

[2] https://blog.roboflow.com/whats-new-in-yolov8/

[3] https://docs.ultralytics.com/

[4] https://ijsrem.com/download/artificial-intelligence-based-detection-of-suspicious-activity-in-atm-using-yolo-algorithm/

[5] https://mediapipe-studio.webapps.google.com/home

[6] . Erhan et al., “Scalable Object Detection Using Deep Neural Networks,” IEEE Conference on Computer Vision and Pattern Recognition (CVPR),2019

[7] A. Parab, A. Nikam, P. Mogaveera and A. Save, "A New Approach to Detect Anomalous Behaviour in ATMs," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 774-777: