RESPOGUARD: DEVELOPMENT OF AN ANOMALY DETECTION SYSTEM FOR REAL-TIME SURVEILLANCE IN BARANGAY 294 BINONDO MANILA USING MACHINE LEARNING

Jayogue, Justin

Lawrence C.

Medina, Marc

Samuel R. Pallar,

Christian James

Pasion, John Paul F.

Veñales, Mark Joseph Emmanuelle
A.

BSCS-4B-M

A Project

Presented to the

Faculty of the

Computer Studies

Department College

of Science

Technological University of the

Philippines Ayala Boulevard, Manila

June 2024

Acknowledgement

We express the deepest appreciation to the individuals who played a crucial contribution to the completion of this thesis: First and foremost, we would like to acknowledge our deep appreciation to our Almighty God for His abundant blessings, everlasting grace, and unwavering guidance throughout this project. We would also like to thank our thesis advisor, Prof. Jan Eilbert Lee, whose steadfast support and consistent assistance were invaluable, particularly during challenging times encountered in the conduct of the research process. His diligence, direction, and extensive expertise were shared generously with, significantly contributing to the progress and quality of this study. Without his guidance and persistent help this would not have been possible Our heartfelt appreciation goes out to our circle of friends, who stood by us through thick and thin, providing their unwavering support and valuable knowledge and experiences. We are truly indebted for their presence in our lives. We express sincere gratitude to Seydx, the creator of the "camera.ui" repository on GitHub. Their CCTV UI project served as a valuable reference and inspiration for aspects of this study. Additionally, we would like to express our gratitude to all those who took the time to offer their thoughts and feedback on our project and our respondents, who demonstrated their support and willingness to share their precious time to evaluate our work. Their contributions were instrumental in shaping the outcome of this research. Lastly, we extend our most profound appreciation to our parents and family, who consistently provided us with financial support, enabling us to pursue and complete this project. Their unwavering love, encouragement, and inspiration were fundamental to our journey, and we are forever grateful for their presence in our lives.

Abstract

Respoguard is an anomaly detection system that combines CCTV technology and machine learning algorithms for real-time monitoring in Barangay 294 in Binondo, Manila. CCTV and machine learning work together to promote proactive monitoring and early anomaly identification, both of which are essential for improving community safety. The researchers developed a web application that allows for the immediately accurate reporting of abnormalities to barangay officials. The system's major programming language is Python, and its user interface is built with Vue.js to give a simple interface for live video surveillance and comprehensive report generation features. The user interface included quick registration, simple dashboard navigation, and access to a variety of services like notifications, camera views, and system customizations. Using the ISO 25010 to rate. 30 respondents evaluated the system including ten (10) IT Professionals, ten (10) Barangay officials, and ten (10) Barangay citizens. It has a rating of 3.76 for Functionality, that is Highly Acceptable, and 3.55 for Performance, Usability, and Efficiency, which is also Highly Acceptable. The rating for maintainability, portability, and design is 3.63, which is highly acceptable.

TABLE OF CONTENTS

List of Tables

List of Figures

List of Appendices

CHAPTER 1

THE PROBLEM AND ITS SETTING

Introduction

In an era of constant technological advancements, addressing complex societal challenges require innovative solutions. RespoGuard is a project that uses machine learning to enhance community security at the barangay level, going beyond just software or systems to create a safer and more peaceful environment. With machine learning algorithms, it aims to enhance efficiency and effectiveness in anomaly detection by aiding barangays like Barangay 294, to respond to security threats proactively, lower crime rates, and improve the safety and security of their residents' living environments. This creative method offers a thorough and data-driven approach to crime prevention by linking new and innovative technology with local knowledge. RespoGuard can spot probable criminal activity and offer insightful information to local authorities by analyzing massive volumes of data. In the fight to keep neighborhoods secure, the ability to identify anomalies in the future is now foreseeable because of RespoGuard. Together, with the use of machine learning, one can now create a safer, more secure future for barangays.

Background of the Study

Barangay is the center of Filipino community life; it embodies a certain intimacy and sense of shared living. There is a distinct sense of friendship and solidarity among these tightly connected groups. However, just like other communities, this place has considerable difficulties, particularly in terms of safety and crime.

Most Barangays still use outdated and ineffective manual reporting and traditional procedures as their primary means of crime monitoring and detection, including Barangay 294. This dependence causes response time to lag and occasionally makes it impossible to deter anomalies.

However, there is hope that the amazing advancements in technology, particularly in the area of machine learning, can transform crime prevention and detection in these communities. Machine learning can completely alter industries, especially those like computer vision and data analysis. These complex algorithms can analyze and make sense of a vast amount of data, spot trends, and anticipate probable criminal activity. In turn, this can be of great use to local law enforcement in preventing or addressing similar incidents before they become more serious.

Imagine a situation where security cameras equipped with these modern machine-learning algorithms can spot suspicious activity or behavior instantly. Law enforcement and community leaders may be able to quickly intervene or stop danger before it starts because of this early detection.

The integration of such advanced technology in Barangay 294 signifies more than a mere system enhancement, it embodies a substantial investment in the safety and overall welfare of our community. The primary goal is to provide our local law enforcement and community leaders with the necessary resources to safeguard its citizens and maintain peace in these interconnected areas. This advancement in technology is comparable to extending an alert eye and a helping hand, to boost and strengthen the efforts of those charged with safeguarding our safety and security.

Objectives of the Study

General Objective

To develop a system using advanced machine learning to help law enforcement monitor the community for anomalies. By analyzing various types of crime data, the researchers want to train the system to recognize unusual activities or outliers that could signal potential threats. This means creating a tool that assists law enforcement in quickly identifying and responding to irregular events, ultimately allowing them to prevent crimes before it happens and at least minimize its impact during the activity. The goal is to make communities safer by providing law enforcement with a proactive and effective means to detect anomalies and swiftly act, creating a more secure environment for everyone.

Specific Objective

The study has the following specific objectives:

1) Design and implement a web application with an anomaly detection system with the following features:

   1.1 To detect anomalies with an acceptable level of accuracy.

   1.2 Establish a notification/alert mechanism to promptly inform Barangay officials about detected anomalies.

   1.3 Create and implement a web application for live surveillance.

   1.4 Develop a user-friendly interface customized for the monitoring of multiple cameras.

   1.5 Implement a feature for generating comprehensive reports.

2) Develop the system using the following technologies:

   2.1 Utilize the Python programming language as the primary development framework.

2.2 Utilize the hardware such as Digital Video Recorder (DVR), Closed-Circuit Television (CCTV), and Computer/Laptop.

2.3 Create a Vue.js framework for the user interface of the web application.

3) Test and improve the system based on criteria such as accuracy, reliability, and usability.

4) Evaluate the system using the ISO 25010 standard to ensure adherence to recognized software quality attributes.

Scope and Delimitations of the Study

Anomaly refers to any behavior or activity that differ from the established normal patterns. Its recognition is crucial for maintaining a secure and well-regulated environment. This project aims to develop and implement machine learning-based anomaly detection in Barangay 294. The researchers relied on gathering and utilizing historical crime data obtained through interview questions and documented frequent incidents by Barangay 294, including different reported incidents, their locations, and related timestamps. This information covered a variety of criminal offenses, such as fights, robbery, shooting, road accidents, and assault based on the most usual incidents in the barangay. A more detailed and accurate overview of local crime patterns was possible because of the system's ability to detect various sorts of anomalies.

However, there are several project limitations that must be acknowledged. For hardware, the constraints of fixed camera positions, acknowledging scenarios where camera repositioning is not a feasible option, the limitation for camera resolution is 1080 pixels, for hard disk it requires 1 terabyte (TB) or higher, for random access memory (RAM) at least four gigabytes (GB), and for the processor it requires at least Core i3. Its efficacy was based on the accessibility and quality of previous incident data clips, with potential drawbacks due to data that is insufficient, incorrect, or out of date. The anomaly detection system's findings and insights may not be generalized because they were designed for the particular barangays where it is used. Additionally, the confidentiality of the data is maintained, with certain clips intentionally restricted from viewing or collection. The researchers won't take into consideration the multitude of outside elements that affect the data, like monetary situations, social dynamics, and legal frameworks. Due to the system's lack of legal authority, ethical and legal issues about the use of technology in law enforcement fall beyond the scope of this project. The project's scope does not include continuing maintenance and updates because they demand ongoing work and resources beyond its initial goals.

The project RespoGuard incorporates crucial limitations to govern its functionality. It underscores the imperative role of human intervention, recognizing that while the system excels in anomaly detection, it is not entirely autonomous. Trained personnel are essential for validating and providing contextual analysis of detected anomalies, acknowledging the inherent lack of 100% accuracy in the system. Additionally, the system doesn’t predict anomaly capabilities, its main focus is solely on spotting unusual activities, steering clear of trying to foresee specific criminal actions. This deliberate choice ensures a straightforward and precise purpose for the anomaly detection system. The system is positioned as a tool to enhance surveillance, offering real-time detection and alerting, with human operators retaining the responsibility for interpretation and subsequent actions based on the identified anomalies. Furthermore, the system avoids the task of classifying specific anomalies, leaving the detailed analysis and categorization to be performed by human operators. The deliberate choice of offline operation, with periodic data uploads for analysis aims to strike a balance in resource utilization. The decision to implement the system as a website application, rather than a standalone software, is rooted in the pursuit of accessibility and ease of use across devices without requiring extensive installations. Collectively, these considerations shape the system's role as an effective support system, empowering human decision makers in the realm of barangay surveillance.

Significance of the Study

The automated security system holds significance for a wide field of individuals and a group within a community.

Residents:

The automated security system ensures that residents experience increased personal safety by promptly detecting and responding to potential anomalies and emergencies. Also, quick emergency response for residents benefits from a more efficient and timely emergency response system, providing a sense of security in their daily lives.

Barangay Officials:

To improve management for Barangay officials to gain an advantage in managing and responding to incidents, bringing better governance, and ensuring the safety of their society. It can enhance decision-making for the system to support barangay officials in making informed decisions by providing real-time information on potential threats and incidents.

Law Enforcement or Tanod:

Law enforcements and Tanod personnels benefit from enhanced anomaly detection capabilities, aiding or supporting them in maintaining law and order within the community. The system enables law enforcement and tanod to respond quickly and effectively to incidents, minimizing the impact on community safety.

Future Researchers:

This study provides opportunities for future researchers to contribute to technological advancement by exploring and expanding upon the real-time machine learning detection system. The research offers a foundation for future studies on automated security systems, allowing researchers to build upon existing knowledge for continued improvements.

CHAPTER 2

CONCEPTUAL FRAMEWORK

CCTV

CCTV is a surveillance tool used for monitoring potential crimes and anomalies by providing monitored areas. The research investigates how the presence of CCTV affects anomalies and crimes in preventing and detecting bad events. These days, CCTV surveillance cameras are familiar faces on our highways, airports, sports stadiums, fuel service stations, ATMs, shopping malls, offices, schools, universities and along railway lines to mention a few. They even found their way into neighborhoods, security estates, and private homes (Basimanyane and Gandhi, 2019).

In areas where CCTV is effective, there is a notable increase in the likelihood of resolving criminal incidents across various offense categories, except for drug or weapon possession and fraud. Notably, visual evidence tends to be more accessible for more serious offenses, while its availability decreases for incidents occurring at unspecified times or specific locations. While this study specifically focuses on crimes within railway settings, it suggests that CCTV serves as a valuable investigative resource for diverse criminal activities. Nevertheless, the utility of CCTV is constrained by factors such as insufficient coverage in public spaces. To enhance its effectiveness, the study proposes several recommendations for broader CCTV implementation. CCTV increases the likelihood of giving a solution over incidents across different categories, except drug or weapon possession. CCTV serves as the saved data which can become a resource for possible criminal activities. The study relates to the effectiveness of the CCTV for further implementation (Ashby, 2017).

According to Falangon, R. (2022), CCTV installation has gained widespread acceptance, with varying reasons for installation depending on the owner or caretaker. In Bontoc, the capital town of Mountain Province, most CCTV installations, accounting for 80.85% of respondents, are in business establishments. As the center of trade and commerce, business owners in Bontoc use CCTV cameras primarily for monitoring and safeguarding their establishments. Residential houses rank second at 8.51%, often installed to deter potential robbers, especially when located near busy streets. Schools and offices follow at 4.26%, with some lacking CCTV initially, and churches come last at 2.13%. Churches install CCTV cameras not only to prevent robberies but also to aid in criminal and traffic accident investigations within their vicinity.

Anomaly Detection

According to Chandola & Kumar (2009), the prediction of a person's body part or link position from a captured image into a video. The study shows the detection of human activity from real-time CCTV video. Human Anomalies are a greater issue in computer vision that have been studied for over 15 years. It indicates that a large range of purposes, from action recognition to video surveillance, can benefit from anomaly detection, which involves approximating human position. However, precision and resolution are limited by affordable extent sensors, specifically when used inside. Neural networks offer an answer to these problems. To stop crimes and accidents, video analysis is needed for spotting suspicious activity in public spaces like banks, malls, and barangays, etc., It is necessary to have AI video surveillance armed with real-time monitoring and alarm production. However, there have been little investigation into the application of convolutional neural networks (CNNs) for the detection of suspicious activity; instead, most current research focuses on image analysis (Welsh, B. C., & Farrington, D. P. 2004). Monitoring systems help drop anomaly circumstances and whether the CCTV monitoring impacts are continuing using data from several Polish cities. Quasi-experimental methods are used by the researchers to apply police data from four types of anomaly incidents from 2005 to 2014, as well as camera position. A preventive impact was witnessed in 10 matched manner/comparison zones studied. The analysis shows that CCTV cameras in Polish cities decrease anomaly, and the effect varies depending on the class of anomaly. CCTV is not likely to have had an impact on the reduction in anomalies in Poland (Matczak, P., 2021).

A novel approach to smart city security is introduced by analyzing video stream data using a hybrid deep learning algorithm and neural networks. On the other hand, the suggested method aims to quickly detect and evaluate criminal activities, relieving the burden on law enforcement and promoting an effective anomaly detection system. Under the constraints, auto-regressive models method guarantees data processing in real-time and identifies patterns of criminal activity. Neural network promises a revolutionize changes in anomaly detection techniques for safer places by improving accuracy, reducing false reports, and ensuring the adaptation of the revolutionizing development of smart city infrastructure (Chackravarthy, 2018).

The study by Kooij, J.F et al. (2015) delves into the diverse array of image features proposed for human activity recognition, emphasizing the significance of motion as a potent identifier, particularly for overt violence detection in various applications. The identified features for single-person activity classification encompass Spatio Temporal Interest Points (STIPs), shape context, optical flow, spatial position and velocity, Motion Histogram Images, and approximate body-part positions. Notably, the integration of Convolutional Neural Networks (CNNs) to directly learn visual features from extensive datasets has gained traction, demonstrating applicability to video classification. The study underscores the challenges in isolating foreground motion features from background elements, given potential contributions from other objects and camera movements. Moreover, the paper highlights the need for comprehensive approaches to merge behavioral observables into activities with extended temporal scopes, showcasing methods such as Petri Nets, context-free grammars, and logic-based techniques. The recognition of activities involving multiple individuals, like group dynamics, necessitates trajectory-based features such as relative position and velocity, surpassing the limitations of single-person activity features. Overall, the review accentuates the evolving landscape of human activity recognition methodologies, incorporating both low-level features and sophisticated frameworks to address the intricacies of diverse scenarios.

Predictive anomaly analytics is a process of analyzing a dataset to expose hidden patterns that can be useful in predicting anomaly events Asor, J., and Sapin, S., (2020). It involves the application of machine learning algorithms to develop AI that can be integrated into computer systems. The goal of the latest project was to develop a management system for anomaly records that implements predictive anomaly analytics to predict anomaly incidents in Calauan, Laguna, Philippines. A project in Laguna State Polytechnic University, Philippines successfully developed a management information system capable of forecasting anomalies using predictive anomaly analytics and the software development life cycle. The predictive model was designed using multinomial logistic regression, which achieved a total accuracy of 86.60% and prediction confidence. The study also found that regression is better than other classification algorithms in predicting anomaly incident. The research labeled Dayap being the most vulnerable barangay in Calauan, Laguna, for different index anomaly such as rape, murder, homicide, and illegal drugs. This study shows the potential of predictive anomaly analytics in developing a trustworthy and data-driven approach to anticipating anomalies, enhancing proactive efforts to safeguard the community and combat anomalies.

Surveillance System

Surveillance is heavily implemented upon various segments of daily life. To keep a balance of peace and safety in communities, indoor and outdoor facilities, private and public institutions, etc., constant monitoring is required, thus increasing the demand for surveillance, specifically video surveillance. According to a survey, the global surveillance technology market worldwide was valued at over 130 billion U.S. dollars and expected to exceed 148 billion U.S. dollars in 2023. The market is then expected to amount to around 235 billion U.S. dollars by 2027 (Statista, 2023). As the research focuses on CCTVs' surveillance effectiveness towards detecting anomalies in a certain area, recognizing the importance of effective monitoring through the assistance of video surveillance systems serves as the backbone for cutting-edge security strategies used throughout the implementation of smart security (Mammoth Security Inc., 2024).

With the evolution of technology, various forms of surveillance systems have been produced which aims to improve the state of video surveillance and the general's perception towards its effectiveness in the modern day. Surveillance systems have to cope with several challenges, including, but not limited to, algorithmic and infrastructure challenges. Thus, surveillance systems have to adapt with the emerging network and infrastructure technologies, such as cloud systems in order to provide more robust and reliable services (Tsakanikas & Dagiuklas, 2017). To portray the system used that aims to solve these problems, the researchers categorized two forms of surveillance operating systems; hardwares and softwares.

A Digital Video Recorder (DVR) records motion videos in a digital format to a hard disk. This includes various models such as stand-alone, Personal Computer (PC), television, cable or satellite. Sizes include small, portable, desktop, industrial and commercial. DVRs serve as a solid foundation for video surveillance as it offers better quality and search capabilities, live viewing and playback, remote access, and easier integration with security systems. (Ajenikoko, et al., 2020). As this research aims to identify anomalies and potential violent activities within a local community, a hardware with easy installation features is an advantage as it directly improves the flexibility and accessibility of the detection system which will be implemented within the area. With various actions being recorded throughout the duration of the day, the DVR system's neural network processing is also a crucial component in accomplishing the real time alert detection that will enhance the security of the community. But compared to NVR, analog cameras are used which cannot process raw video data from the source (i.e. the camera itself) but rather sends signals towards coaxial cables leading to the DVR.

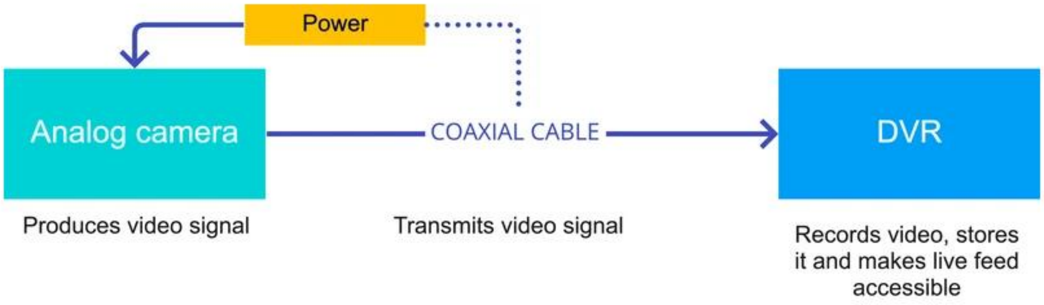


Figure 1*: Digital Video Recorder Flow Diagram [2]*

A Network Video Recorder (NVR) is an Internet Protocol (IP) based device that sits on a network. The basic function of an NVR is the simultaneous recording and remote access of live video streams from an IP camera. An NVR does not have a dedicated keyboard and monitor. All viewing and management of NVR takes place remotely over the network via a PC (Ajenikoko, et al., 2020). Unlike DVR, IP based devices such as an NVR can process raw video data at the source and is sent through an ethernet cable or via WiFi. To assist both forms of surveillance systems, a switch is used to enable several devices and connect them to the same network, making simultaneous recording and monitoring possible and easing the process of gathering data. This research investigates the most effective surveillance operating system and by testing NVR along with the neural network processing feature of DVR, the chances of achieving successful results increase, further solidifying the positive outcome of developing a real time security system that will combat anomalies.

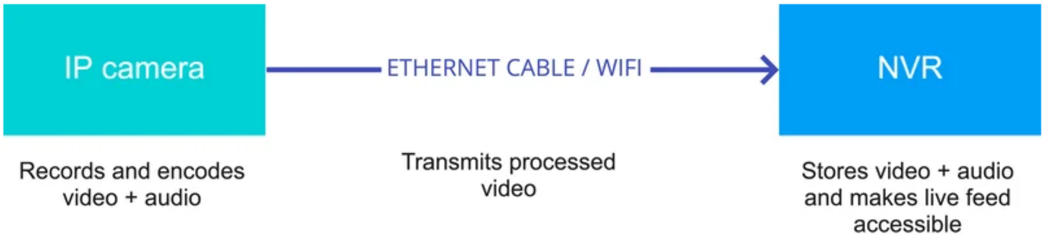

IP camera
ETHERNET CABLE / WIFI
NVR
Records and encodes video + audio
Transmits processed video
Stores video + audio and makes live feed accessible

Figure 2*: Network Video Recorder Flow Diagram [2]*

Noticeably, security systems are faced with common enemies; continuous weather or lighting changes, wide coverage areas, and immense details in recording. In line with the hardware to be used in this research, the researchers need an operating system that can balance the detection technology and simultaneous recording done. As the researchers aim to develop their own operating system (OS) to be used in surveillance, several other technologies that fall in line with the objectives of the research were used as inspiration, namely, Hikvision's *thermal imaging* technology. According to Hikvision's official website, this technology features image production that is unaffected by lighting conditions and has an "intrinsic advantage for video content analysis (VCA)". Taking the adaptability and quality analysis advantages, the developed OS will include such characteristics along with various improvements.

Detection System

The OS to be created and used by the researchers will detect objects on-camera that may be potential weapons used for violent scenarios. Objects such as knives, hammers, and guns used by perpetrators are likely to be to be detected. These data collected will be sent as an alert signal to the barangay personnels present in the area. Related studies state that with knives' wide class and reflective property, this reduce its visibility in video sequences (Glowacz, et al., 2015). Such issues are countered by immediate alert-and-response of the detection system to the human operator. Along with this, the detection system under the OS also records motion. Any potential anomaly movement (i.e. sneaking, circling the neighborhood repeatedly, entering properties, raising weapons, etc.) to be caught in the detection algorithm set in the CCTV systems will trigger an alert. Face detection comes as the most important data in surveilling crime scenarios as it directly identifies the person, making the whole operation of capturing and preventing crimes easier. Thus, the developed detection system takes immense priority on identifying the persona on-camera as stated in studies. Face recognition has received attention due to its applications, and image analysis that are useful in animation, human-computer interface, medicine, and security (Ullah, et al., 2022).

As face recognition from the computer can be applied until today, this process of authenticating people for crime prevention raises a chance for the crime rates to decline in the upcoming years

Machine Learning

Over recent years, researchers and criminology specialists have shown significant interests in the application of Machine Learning (ML) methods for anomaly prediction and detection. Numerous research studies have been conducted on anomaly prediction, employing various machine learning techniques such as KNNs, Decision trees, Naïve Bayes, and Random Forest, among others. This research study consists of a relative analysis of 51 current studies, exposing that the observed learning approach is the most frequently used method by researchers in this field (Alsubayhin, et al., 2023).

Machine learning and data mining are now essential tools to prevent and detect abnormal anomalies. Researchers use the free source data mining program from WEKA to carry out a comparison analysis between the patterns of anomaly from the University's Communities and the anomaly Unnormalized Dataset of Mississippi's real anomaly statistics data. Researchers used Additive Regression, Decision Stum, and Linear Regression on the Communities and anomaly Dataset with the same constrained set of features. The linear regression algorithm shows the best overall performance. The objective of this study is to show the efficiency and accuracy of machine learning algorithms developed in data mining analysis for predicting patterns of violent anomaly (McClendon & Meghanathan, 2015).

It takes a lot of time to identify offenders or search for individuals on CCTV footage following a significant incident or anomaly scene. According to members of the Goa branch's cyber cell, they force several department employees to physically sit in front of laptops and PCs to go through CCTV footage to identify and track down the guilty because they lack an automated mechanism to perform this work for them. This is a labor- and time-intensive technique.

Researchers have attempted to evaluate the current state of technology in this study and offer an innovative approach for criminal detection and recognition that make use of cloud computing and machine learning. If adopted by our anomaly agencies, this system will undoubtedly aid them in identifying criminals from CCTV footage. When implemented appropriately, the suggested approach can assist not only locating criminals but also, in using CCTV footage from the relevant location, to locate missing persons and children at various locations, including railway stations. Current solutions rely on conventional facial recognition algorithms, which can be problematic in India's dynamic surroundings due to variations in light, weather, and most importantly, orientation.

Certain CCTV cameras have poor positioning and are prone to tilting, which drastically increases inaccuracy. To construct the suggested system, this research study suggests using Microsoft Azure Cognitive Services and the Cloud system. To assess the efficacy of the suggested System, the next part of this research will attempt to compare the suggested methodology with conventional methods such as HAAR cascade. This is because a project of this sensitivity requires a high degree of precision record (Shirsat et al., 2019). The study shows the recognition for public places such as airports, train stations, parks, and malls are commonly categorized by large crowds. The repetitive growth in urban residents contributes to a constant increase in the flow of people to these areas each year (Alsubayhin, et al., 2023). The difficulty of an anomaly results in punishment by a governing body. The rate and classes of illegal activities are on the rise, triggering agencies to develop effective techniques for preventive measures. In the existing landscape of escalating anomaly rates, traditional anomaly-solving methods are insufficient, being both slow and less efficient. The strategies for the development of the prediction of detailed information or data about anomalies before they happen or the actual creation of the machine to aid law enforcement to lessen the problem of the police and provide prevention. The study integrates machine learning and computer vision for the outcome of prediction and prevention of anomalies (Shah & Bhagat, 2021).

Assisting society requires identifying and minimizing anomaly rates. Gathering and analyzing data using Big Data methods to know the critical factors and attributes are responsible for the anomaly hotspots' blocking. Conventional machine learning-based anomaly detection techniques and algorithms sometimes fail to produce important prime features from anomaly datasets, which results in less accurate anomaly pattern predictions. The objective of this work is to do vulnerability analysis and extract important attributes, such as anomaly chances, anomaly trouble spots, and time zones, to develop the machine learning algorithm's accuracy (Palanivinayagam et al., 2021). According to Criminal Detection and Recognition Using ML (2023) Businesses and cities worldwide are experimenting with artificial intelligence to reduce and deter anomalies while responding more rapidly to ongoing criminal activities. The driving force behind many of these endeavors is the belief that criminal behavior can be largely predicted, requiring the capability to analyze vast amounts of data to identify trends beneficial to law enforcement. Just a few decades ago, such data analysis was technologically impractical, but recent advancements in machine learning should now make it achievable once again. The study shows the recognition for public places such as airports, train stations, parks, and malls are commonly categorized by large crowds. The repetitive growth in the urban residents contributes to a constant increase in the flow of people to these areas each year. The article has comparative data mining technologies for determining anomalies and identifies the Decision Tree as the most effective method for performance criteria like accuracy (Quiroz-Vázquez, 2023).

Data mining has been used to model anomaly detection and prevention categorization issues. Manually addressing the high volume of anomaly that is being committed increases anomaly. Prevention techniques are a time-consuming and difficult task. In the related study, data mining approaches are investigated to forecast the terms anomaly and criminality are interchangeable. Researchers use machine learning methods to predict traits and events from a dataset of criminal activity outcomes. The researchers are also going to conduct a comparison of several classification strategies. Prevention techniques are a time-consuming and difficult task. In the related study, data mining approaches are investigated to forecast the terms anomaly and criminality are interchangeable. Researchers use machine learning methods to predict traits and events from a dataset of criminal activity outcomes. The researchers are also going to conduct a comparison of several classification strategies (Saeed et al., 2015).

Weapon Detection

Human supervision and intervention are still necessary. The researchers need a system that is capable of automatically detecting these illicit actions. Real-time weapon detection remains a significant problem even with the most advanced CCTV cameras, rapid processing hardware, and state-of-the-art deep learning algorithms. The difficulty of the task is increased by noticing variations in angle and obstructions caused by the individual holding the firearm and by those nearby. This effort aims to create a safe space by applying cutting-edge open-source deep learning algorithms to CCTV footage as a source to identify dangerous weapons. To decrease false positives and false negatives, researchers have built binary classification using the pistol class as the source class and using the relevant confusion objects inclusion idea. Since there was no pre-current dataset for a real-time scenario, researchers created their own using their camera, manually collected images from the internet, obtained data from YouTube CCTV footage, accessed data from the University of Granada's GitHub repositories, and the Internet Movies Firearms Database (IMFDB) at imfdb.org. Region proposal/object detection and sliding window/classification are used in the study. VGG16, Inception-V3, Inception-ResnetV2, SSDMobileNetV1, Faster-RCNN Inception-ResnetV2 (FRIRv2), YOLOv3, and YOLOv4 are limited of the algorithms that are employed. These full methods occurred and were measured in terms of accuracy and recall, which matter more when object detection than accuracy. Yolov4 outperforms all other algorithms, with an F1-score of 91% and a mean average precision that is 91.73% higher than the previous record (Bhatti et al., 2021).

Related Studies

The inspiration of the paper is that the event detection algorithm is based on trajectories designed for CCTV systems. The related study shows the comparison of parameters with semantic description, the system can detect and have an appropriate image processing technique to provide an intelligent system able to detect anomaly situations (Fuentes & Velastin, 2004). The researchers use Raspberry Pi to create a low-cost AI-based home security system. The study used to photograph and record a live area using a Raspberry Pi and a USB webcam, detecting motion. The suggested system implements multiple features via node-red Flows using IBM's Internet of Things software library. There are two laws formed. When motion is detected, the first blink causes the camera to start taking photographs. The image is subsequently forwarded for processing to the visual recognition node. To examine the image, utilize the second low. with a visual recognition node powered by AI. The visual recognizer receives the image for examination (Luu, et al., 2019).

Garg & Verma (2016) studied that algorithms have a lot of strengths in building a system. The related study shows the based on multi-algorithms such as HAAR, Local Binary Pattern or LBP, Histogram of Oriented Gradients or HOG which are able to produce or provide: variations of shapes, illumination effect, orientation, partial occlusion and shadowing effect. The findings show true positive rate and false positive rate of computation time of the system's performance.

The topic shows the storage optimization of video of CCTV cameras using MSE (Mean Squared Error) between frames of each video. The use technique will be maintaining the information or data and the quality of the clips or footage (Arora, et al., 2016). The task of automation and recognition has been proposed with algorithms that can alert human operators for object detection. The research shows the classifier, pattern recognition, and object detection. The sensitivity and specificity are significantly better than the previous study (Grega et al., 2016).

Auto face detection doesn’t require any database at all for images. It creates its collection of images and frames, and then tracks the future occurrences of those images Eigenface, fisherface, LBPH, and SURF are the types of algorithms for face recognition. The analytics show that the researchers use SURF to compare images to know every single face that comes up in the system (Sathyadevan, 2014). This AI-based desktop application, is made only to begin recording when a person or human face is recognized. This suggested system includes two detection modes; human body identification and human-face identification, which is based on Linux OS and deep learning algorithms and OpenCV libraries (Alajrami et al., 2019). The study used descriptive and RAD with a face recognition algorithm. LBP or the Local binary pattern histogram, Eigenface, and Fisherface. The study shows the statistics with the percentage of 95.92% accuracy rate. The study required the implementation of the system in PNP to help detect the criminals to prevent possible crimes for happening (Lumaban, 2020).

Conceptual Model of the Study

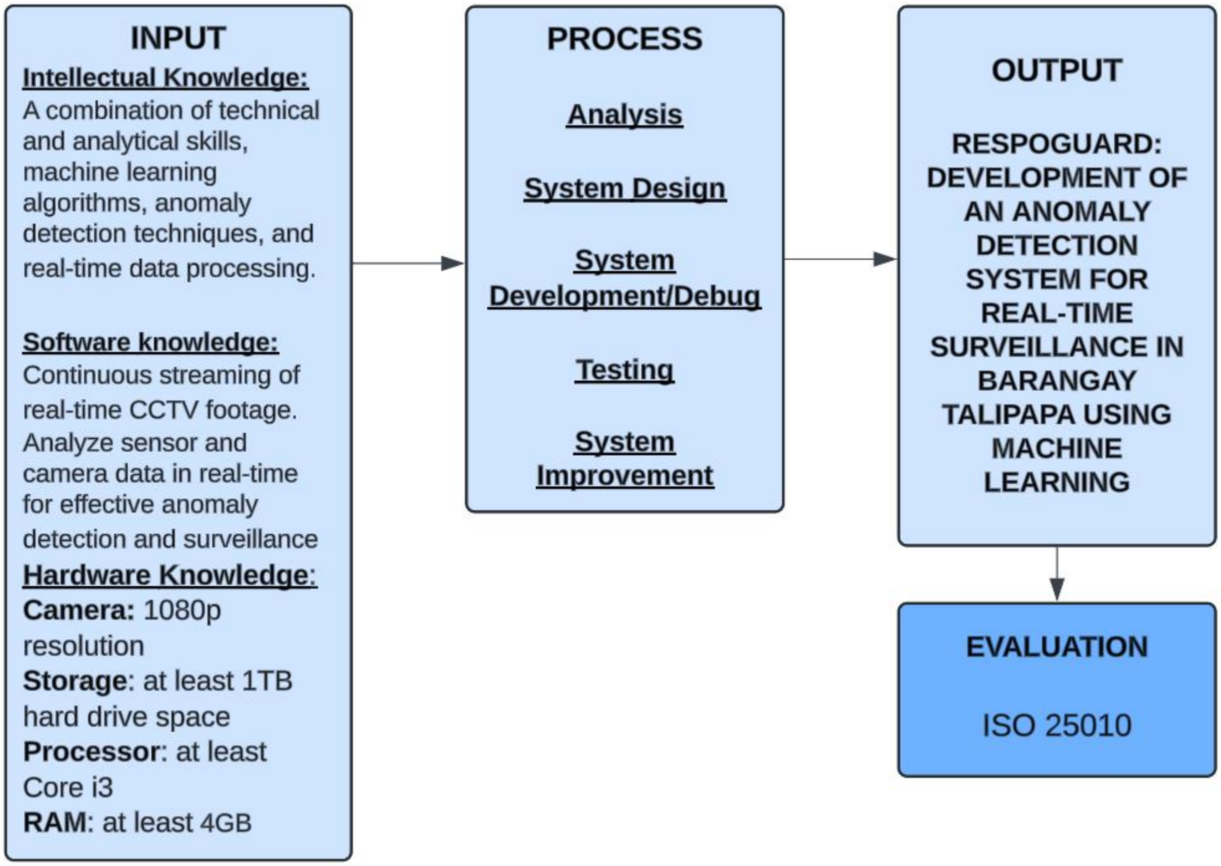

INPUT
Intellectual Knowledge:
A combination of technical and analytical skills, machine learning algorithms, anomaly detection techniques, and real-time data processing.
Software knowledge:
Continuous streaming of real-time CCTV footage. Analyze sensor and camera data in real-time for effective anomaly detection and surveillance
Hardware Knowledge:
Camera: 1080p resolution
Storage: at least 1TB hard drive space
Processor: at least Core i3
RAM: at least 4GB
PROCESS
Analysis
System Design
System Development/Debug
Testing
System Improvement
OUTPUT
RESPOGUARD: DEVELOPMENT OF AN ANOMALY DETECTION SYSTEM FOR REAL-TIME SURVEILLANCE IN BARANGAY TALIPAPA USING MACHINE LEARNING
EVALUATION
ISO 25010

***Figure 3**: Conceptual Model of the Study*

The model shows the relationship of the three main components of the research paradigm, Input, Process, and Output.

The **input** includes intellectual knowledge, software knowledge, and hardware knowledge. The system requires technical and analytical skills in machine learning algorithms, anomaly detection techniques, and real-time data processing. Knowledge in both software and hardware are also required such as analyzing camera data and specs of the devices that will be used.

The **process** in conceptual model includes analyzing, designing, system development, testing, and system improvement of the Development of an Anomaly Detection System for real-time surveillance in Barangay 294 using Machine Learning.

Analyze. During this phase, system functionalities and important components were gathered that is crucial for the development of the system.

System Design. This is also known as the planning stage. Creating the diagrams such as Data Flow Diagram, System Flowchart, and UML Diagram. It also includes creating the structure of the system, the user interface and database.

System Development/Debug. This is the stage for executing the design and the plan as well as checking the code or program if it has rising issues.

Testing. This is the assessment stage or evaluation phase where the functionalities of the system will be tested if working properly.

System Improvement. This phase fixes system issues if any. It includes the enhancement of performance, efficiency, and quality of the system.

The **output** is the development of the Respoguard: Development of an Anomaly Detection System for Real-time Surveillance in Barangay 294 using Machine Learning

Operational Definition of Terms

1. **Adaptive Learning:**

Operational Definition: Adaptive learning, within the scope of this study, refers to the machine learning model's ability to continuously evolve and improve its accuracy over time. This involves ongoing training on new data to enhance the system's effectiveness in recognizing and classifying events.

2. **Anomaly**

Operational Definition: Defined as an uncommon or irregular event, sometimes connected to incidents or criminal activities that depart from the anticipated or customary patterns within the community.

3. **Closed-Circuit Television (CCTV) Infrastructure:**

Operational Definition: Refers to a network of high-resolution cameras strategically positioned in Barangays. These cameras capture and transmit video footage for real-time monitoring and analysis.

4. **Community Involvement Mechanism:**

Operational Definition: The community involvement mechanism is a structured system that enables residents to provide feedback, reports, and observations related to security concerns in Barangays. It includes reporting channels and interfaces for community engagement.

5. **Event Recognition:**

Operational Definition: Event recognition is the process by which the machine learning algorithms identify and categorize specific activities or incidents in real-time CCTV footage, such as suspicious behavior, intrusions, or public disturbances.

6. **Machine Learning (ML):**

Operational Definition: Machine learning refers to a subset of artificial intelligence (AI) that enables computer systems to automatically learn and improve from experience. Specifically, it involves the use of algorithms to analyze CCTV data and identify patterns, anomalies, and events relevant to surveillance in Barangays.

7. **Privacy Safeguards:**

   Operational Definition: Privacy safeguards encompass measures and protocols implemented to protect the privacy rights of individuals captured in CCTV footage. This includes encryption, access controls, and adherence to legal and ethical standards governing the use of surveillance technologies.

8. **Real-Time Surveillance:**

   Operational Definition: The continuous and immediate monitoring of CCTV footage allows for the instantaneous analysis and recognition of events as they occur in Barangays.

9. **User Interface for Real-Time Monitoring:**

   Operational Definition: The user interface is a graphical representation designed for ease of use, allowing authorized personnel to monitor the real-time CCTV feed, view alerts, and access visualizations of events. It serves as an interactive platform for decision- making.

CHAPTER 3

METHODOLOGY

Project Design

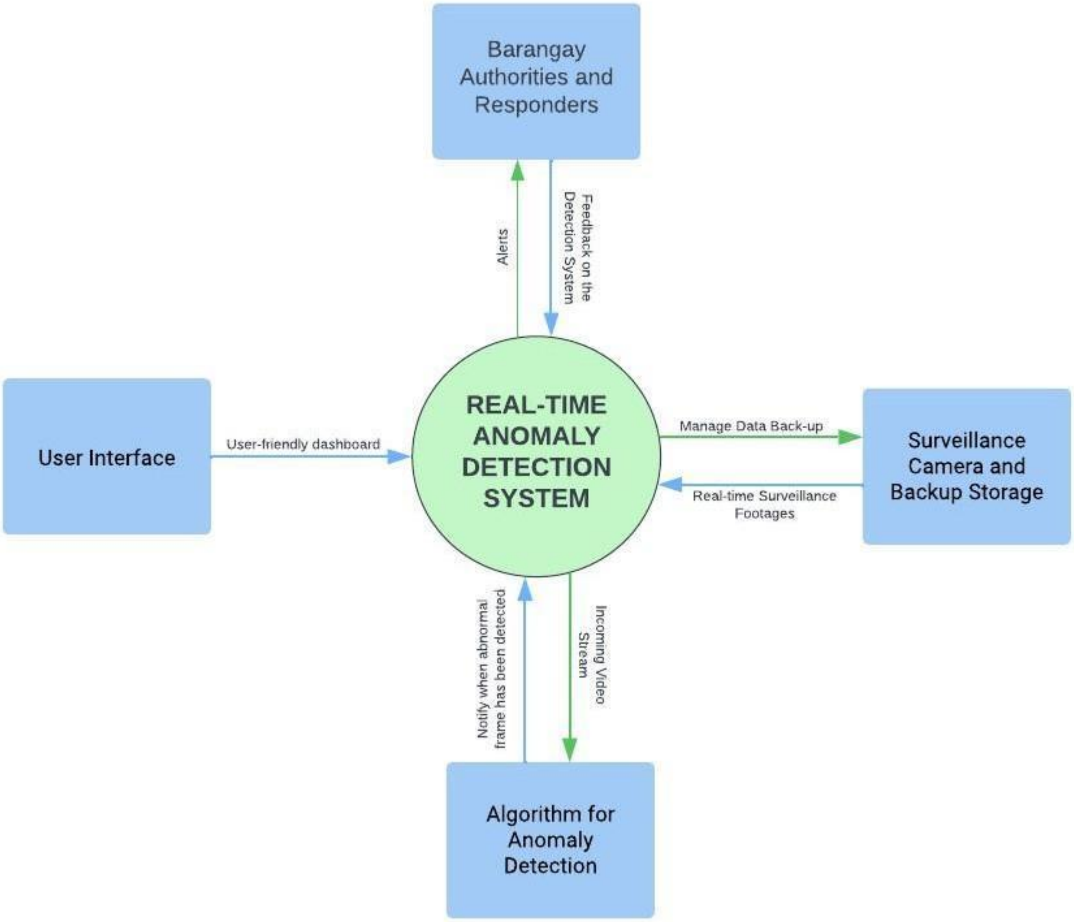

Barangay Authorities and Responders
Alerts
Feedback on the Detection System
User Interface
User-friendly dashboard
REAL-TIME ANOMALY DETECTION SYSTEM
Manage Data Back-up
Real-time Surveillance Footages
Surveillance Camera and Backup Storage
Notify when abnormal frame has been detected
Incoming Video Stream
Algorithm for Anomaly Detection

***Figure 4**: Data Flow Diagram (Level 0) for the Anomaly Detection System*

Figure 4 is the data flow diagram of the Real-Time Anomaly Detection System that showed the interactions between various components within a system. The important elements were the following:

1. Barangay Authorities and Responders

The Barangay Authorities and Responders were essential contributors who received alerts generated by the anomaly detection system. These notifications might indicate probable anomalies or suspicious activity detected by the surveillance system. The system then received data from different authorities, creating a continuous process for continual improvement and adjustments.

2. Surveillance Camera and Backup Storage

Surveillance cameras served as the eyes of the system, capturing real-time footage from the designated areas. After processing the data, which was necessary for data preservation, the system stores it in a backup.

3. Algorithm for Anomaly Detection

The heart of the system lay in the anomaly detection algorithm. This algorithm continuously analyzes the incoming video stream from surveillance cameras, applying advanced pattern recognition and anomaly detection techniques. If the system finds an action or frame to be abnormal, it sends notifications to the authorities so that appropriate actions take place.

4. User Interface

User interface was the tool through which system administrators as well as other personnel interact with permission. It presented a UI for the administrative end that updates the information, alerts, and statistics regarding the surveillance data in real-time. From the point of view of a user, the application was convenient in terms of configuring the settings of the system, observing the previously received data, and addressing the alerts.

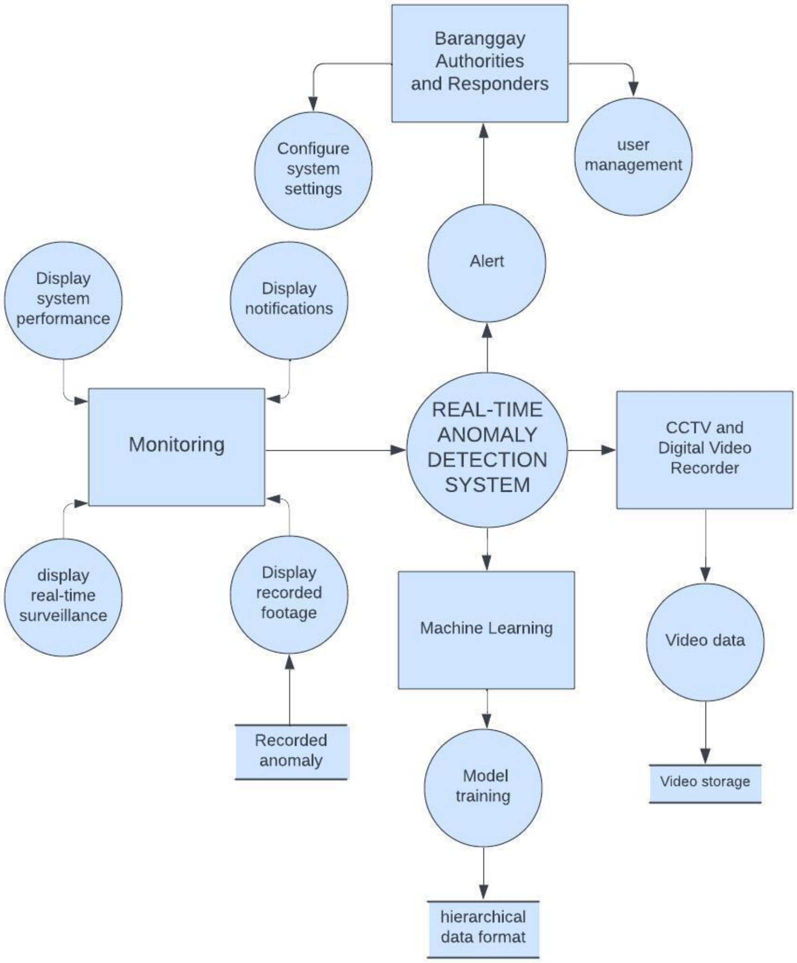

Baranggay Authorities and Responders
Configure system settings
user management
Alert
Display system performance
Display notifications
Monitoring
REAL-TIME ANOMALY DETECTION SYSTEM
CCTV and Digital Video Recorder
display real-time surveillance
Display recorded footage
Machine Learning
Video data
Recorded anomaly
Model training
Video storage
hierarchical data format

***Figure 5**: Data Flow Diagram (Level 1) for the Anomaly Detection System*

The surveillance system's data flow diagram (DFD) level 1 included several external entities and processes that were combined to enable thorough administration and monitoring. The Monitoring entity comes with features such as notifications, real-time surveillance, recorded footage, and system performance display. These procedures communicated with data store to obtain the information required for efficient monitoring. To retrieve and display previously recorded anomalies, the "Display Recorded Footage" function made use of the "Recorded

Anomaly” data store. Continuous video data was made available for both live and recorded viewing by the CCTV and Digital Video Recorder entities. This data was kept in the “Video Storage” data store.

The authorized users can change the parameters of the surveillance system and manage the accounts, through the protocols for user management and system configuration provided by the Barangay Authorities and Responders entity Meanwhile, the machine learning entity invested time in training models, utilized data structures to enhance the system's ability to predict. This method improved the detection and analysis of surveillance footage. Moreover, the DFD illustrated the structured interactions between entities, processes, and data stores that provided the efficient operation and management of the surveillance system.

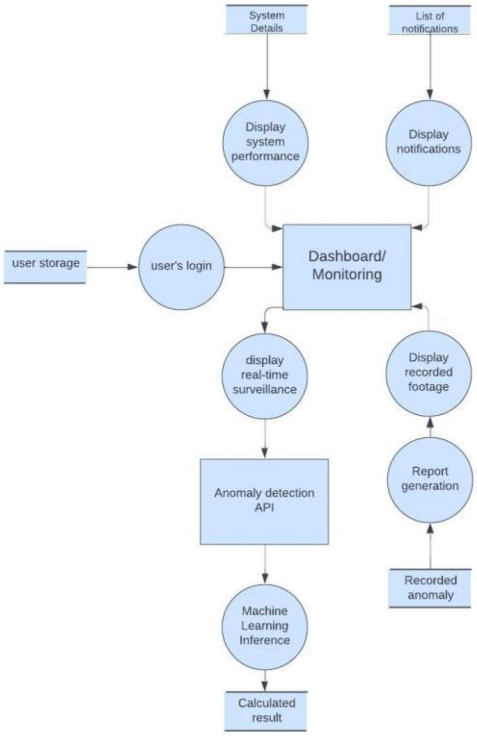


Figure 6*: Data Flow Diagram (Level 2) for the Anomaly Detection System: User Interface/Dashboard Monitoring*

The surveillance system's data flow diagram (DFD) showed two main external entities: (1) Monitoring and (2) Anomaly Detection API. Monitoring was responsible for controlling vital functions such as showing recorded video, creating reports, showing real-time surveillance, user logins, system performance, and notifications. All these functions work together with data stores to ensure effective data retrieval and storage.

Specifically, anomalies were compiled into comprehensive reports and recorded footage was accessed for examination. With the "Machine Learning Inference" method, the Anomaly Detection API improved analytical skills by identifying anomalies in video data and saving the results in the "Calculated Result" data store. Through this integration, possible dangers are dealt with by the system in a proactive as well as reactive manner.

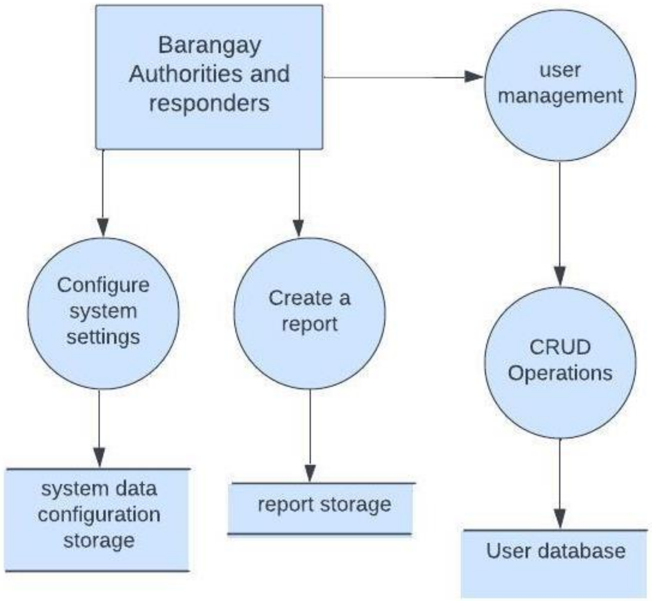

Barangay Authorities and responders
user management
Configure system settings
Create a report
CRUD Operations
system data configuration storage
report storage
User database

***Figure 6a**: Data Flow Diagram (Level 2) for the Anomaly Detection System: Barangay Authorities and Responders*

The entity most closely linked to the functions of the basic surveillance system operation and the management of the DFD was the Barangay Authorities and Responders. For these users, the Configure System adjustments process allows them to modify all the settings in the system. All modifications were made to be stored in the System Data Configuration Storage. It made it easier for the detail surveillance and report can easily create using the Create a Report method and then store it in the Report Storage for future use and action.

In addition, the authorities maintained and controlled users efficiently due to the User Management process and CRUD operations sub-process. The User Database was responsible for all aspects of the user including account creation, reading account detail, modification of user information and deletion of User accounts. These procedures and data sources were used to validate the surveillance system configuration, security measures, and the ability of the system to generate the necessary reports for analysis and decision-making as indicated in the case.

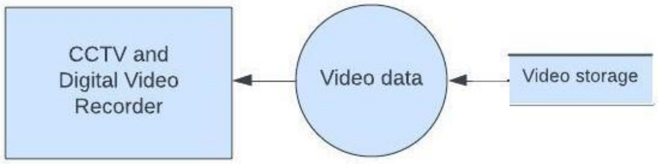


Figure 6b*: Data Flow Diagram (Level 2) for the Anomaly Detection System: CCTV and Digital Video Recorder*

The figure showed how the CCTV interfaces with the Digital Video Recorder (DVR) and the Video Data. These records were captured and transmitted through the CCTV and the digital video recorder, then processed and stored in the Video Storage data store. This way, you were confident that all the video data was systematically stored for future use and further analysis.

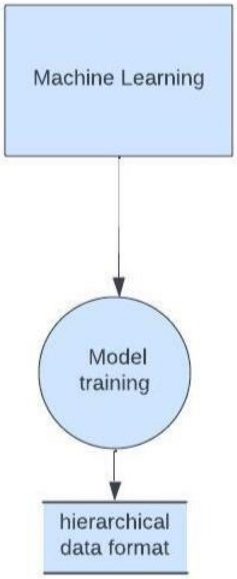


Figure 6c*: Data Flow Diagram (Level 2) for the Anomaly Detection System: Machine Learning Model*

The process between Model Training and the external entity, Machine Learning, can be observed in the DFD. In this system, the specific Machine Learning entity provided the necessary data for models and these models go through this process of training. The trained models were stored onto the data store shelf of the Hierarchical Data Format for ease of access and use in subsequent machine learning techniques.

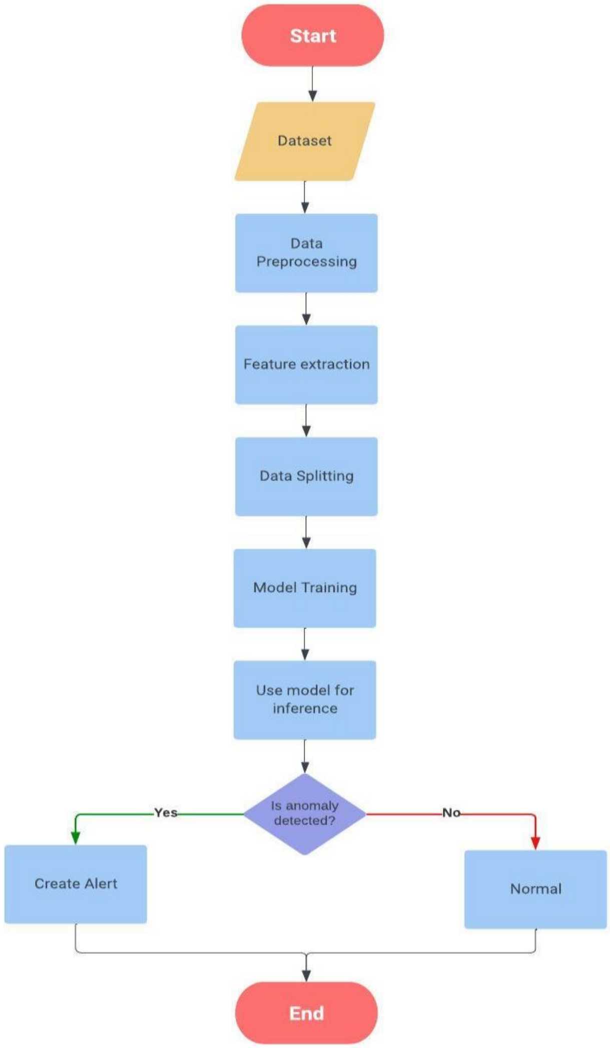


Figure 7. *System Flowchart for the Anomaly Detection System*

1. **Input Data**
   - Raw inputs were used in the first training and test video.
2. **Data Processing**
   - Data augmentation adds value to real training data.
3. **Feature Extraction**
   - Select features for the training model.
4. **Data Splitting**

- Split the data in the feature space into a training set and test set once all the features were extracted.

5. **Model Training**

- Feed the new data into the machine learning model using the extracted features.

6. **Evaluation**

- By the end, apply the trained model on new videos.

7. **Anomaly Detection**

- Perform an anomaly detection with the help of the output that was created by a model.

8. **Result Labeling**

- If an anomaly is detected, label the frame as anomalous; otherwise, label as normal.

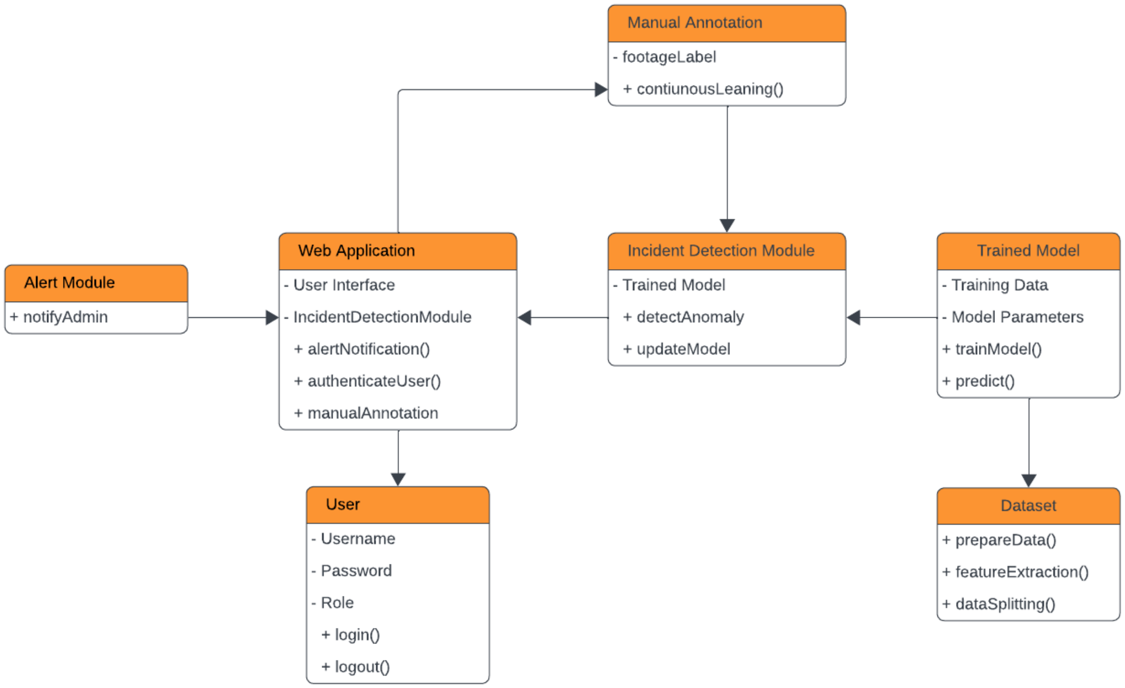


Figure 8*: Unified Modeling Language Diagram for the Anomaly Detection System*

The simplified representation of the web application for the anomaly detection in the

Barangay 294 was presented in the form of a UML diagram below: There were several occurrences that the system used machine learning techniques to recognize them, and these were; abuse, assault, fighting, road accidents, robbery and shooting.

1. **Web Application**
    - This was the component of the system where most of the personnel from the barangay met and where most system transactions took place.
    - It also includes methods of anomalous visualization and user authentication.
2. **Anomaly Detection Module**
    - Save the first step of the initial data processing to detect anomalies.
    - It is based on a machine learning algorithm that identifies the given types of anomalies.
    - Also involved in the process of modification of the model each time it is required.
3. **Machine Learning Algorithm**
    - This was the basic data processing module that was used to identify an anomaly.
    - This entailed the process of feeding the training data to the model and then estimating the future outcome given new data.
4. **User**
    - It stands for the users of the system that may include the personnel of the barangay.
    - It has functions for verifying the login credentials of the user and for logging out the user.
5. **Data Preparation:**

- A sub-module which had the responsibility of pre-processing the data before it was processed by the learning machine algorithm.
- Included methods like prepareData(), featureExtraction(), and dataSplitting().

6. **Anomaly Labeling**

- Enabled the users to indicate the identified outliers to make corrections for the improvement of subsequent performances.
- Provided methods for labeling anomalies and supporting continuous learning continuousLearning().

Project Development

Determine Project Objectives: The first phase of the Spiral Model which this project steered its goals and objectives. This involved analyzing what needs to be achieved, who will be involved in the implementation of the project, and what the system required.

Alternatives: The second phase of the model entailed sought other ways of dealing with the problem, after determining that a linear method doesn't work. This involved doing some research on the different data analysis techniques and the machine learning algorithms that were used in the development of the Anomaly Detection System.

Restrictions: The last task of the design phase within the context of the Spiral Model was the identification of constraining factors that acted as the defining point of the undertaking. These were referred to as limiting factors. Whereas, as the system unfolds that means identifying aspects that may be perceived to be high risk and then generating ways and means to lessen that volatility.

Planning Stage: This step was the fourth in the spiral model and involved planning for the creation of the anomaly detection system as well as brainstorming on the architecture of the system. This involved offering a clear explanation of the details of the project, stating the assets that would be needed in the execution of the project and estimating the duration of the project implementation.

Iteration: The development of the Spiral Model was going to be gradual to include all four stages of the model at each spiral level. A particular system feature was constructed in each iteration; however, before moving forward to build the next system feature, it reviewed and evaluated.

User Interface Design

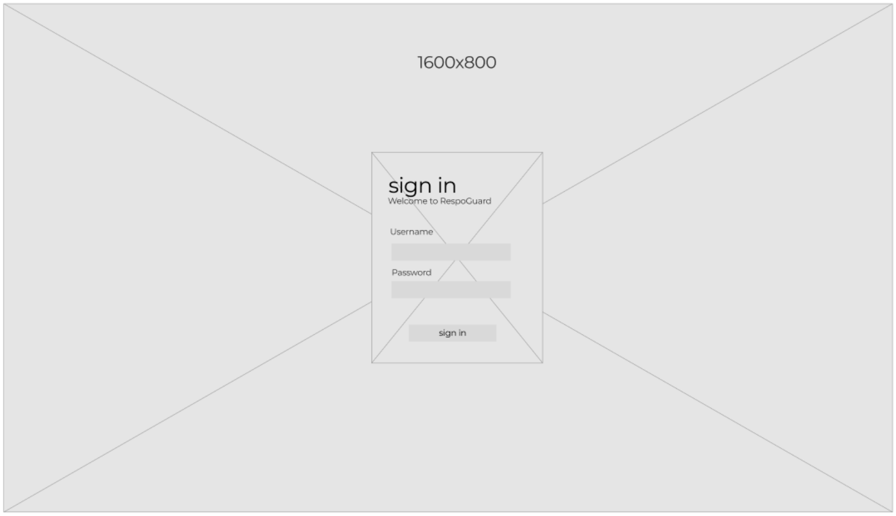


Figure 9. Wireframe User's Login for RespoGuard

Figure 9 shows a wireframe of the user's login where the Barangay personnel gains access to a system by entering their credentials such as username and password. It will verify the user's identity and grant them access to the system's resources and functionalities based on their authorization level.

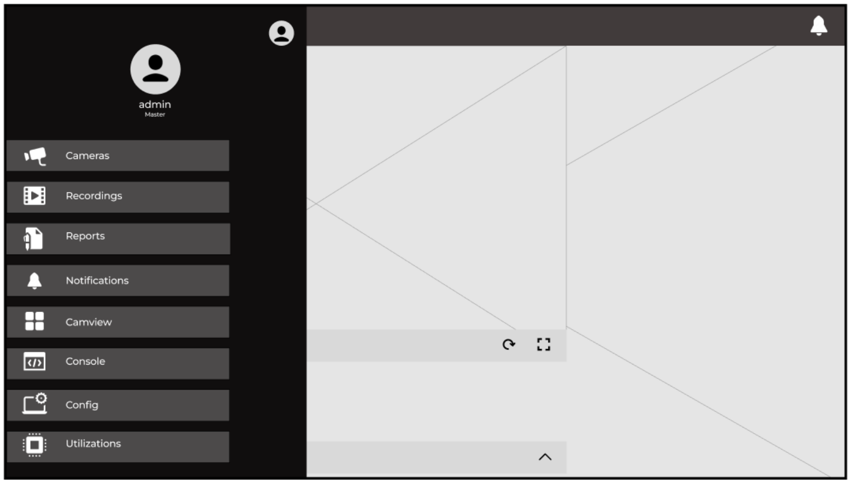


Figure 10. Wireframe for User’s Navigation Bar for RespoGuard

For surveillance personnel, the navigation bar is an essential instrument that offers easy access to key features. It serves as the main hub for keeping an eye on security, organizing recordings, creating reports, and getting alerts in addition to viewing camera feeds. With the ability to adjust settings, examine footage from cameras, and monitor system usage, every tab gives users the ability to quickly identify and address possible security risks.

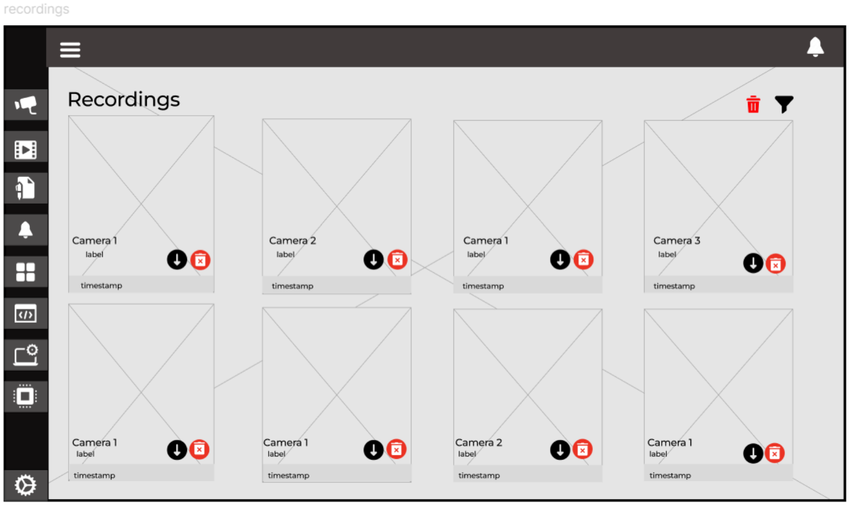


Figure 11. Wireframe Page for Recordings of RespoGuard

It serves as a repository for archival surveillance footage, enabling barangay staff to review past events and situations. It is a tool for investigative work, allowing users to examine footage that has been captured, spot irregularities, and compile data to improve security and incident response procedures.

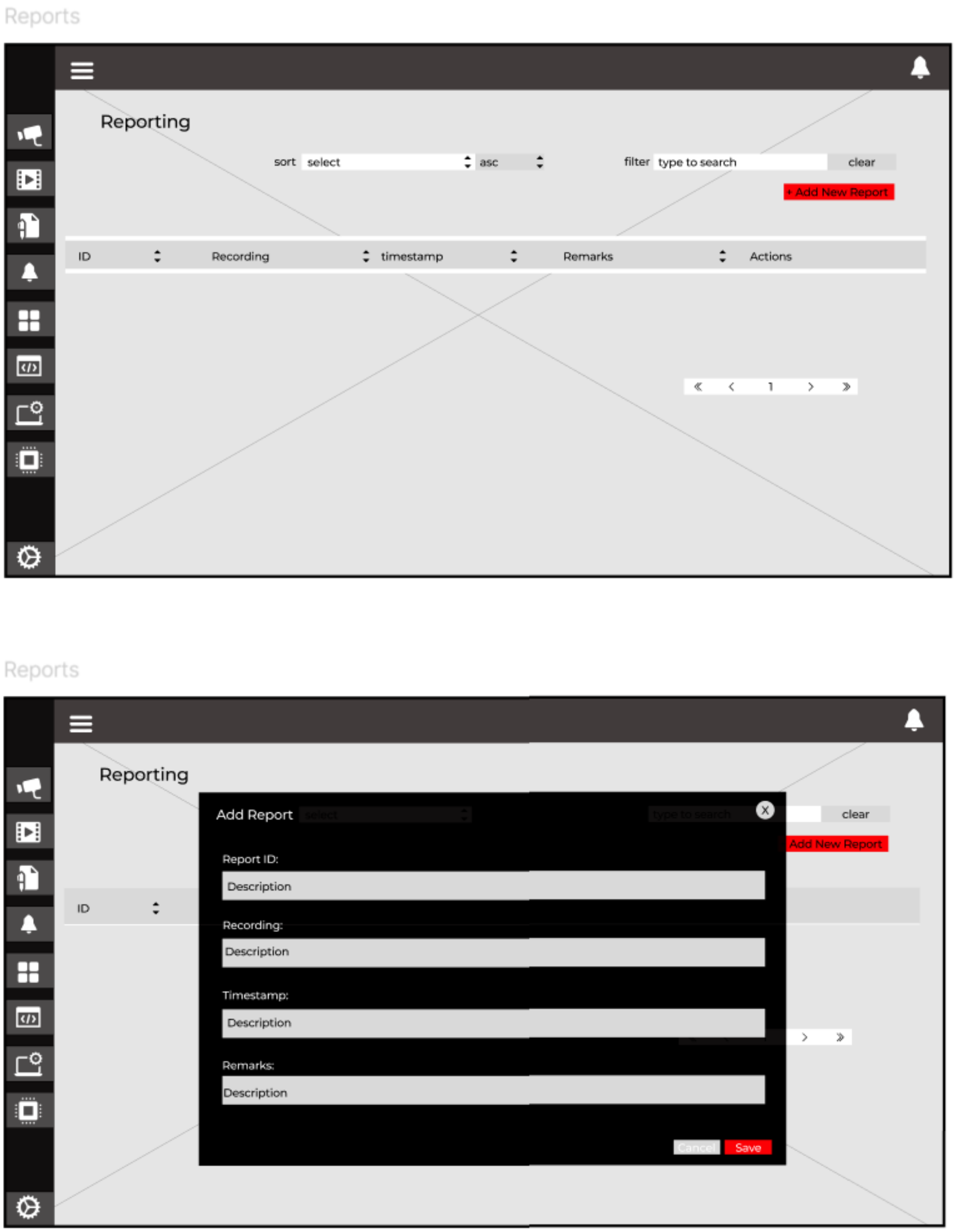


Figure 12. Wireframe Page for Reports of RespoGuard

The page represents the Reports tab which is designed to simply show the reporting process. It allows users to create a report, compile and customize the report details by selecting the specific parameters like the timestamps, camera locations and the type of incidents.

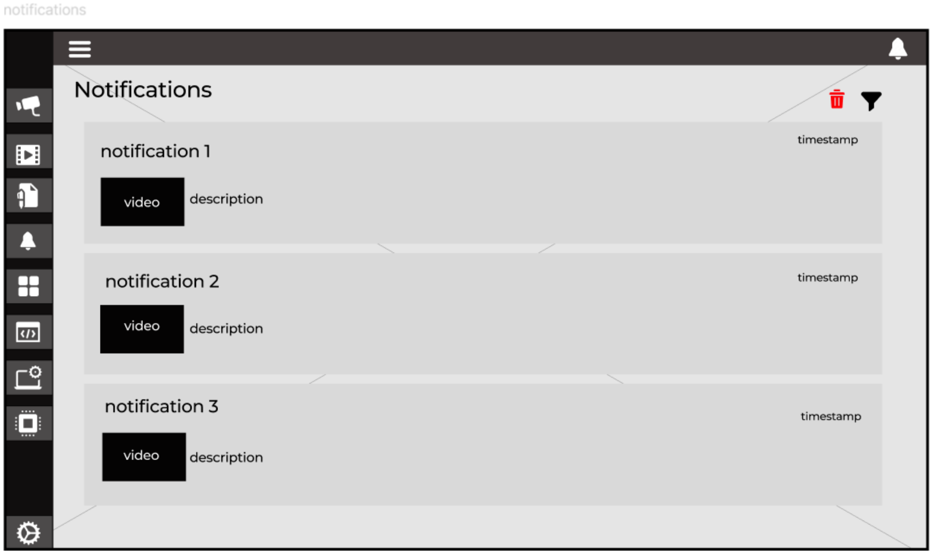


Figure 13. Wireframe Notification Page for RespoGuard

The Notification page can be the users' first reference point where they get instant messages and alerts for any unusual activities picked by the software on the monitored data. It gives the Barangay personnel the information they need to look into possible problems efficiently and take appropriate action.

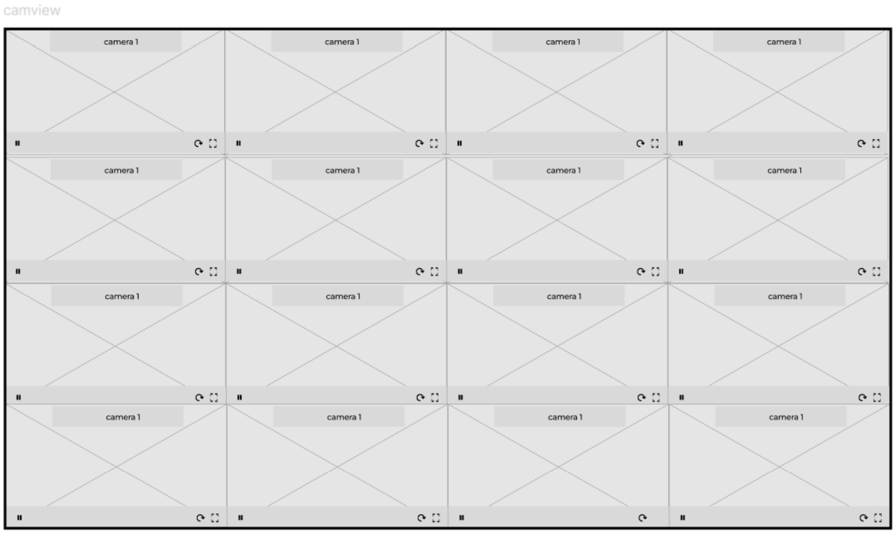
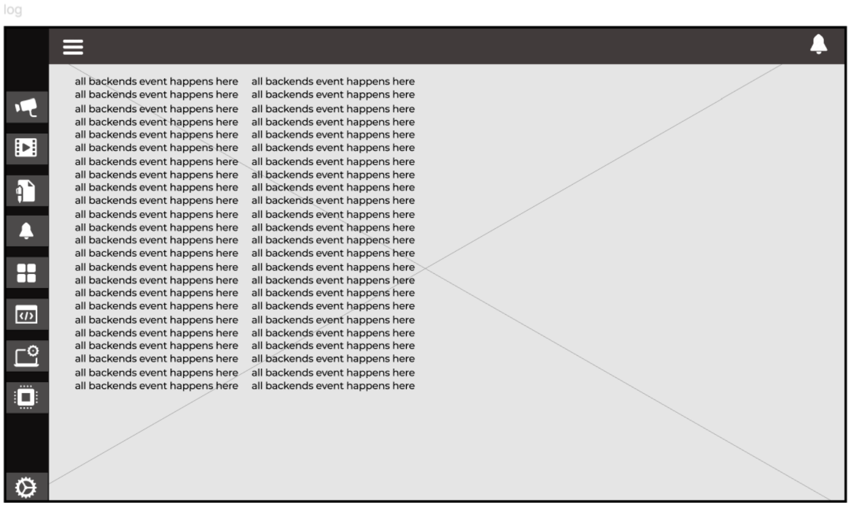


Figure 14. Wireframe for Live CCTV Grid for RespoGuard

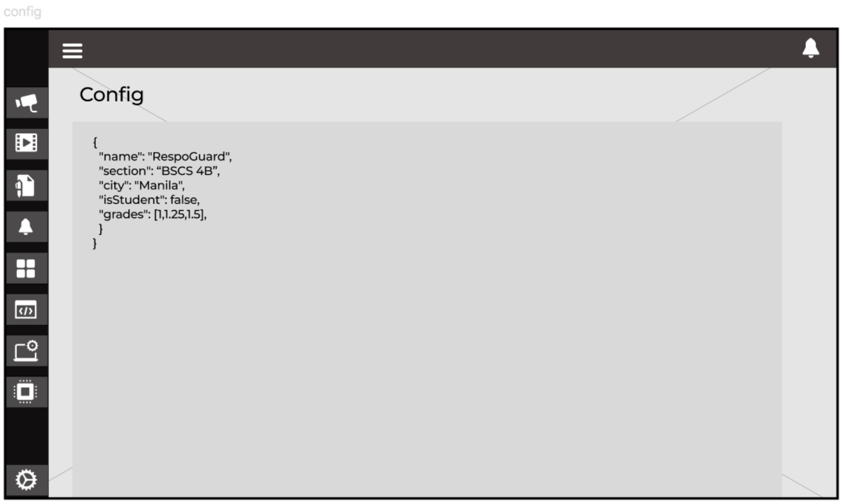
Figure 14 shows the wireframe for the structured grid layout displaying real-time video feeds from the security system. By allowing the Barangay personnel to watch numerous video feeds at once, this function enables quick detection and action in the event of any anomalies or suspicious activity inside the monitored area.



```
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
all backends event happens here    all backends event happens here
```

Figure 15. Wireframe for System Log for RespoGuard

The system log includes important events including anomaly detections, camera activations, anomaly alerts, and hardware malfunctions like camera offline instances. To provide efficient management of system performance and security, it acts as an extensive inspection, helping Barangay personnel to examine previous actions, identify problems, and evaluate information around spotted abnormalities.



```
{
  "name": "RespoGuard",
  "section": “BSCS 4B”,
  "city": "Manila",
  "isStudent": false,
  "grades": [1,1.25,1.5],
  }
}
```

Figure 16. Wireframe for CCTV Configuration for RespoGuard

Barangay personnel can configure and modify CCTV camera parameters, including resolution, bitrate, and frame rate, in the CCTV configuration area. This feature ensures effective use of computing resources by enabling users to customize the system to particular monitoring requirements.

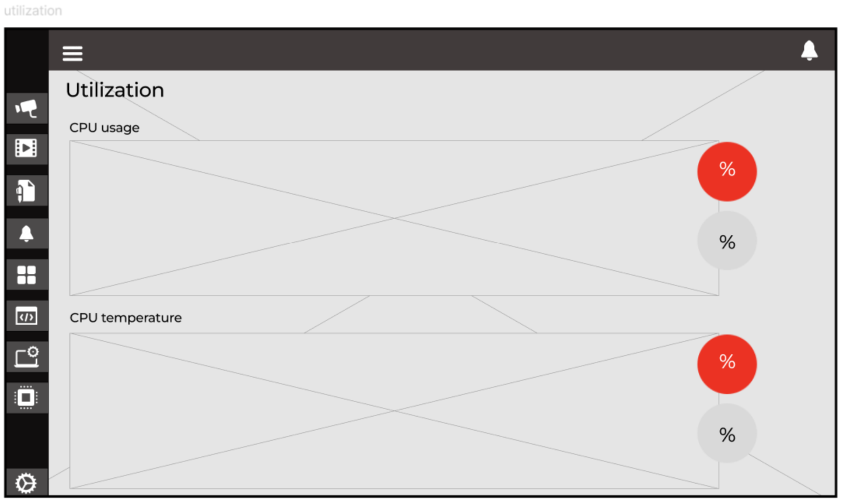
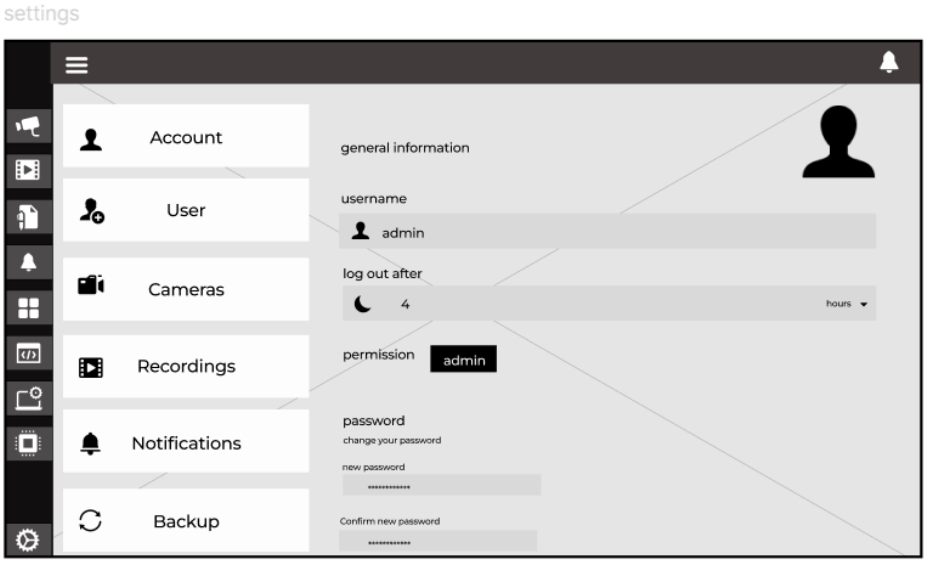


Figure 17. Wireframe for Sources Utilization for RespoGuard

The figure above is the wireframe of the Sources Utilization page of the system which includes the monitoring and management of resources, such as CPU usage, memory consumption, and processing components. With this feature, Barangay personnel can make sure that the anomaly detection system operates consistently even in situations where workloads are heavy, optimize system performance, and allocate resources efficiently.



username
admin

log out after
4 hours

permission admin

password
change your password
new password
••••••••••••
Confirm new password
••••••••••••

Figure 18. Wireframe for Settings Page for RespoGuard

The Settings page serves as a complete control center for users to monitor and adjust many parts of the system. It has sub-pages such as Profile, Cameras, User, Recordings, Backup, and System Configuration. This interface gives users the ability to customize the system to meet their unique requirements, from setting up user profiles and camera settings to handling recordings and system backups, guaranteeing effective operation and precise anomaly identification.

Operation and Testing Procedure

Software evaluation and testing of the system to make sure the system is free of issues, functionality and user friendliness. There should be errors or any glitches that could affect the user experience using the software.

SYSTEM FUNCTION	PROCEDURE	EXPECTED OUTPUT
Registration	• Direct to sign-in page. • input the default username. • Input the default password. • Click the "Sign In" button. • Access the account/dashboard upon successful sign-in.	• Successful login/ Redirecting to the Dashboard. • Incorrect email and password display an error output • Server error: if shows a code bugs and error.
Dashboard	• Log in to Dashboard • Navigate to camera views • View overall camera feeds • Check notifications • Has a navigation bar on sides (cameras, Recordings, reports, notifications, camview, console, config, and utilizations. • Ensure that all connected cameras are	• Provide a comprehensive overview of system status, camera views, camera feeds and camera zoom. • Sort feature • Allows to personalize the system overall via dashboard • Display notification tab or icon • Display notifications details

	listed and streaming live. • Check for the presence of essential elements such as navigation menus, any notifications/alerts, as recent activity, or system status. • Verify that users can navigate seamlessly.	• Provides intuitive pathways between camera views, notifications and other features.
Cameras tab	• Access the Camera tab • View and navigate total number of cameras • Observed the count of cameras on the tab • Check the status of each camera • Configure each camera • Select a specific camera to configure. • Edit and redirect to reports • Ensure that live feeds display smoothly. • Ensure that all connected cameras are listed and streaming live.	• Live camera feeds should be displayed accurately and in real-time. • Monitors can be viewed into specific zones for better management. • Provide a display of total number of cameras • Provide camera status if it is on/off for each camera. • Provide a specific description about the name of the camera and timestamp.
Recordings tab	• Access the recording page tab • View the number of caught videos of detection. • View the total count of recorded videos associated detection alarms. • Review the list of recorded videos. • Checking for the timestamp of each video • Edit, download or delete the specific recorded video.	• Display the number of caught videos of the detection • Provides an overview of the total count of recorded videos • Listed Sequentially of each video. • Timestamp must show when the detection happens. • Controls (play, pause, download, and screen view)

	• Download the specific video for report page/tab	
Reports tab	• Redirect to the report page/tab. • View the downloaded video and locate the form to fill up the report. • Fill up the form. • Enter relevant details regarding the report like the description, and types of detection, and manually classify the detection video. • Click the "Submit" button or equivalent action to send the filled-up form report. • Navigate back to the main dashboard or other sections as needed.	• Successfully direct to report tab • The form with a complete description must be saved in the reports tab • Types of detection is classified • Clearly labeled after submitting.
Notification tab	• Navigate to the notification tab • Review detected video notifications • View anomaly detection notifications • Check if there is error sign-in or error logins of users • Check for notifications when camera go offline or disconnected.	• Detected video notifications • Notifications regarding to detected actions by cameras • Error Log-in or attempts notifications • Camera disconnections notifications • Take action like view the detected video notifications, Log-in error or attempts and camera reconnecting.
Cam view tab	• Navigate to Cam view tab • View the list of cameras • Locate the grid layouts of the cameras • Select a desired grid layout into 1x1,2x2,4x4 of your choice.	• Contains the list of cameras • Grid layout options • Camera preview per grid

Console tab	• Access to the console tab • Look for the list of backend events or possible problems • Monitor the anomaly detection status • Configure the console and to access to system logs or diagnostics.	• List of backend operations that currently happening in the system • UI system status indicators • Logs and Diagnostics
Config	• Look for fields where users can update system camera settings • Edit system settings • View configuration files • View config files directly from the interface.	• Update system information or config file • Allows users to apply changes via code and made to the configuration. • Allow the user to inspect the underlying code in the config tab.
Utilizations	• Review the list of hardware in the system and its performance. • Checking of CPU usage • Monitor temperature status	• Provide an overview of the system component status. • Display the CPU usage • Display the temperature status of the components
Settings tab	• Access the settings tab • Exploring of settings categories: Profile settings, appearance settings, Interface settings, user management settings, camera, and recordings settings. • Configure layout and organization preferences for the system. • Edit, Add, and remove user accounts,	• Allows to view the overview of the settings tab • Provide different setting categories • Configure each setting according to user's preference • Add and remove users • Camera performance • User-friendly settings • Save changes • Functionality

	including the admin privilege. • Configurations for cameras, like, quality, resolution, and IR features • Navigate to Specific Settings • Check for saved changes • Test functionality	

Evaluation Procedure

The ISO 25010 will serve as the basis for the evaluation tool that will be used to determine whether the system is acceptable.

The following are the procedures to evaluate the system:

1. Invite a total of 30 respondents, including ten (10) IT professionals, ten (10) barangay authorities, and ten (10) barangay citizens.
2. The researchers will demonstrate to the respondents how to use the system.
3. In order to determine whether or not the responders can use the system independently, they will now be invited to try it out.
4. Using the 4-point Likert scale displayed in Table 1, the respondents will be asked to assess the system using the provided assessment forms.
5. The completed evaluation forms will be processed, and the data collected will be calculated to ascertain the mean ratings.
6. The 4-point Likert Scale presented in Table 1 will also be used to interpret the adjectival ratings for the mean ratings.

Scale	Adjectival Rating	Range
4	Highly Acceptable	3.4 – 4.0
3	Very Acceptable	2.6 – 3.3
2	Acceptable	1.8 – 2.5
1	Not Acceptable	1.0 – 1.7

4-point Likert's Scale

Table 1

Table 1, The 4-point Likert scale, adjectival ratings and range are shown for each rating. The Likert scale was deployed in the system assessment on a number of factors, including Functionality, Performance, Usability, Efficiency, Maintainability, Portability, and Design.

Statistical Treatment

Weighted Mean

Since calculating the weighted mean is the simplest and fastest method of assessing the suggested system, the researchers employed this formula to acquire the result. Below is the formula:

Weighted Mean Computation

$$\textit{Weighted (W)} = \frac{F\ (x_1+x_2+....+x_n)}{n}$$

Figure 19. Statistical Mean Method

F = frequency of numbers on how many times a number is chosen by evaluator

x_1, x_2, … x_n = evaluation rating

CHAPTER 4

RESULTS AND DISCUSSION

Result and Discussion

The study's analysis and conclusions will be explained in this chapter. This chapter completes the project's description, structure, capabilities, and limitations in addition to those already discussed.

Project Description

CCTV is a surveillance tool that provides monitored areas for the purpose of keeping an eye out for prospective crimes and anomalies**.** A group inside a community as well as a large spectrum of people find value in the automated security system. Its ability to identify and react to possible criminal activity, violence, and emergencies allows locals to enjoy excellent personal protection. Barangay officials can respond and improve, since they have the advantage of supervising. Implementing RespoGuard, on a machine learning-based CCTV detection system can temporarily create a sense of community engagement. By providing a system that can detect anomalies in the community, manual surveillance can reduce the manual monitoring and give the personnel a break because there is something that secures the safety of the Barangay. The system is positioned as a tool to enhance surveillance, offering real-time detection and alerting, with human operators retaining the responsibility for interpretation and subsequent actions based on the identified anomalies.

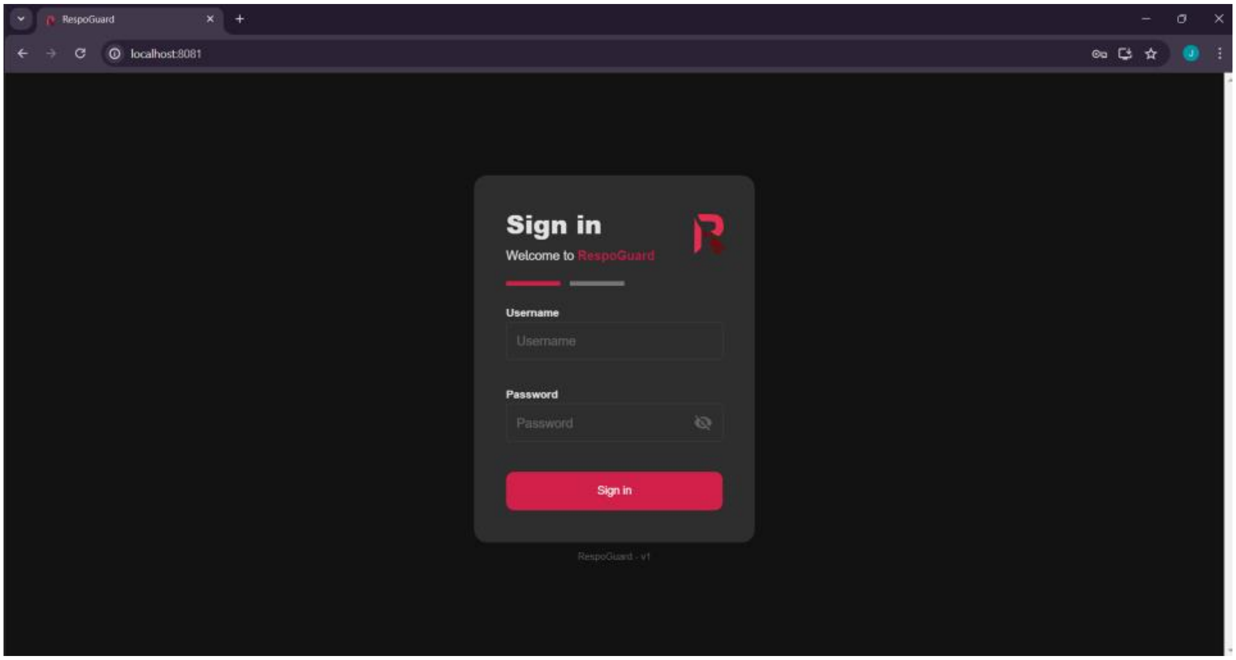
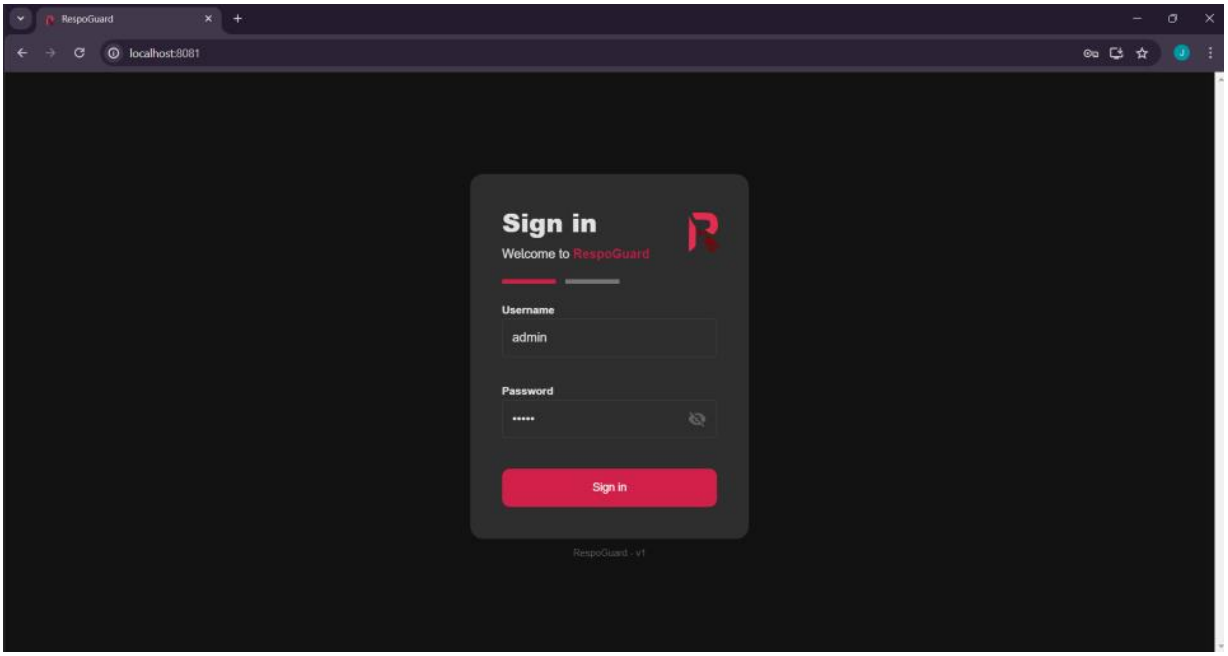


Figure 20. Actual User Interface of the RespoGuard

Project Structure



Username
admin

Password
•••••

Figure 21. RespoGuard's User's Login

Figure 21 illustrates the website user's login where Barangay staff members log in to a system using their login credentials, which include their username and password. Upon confirming the user's identification, it will let them to use the system's features and resources according to their level of authorization.

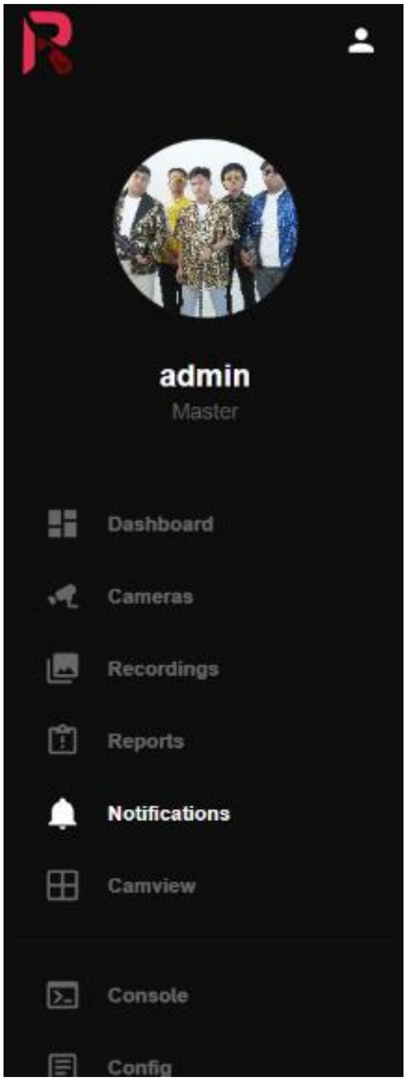


Figure 22. RespoGuard’s Navigation Bar

The Figure 22 shows the navigation bar that provides quick access to important elements for surveillance staff. It acts as the primary hub for monitoring security, managing recordings, report generation, receiving alerts, and watching camera feeds. Every tab provides users with the opportunity to immediately identify and solve any security threats by allowing them to change settings, view camera footage, and keep an eye on system activity.

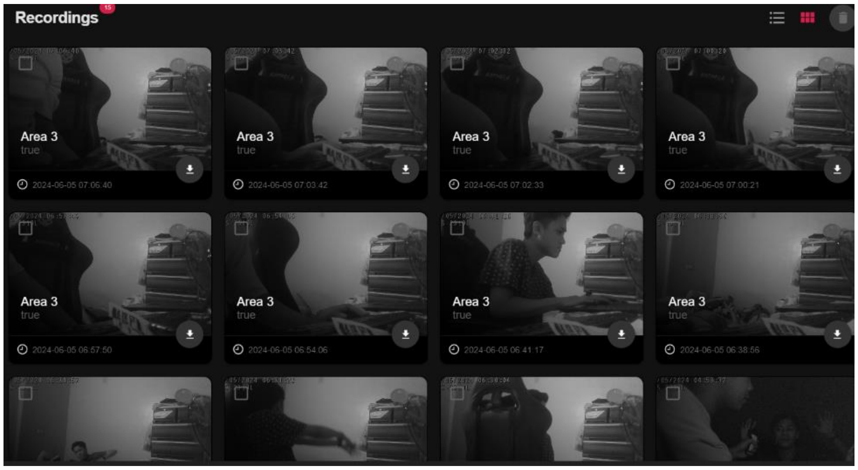
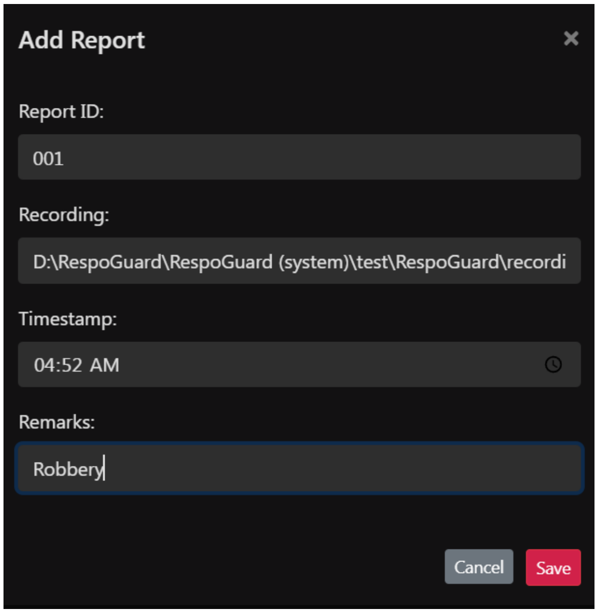


Figure 23. RespoGuard's Recording Page

Barangay staff can assess previous events using the system, which also serves as a storage space for any unusual security footage. Barangay staff can use it as an investigative tool to watch recorded footage, spot irregularities, and obtain data to improve security and incident response procedures.



Add Report ×

Report ID:

001

Recording:

D:\RespoGuard\RespoGuard (system)\test\RespoGuard\recordi

Timestamp:

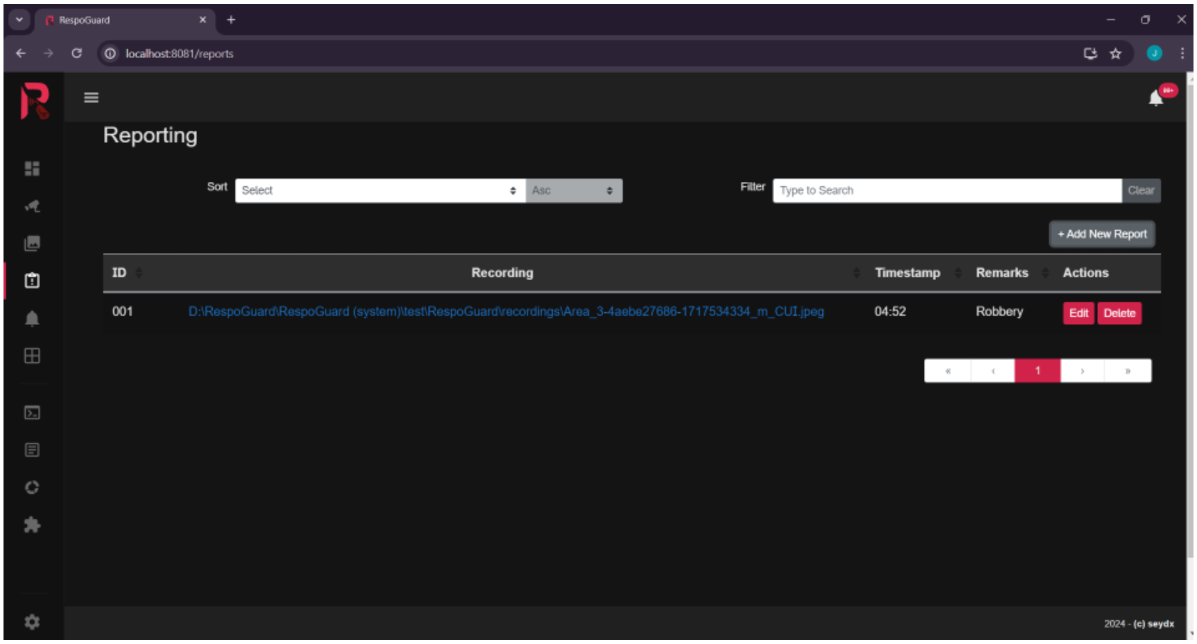
04:52 AM

Remarks:

Robbery

Figure 24. RespoGuard's Adding Report Modal

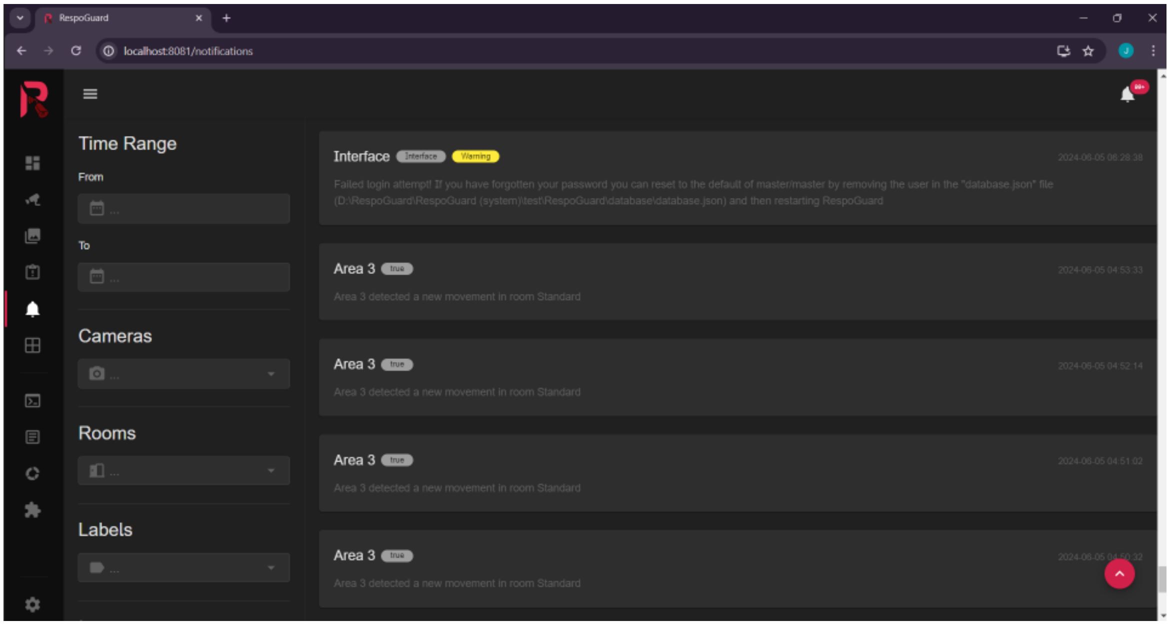
Figure 24 shows the report modal for inserting and updating reports. In the report modal, the barangay personnel can input the report ID, path of the recorded footage, date and time of the recorded event, and remarks to categorize the detected anomaly.



ID	Recording	Timestamp	Remarks	Actions
001	D:\RespoGuard\RespoGuard (system)\test\RespoGuard\recordings\Area_3-4aebe27686-1717534334_m_CUI.jpeg	04:52	Robbery	Edit Delete

Figure 25. RespoGuard's Reporting Page

The figure 25 shows the reporting page, which aims mainly to display the reporting procedure. Users can create a report and then compile its details by selecting particular attributes like timestamps, camera locations, and incident categories.



Interface Interface Warning 2024-06-05 06:28:38
Failed login attempt! If you have forgotten your password you can reset to the default of master/master by removing the user in the "database.json" file (D:\RespoGuard\RespoGuard (system)\test\RespoGuard\database\database.json) and then restarting RespoGuard

Area 3 true 2024-06-05 04:53:33
Area 3 detected a new movement in room Standard

Area 3 true 2024-06-05 04:52:14
Area 3 detected a new movement in room Standard

Area 3 true 2024-06-05 04:51:02
Area 3 detected a new movement in room Standard

Area 3 true 2024-06-05 04:50:32
Area 3 detected a new movement in room Standard

Figure 26. RespoGuard's Notification Page

In figure 26, barangay personnel can get updates and notifications about any abnormalities or strange activity detected in the data that is being viewed instantly by visiting the Notification Page, which acts as their primary point of contact. It provides the information required for the Barangay staff to effectively investigate potential issues and take necessary action.

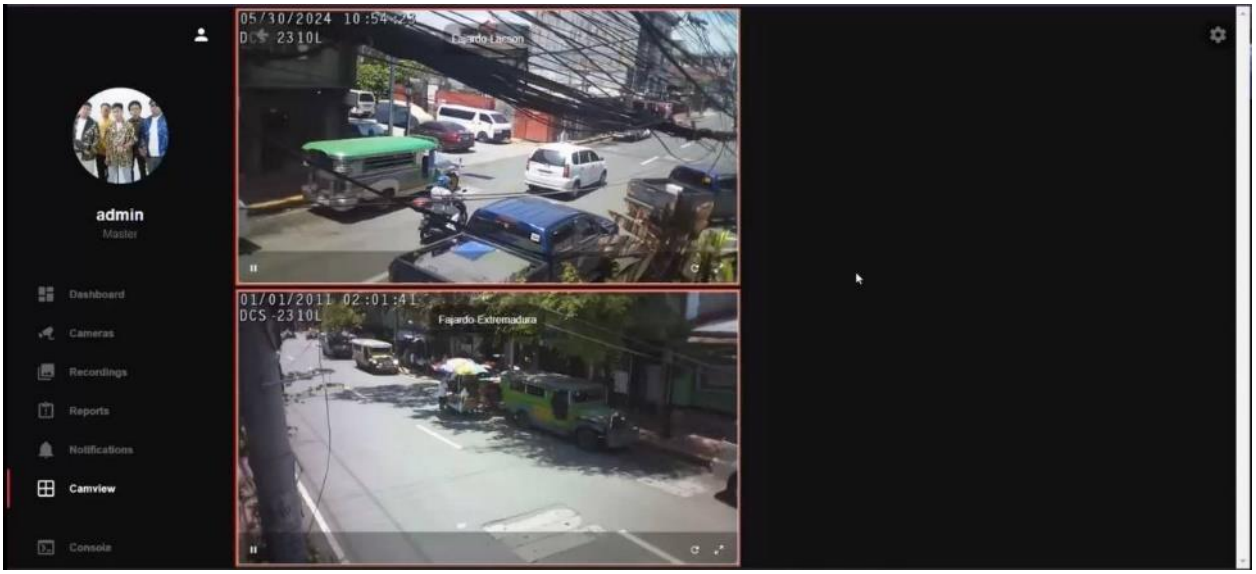
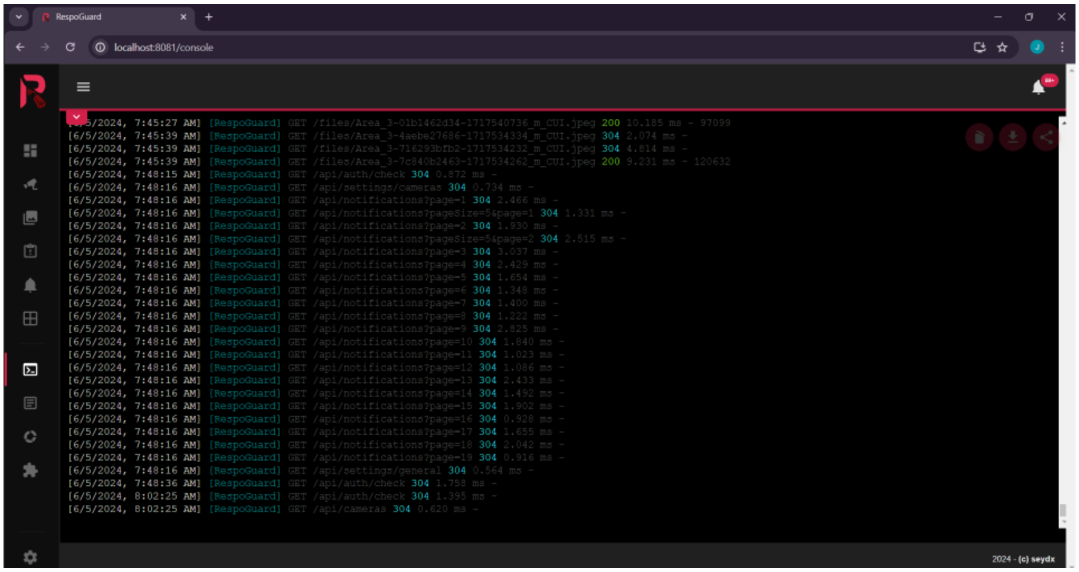


Figure 27. RespoGuard’s Live CCTV Grid

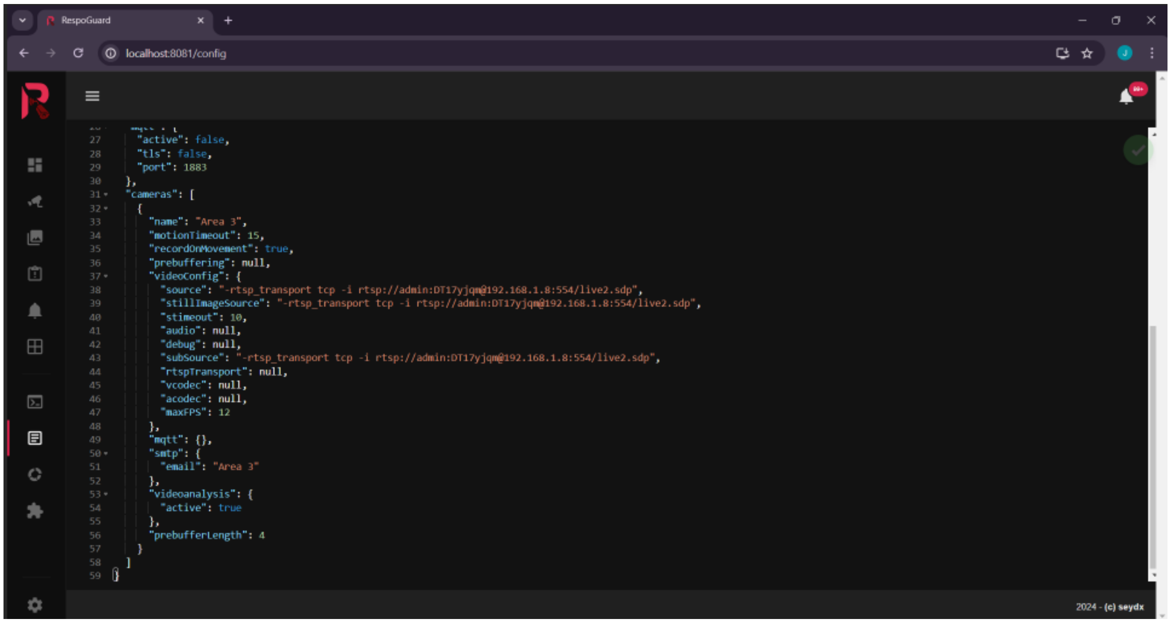
Figure 27 shows the structured grid design that shows the security system's live video feeds. This feature makes it possible for the Barangay staff to monitor many video feeds simultaneously, which facilitates prompt detection and response if any anomalies or suspicious activity occurs inside the monitored area.



```
[6/5/2024, 7:45:27 AM] [RespoGuard] GET /files/Area_3-01b1462d34-1717540736_m_CUI.jpeg 200 10.185 ms - 97099
[6/5/2024, 7:45:39 AM] [RespoGuard] GET /files/Area_3-4aebe27686-1717534334_m_CUI.jpeg 304 2.074 ms -
[6/5/2024, 7:45:39 AM] [RespoGuard] GET /files/Area_3-716293bfb2-1717534232_m_CUI.jpeg 304 4.814 ms -
[6/5/2024, 7:45:39 AM] [RespoGuard] GET /files/Area_3-7c840b2463-1717534262_m_CUI.jpeg 200 9.231 ms - 120632
[6/5/2024, 7:48:15 AM] [RespoGuard] GET /api/auth/check 304 0.872 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/settings/cameras 304 0.734 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=1 304 2.466 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?pageSize=5&page=1 304 1.331 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=2 304 1.930 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?pageSize=5&page=2 304 2.515 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=3 304 3.037 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=4 304 2.429 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=5 304 1.654 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=6 304 1.348 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=7 304 1.400 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=8 304 1.222 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=9 304 2.825 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=10 304 1.840 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=11 304 1.023 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=12 304 1.086 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=13 304 2.433 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=14 304 1.492 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=15 304 1.902 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=16 304 0.928 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=17 304 1.655 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=18 304 2.042 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/notifications?page=19 304 0.916 ms -
[6/5/2024, 7:48:16 AM] [RespoGuard] GET /api/settings/general 304 0.564 ms -
[6/5/2024, 7:48:36 AM] [RespoGuard] GET /api/auth/check 304 1.758 ms -
[6/5/2024, 8:02:25 AM] [RespoGuard] GET /api/auth/check 304 1.395 ms -
[6/5/2024, 8:02:25 AM] [RespoGuard] GET /api/cameras 304 0.620 ms -
```

Figure 28. RespoGuard’s System Log

In figure 28, important events like as anomaly detections, camera activations, anomaly alerts, and hardware failures such as camera disconnection instances are recorded in the system log. It serves as a thorough examination to enable effective management of system performance and security, assisting Barangay staff in reviewing earlier activities, spotting issues, and assessing data regarding anomalies observed.



```
    "active": false,
    "tls": false,
    "port": 1883
  },
  "cameras": [
    {
      "name": "Area 3",
      "motionTimeout": 15,
      "recordOnMovement": true,
      "prebuffering": null,
      "videoConfig": {
        "source": "-rtsp_transport tcp -i rtsp://admin:DT17yjqm@192.168.1.8:554/live2.sdp",
        "stillImageSource": "-rtsp_transport tcp -i rtsp://admin:DT17yjqm@192.168.1.8:554/live2.sdp",
        "stimeout": 10,
        "audio": null,
        "debug": null,
        "subSource": "-rtsp_transport tcp -i rtsp://admin:DT17yjqm@192.168.1.8:554/live2.sdp",
        "rtspTransport": null,
        "vcodec": null,
        "acodec": null,
        "maxFPS": 12
      },
      "mqtt": {},
      "smtp": {
        "email": "Area 3"
      },
      "videoanalysis": {
        "active": true
      },
      "prebufferLength": 4
    }
  ]
}
```

Figure 29. RespoGuard’s CCTV Configuration

Figure 29 shows the CCTV configuration area, barangay staff can adjust and change the resolution, bitrate, and frame rate of CCTV cameras. By letting users customize the system to specific monitoring needs, this feature guarantees efficient use of computing resources.

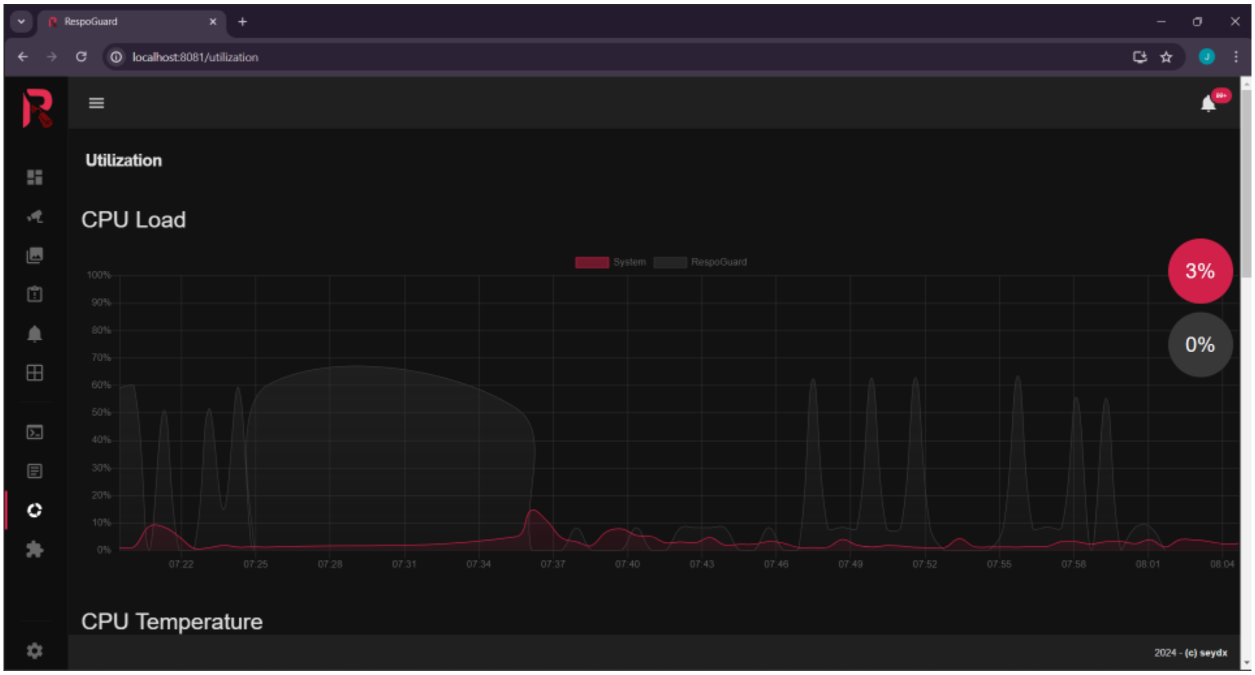
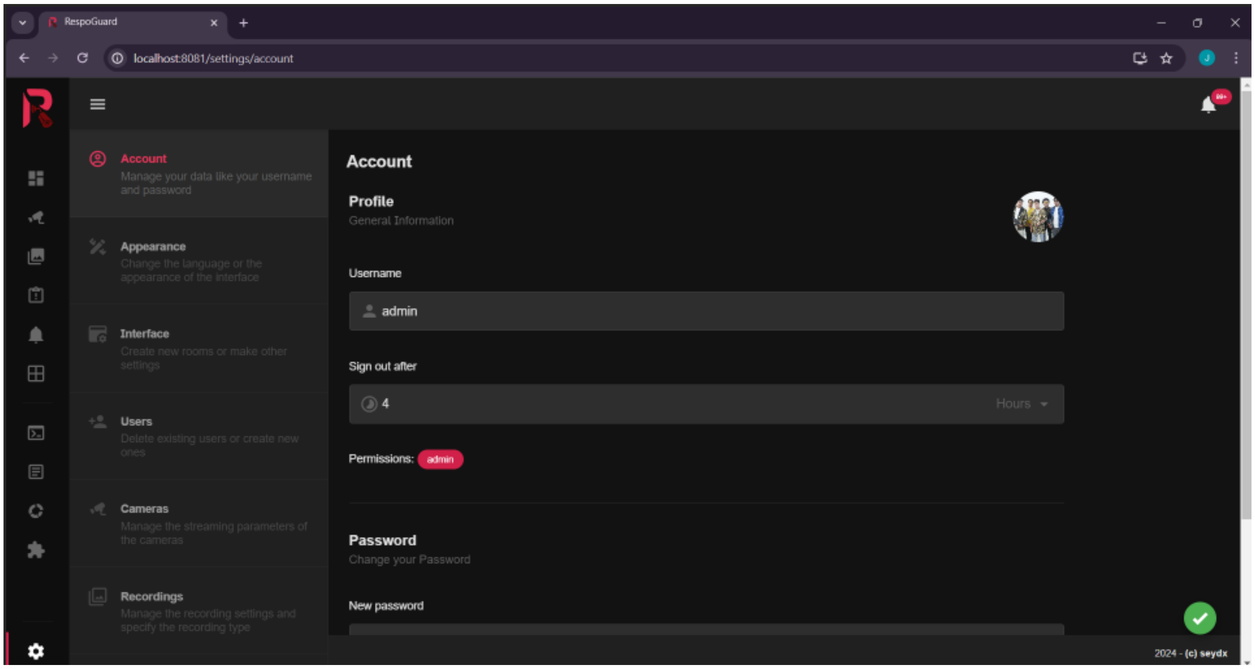


Figure 30. RespoGuard’s Resources Utilization Page

Figure 30 shows the system's resources utilization page, which manages resource management and monitoring, involves tracking CPU and memory usage as well as processing component usage. Barangay staff may maximize system performance and allocate resources effectively using this feature, ensuring that the anomaly detection system continues to function reliably even under high workload conditions.


RespoGuard
localhost:8081/settings/account
Account
Manage your data like your username and password
Appearance
Change the language or the appearance of the interface
Interface
Create new rooms or make other settings
Users
Delete existing users or create new ones
Cameras
Manage the streaming parameters of the cameras
Recordings
Manage the recording settings and specify the recording type
99+
2024 - (c) seydx

Account

Profile
General Information

Username: admin

Sign out after: 4 Hours

Permissions: admin

Password
Change your Password

New password

Figure 31. RespoGuard’s Settings Page

In figure 31, the settings page serves as a complete control center for users to monitor and adjust many parts of the system. It has sub-pages such as Profile, Cameras, User, Recordings, Backup, and System Configuration. This interface gives users the ability to customize the system to meet their unique requirements, from setting up user profiles and camera settings to handling recordings and system backups, guaranteeing effective operation and precise anomaly identification.

System Capabilities

- **Anomaly Detection:** Use machine learning algorithms to systematically identify anomalies, such as shootings, robberies, fights, assaults, and road accidents.
- **Automated Alerts**: Upon detecting anomalies, immediately notify law enforcement or barangay authorities via Telegram and through RespoGuard’s notification page.
- **CCTV Configuration**: The system supports configuration for multiple cameras. Users can add, remove, and configure camera settings including the video resolution, frame rate, and

bit rate.

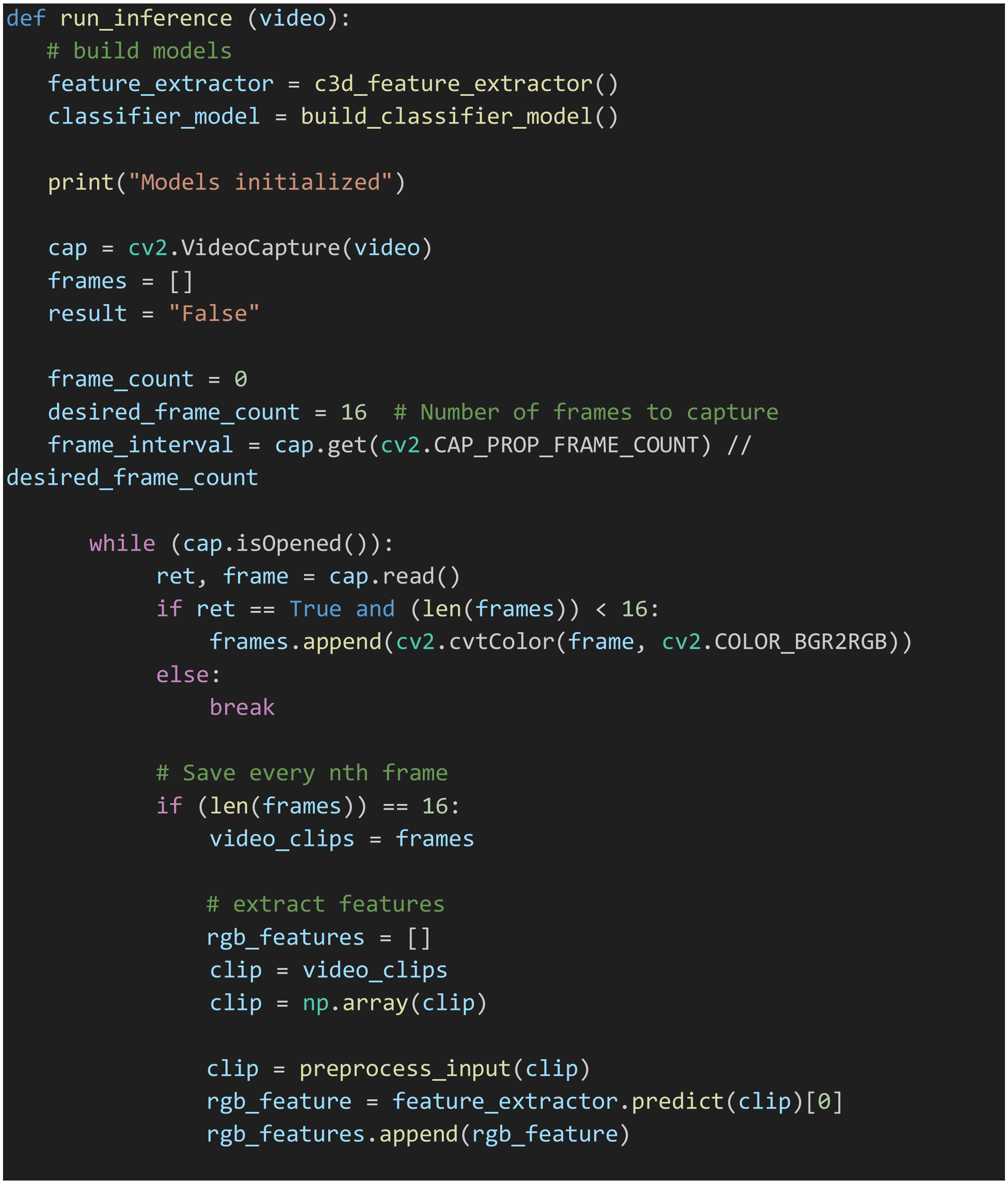
- **Comprehensive Reports**: The system allows barangay personnel to generate detailed reports on detected anomalies, including time stamps, locations, and event category.
- **Continuous Learning**: To increase accuracy over time, update the trained model frequently in response to new data from the generated reports.
- **Event Recording**: All detected anomalous events are recorded for further review and analysis.
- **Hardware Integration:** The system is compatible with various hardware, including Digital Video Recorders (DVRs), Closed-Circuit Television (CCTV) cameras, and standard computers or laptops. The system was already tested using some of the widely used CCTV and DVR such as Dahua and Hikvision.
- **Log in System**: A secure login system ensures data integrity and prevents tampering, allowing authorized personnel to access and manage the data.
- **Real-Time Detection**: It can process live surveillance feeds and detect unusual activities in real-time, allowing for immediate action.
- **Web Application**: Intuitive and user-friendly interface, enabling easy monitoring and management of the surveillance system.

System Limitations

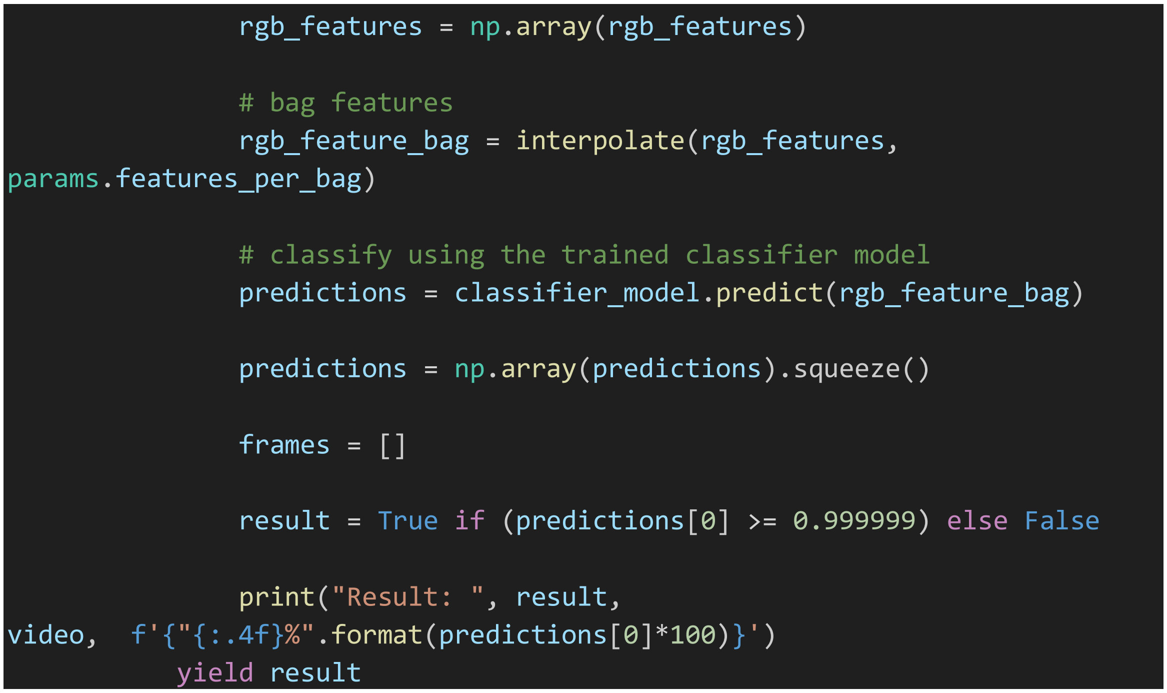
- **Restricted Data Coverage**: Not all locations may be covered by surveillance cameras, creating blind zones where anomalies may go undetected.
- **False Positives/Negatives**: Anomaly detection systems may generate false positives, which misidentify typical activity as abnormal, or false negatives, which fail to identify real anomalies, which compromises the dependability and credibility of the system.
- **Scalability**: Increasing the system's reach or handling higher data quantities may provide technological difficulties in terms of processing power, network throughput, and storage

space.

- **Data Quantity and Quality**: The system's efficacy is largely dependent on the quality and volume of surveillance data that is accessible. Poor or low-quality data can make anomaly detection less accurate.

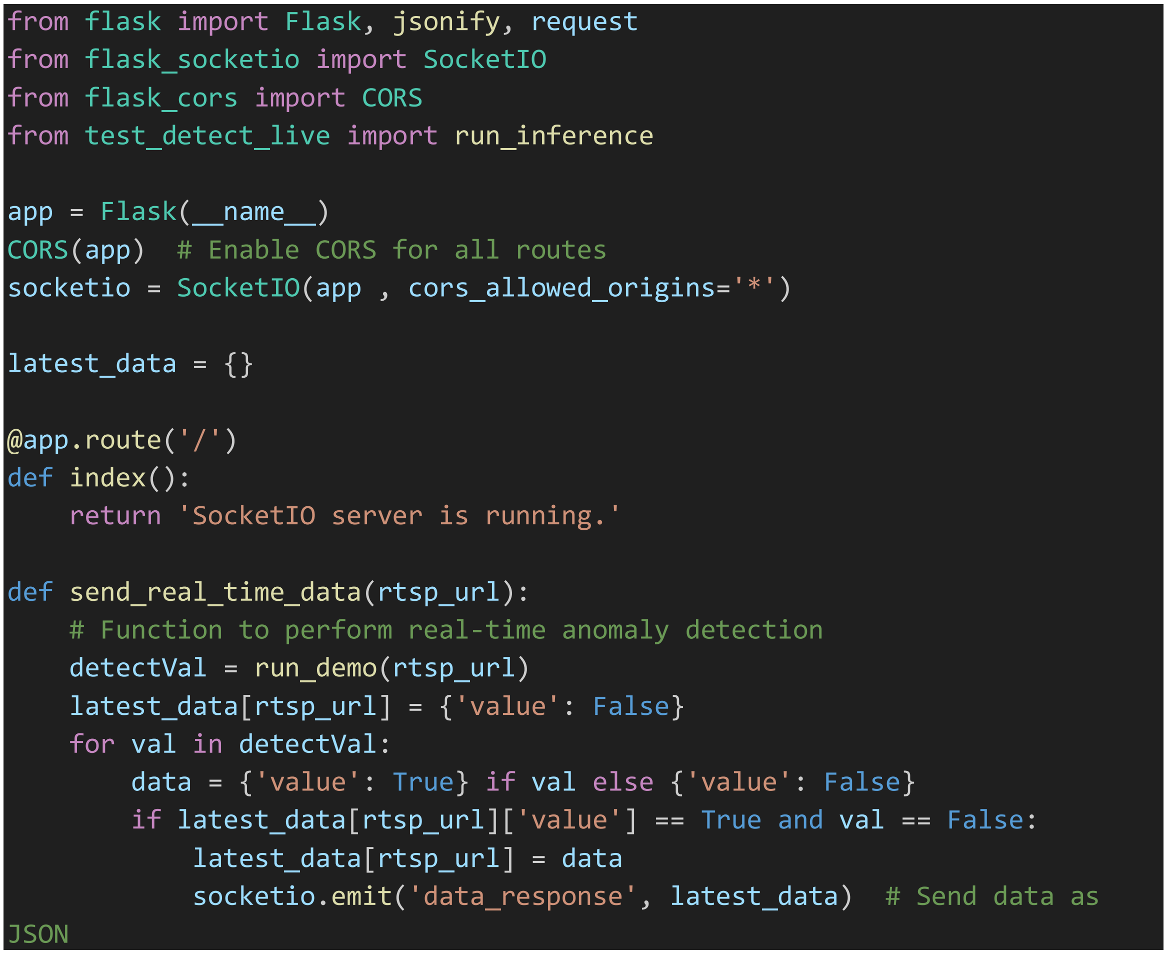


```
def run_inference (video):
    # build models
    feature_extractor = c3d_feature_extractor()
    classifier_model = build_classifier_model()

    print("Models initialized")

    cap = cv2.VideoCapture(video)
    frames = []
    result = "False"

    frame_count = 0
    desired_frame_count = 16  # Number of frames to capture
    frame_interval = cap.get(cv2.CAP_PROP_FRAME_COUNT) //
desired_frame_count

        while (cap.isOpened()):
            ret, frame = cap.read()
            if ret == True and (len(frames)) < 16:
                frames.append(cv2.cvtColor(frame, cv2.COLOR_BGR2RGB))
            else:
                break

            # Save every nth frame
            if (len(frames)) == 16:
                video_clips = frames

                # extract features
                rgb_features = []
                clip = video_clips
                clip = np.array(clip)

                clip = preprocess_input(clip)
                rgb_feature = feature_extractor.predict(clip)[0]
                rgb_features.append(rgb_feature)
```

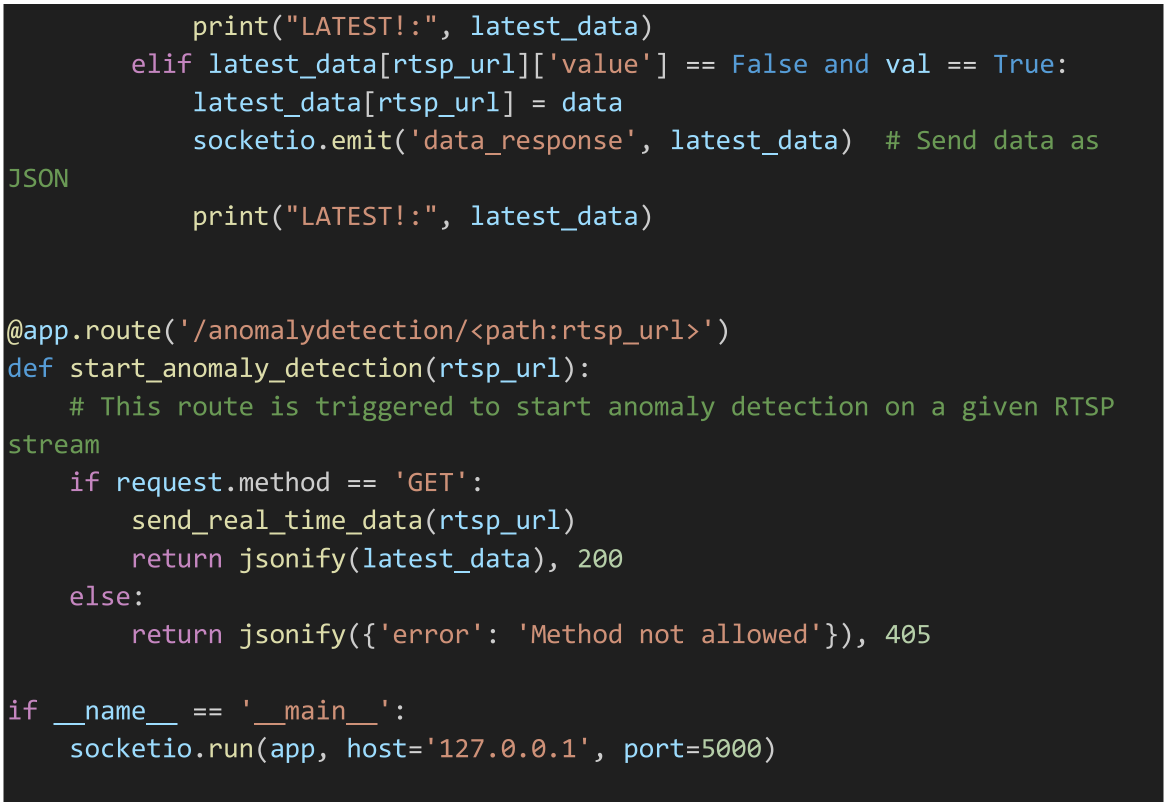


```
               rgb_features = np.array(rgb_features)

               # bag features
               rgb_feature_bag = interpolate(rgb_features, 
params.features_per_bag)

               # classify using the trained classifier model
               predictions = classifier_model.predict(rgb_feature_bag)

               predictions = np.array(predictions).squeeze()

               frames = []

               result = True if (predictions[0] >= 0.999999) else False

               print("Result: ", result, 
video,  f'{"{:.4f}%".format(predictions[0]*100)}')
           yield result
```

Figure 32. *Code snippet for the Inference of Real-Time Stream of a Surveillance Footage*



```
from flask import Flask, jsonify, request
from flask_socketio import SocketIO
from flask_cors import CORS
from test_detect_live import run_inference

app = Flask(__name__)
CORS(app)  # Enable CORS for all routes
socketio = SocketIO(app , cors_allowed_origins='*')

latest_data = {}

@app.route('/')
def index():
    return 'SocketIO server is running.'

def send_real_time_data(rtsp_url):
    # Function to perform real-time anomaly detection
    detectVal = run_demo(rtsp_url)
    latest_data[rtsp_url] = {'value': False}
    for val in detectVal:
        data = {'value': True} if val else {'value': False}
        if latest_data[rtsp_url]['value'] == True and val == False:
            latest_data[rtsp_url] = data
            socketio.emit('data_response', latest_data)  # Send data as 
JSON
```



```
            print("LATEST!:", latest_data)
        elif latest_data[rtsp_url]['value'] == False and val == True:
            latest_data[rtsp_url] = data
            socketio.emit('data_response', latest_data)  # Send data as
JSON
            print("LATEST!:", latest_data)


@app.route('/anomalydetection/<path:rtsp_url>')
def start_anomaly_detection(rtsp_url):
    # This route is triggered to start anomaly detection on a given RTSP
stream
    if request.method == 'GET':
        send_real_time_data(rtsp_url)
        return jsonify(latest_data), 200
    else:
        return jsonify({'error': 'Method not allowed'}), 405

if __name__ == '__main__':
    socketio.run(app, host='127.0.0.1', port=5000)
```

Figure 33. *Code snippet for the API of the RespoGuard's Anomaly Detection*

Project Evaluation

The total number of respondents who were evaluated by the system was 30. The respondents included ten (10) IT professionals, ten (10) barangay authorities, and ten (10) barangay citizens. The system was evaluated by respondents using 10 questions based on Functionality, Performance/Usability/Efficiency, and Maintainability/Portability/Design of ISO 25010.

Table 2. Responses to Functionality by IT Professionals

	Mean	**Interpretation**
Functions that are required for the systems are implemented	3.7	Highly Acceptable
The system's input and output are accurate	3.6	Highly Acceptable
The system's modules are working and connected properly	3.7	Highly Acceptable

There is a substantial system security	3.6	Highly Acceptable
Average	3.65	Highly Acceptable

In the Functionality evaluated by 10 IT Professionals, 92.5% of the respondents gives a Highly Acceptable grade in the statement "*Functions that are required for the systems are implemented*". 90% of the respondents give a Highly Acceptable Interpretation on the system and output accuracy statement. For the 3rd statement, 92.5% of the respondents said it is Highly Acceptable. Meanwhile, for the substantial system security, 90% of the respondents give a Highly Acceptable answer. Overall, 91.25% of the respondents Highly Accepted the Functionality.

Table 3. Responses to Functionality by Barangay Authorities

	Mean	**Interpretation**
Functions that are required for the systems are implemented	4	Highly Acceptable
The system input and output are accurate	3.9	Highly Acceptable
The system Modules are working and connected properly	4	Highly Acceptable
There is a substantial system security	3.5	Highly Acceptable
Average	3.85	Highly Acceptable

In the Functionality evaluated by 10 Barangay Authorities, 100% of the respondents gave a Highly Acceptable grade that the functions that are required for the systems are implemented. 97.5% of the respondents give the system and output accuracy a Highly Acceptable. For the system modules are working and connected properly, 100% of the respondents said it is Highly Acceptable. Meanwhile, for the substantial system security, 87.5% of the respondents give a Highly Acceptable answer. Overall, 96.25% of the respondents Highly Accepted the Functionality.

Table 4. Responses to Functionality by Barangay Citizens

	Mean	**Interpretation**
Functions that are required for the systems are implemented	3.8	Highly Acceptable
The system input and output are accurate	3.7	Highly Acceptable
The system Modules are working and connected properly	3.8	Highly Acceptable
There is a substantial system security	3.8	Highly Acceptable
Average	3.78	Highly Acceptable

In the Functionality that was evaluated by 10 Barangay Citizens, 95% of the respondents gave a Highly Acceptable grade that the functions that are required for the systems are implemented. 92.5% of the respondents give the system and output accuracy a Highly Acceptable. For the system modules are working and connected properly, 95% of the respondents said it is Highly Acceptable. Meanwhile, for the substantial system security, 95% of the respondents give a Highly Acceptable answer. Overall, 94.5% of the respondents Highly Accepted the Functionality.

Table 5. Responses to Performance, Usability, and Efficiency by IT Professionals

	Mean	**Interpretation**
The system is error free (syntax, logic, run-time)	3.4	Highly Acceptable
Easy to operate and remember	3.4	Highly Acceptable
Allows effective use of system resources	3.8	Highly Acceptable
Average	3.53	Highly Acceptable

Ten (10) IT Professionals evaluated the Performance, Usability, and Efficiency. 85% of the respondents give a Highly Acceptable that the system is error free. For the Usability of the system, 85% of the respondents give a Highly Acceptable answer. Meanwhile, for Efficiency, 95% of the respondents Highly Accepted the effective use of system resources. On Average, 88.25% of the respondents Highly Accepted the Performance, Usability, and Efficiency of the system.

Table 6. Responses to Performance, Usability, and Efficiency by Barangay Authorities

	Mean	**Interpretation**
The system is error free (syntax, logic, run-time)	3.3	Very Acceptable
Easy to operate and remember	3.6	Highly Acceptable
Allows effective use of system resources	3.9	Highly Acceptable
Average	3.6	Highly Acceptable

Ten (10) Barangay Authorities evaluated the Performance, Usability, and Efficiency. 82.5% of the respondents gave a Very Acceptable that the system is error free. For the Usability of the system, 90% of the respondents give a Highly Acceptable answer. Meanwhile, for Efficiency, 97.5% of the respondents Highly Accepted the effective use of system resources. On Average, 90% of the respondents Highly Accepted the Performance, Usability, and Efficiency of the system.

Table 7. Responses to Performance, Usability, and Efficiency by Barangay Citizens

	Mean	**Interpretation**
The system is error free (syntax, logic, run-time)	3.4	Highly Acceptable
Easy to operate and remember	3.5	Highly Acceptable
Allows effective use of system resources	3.7	Highly Acceptable
Average	3.53	Highly Acceptable

Ten (10) Barangay Citizens evaluated the Performance, Usability, and Efficiency. 85% of the respondents give a Highly Acceptable answer that the system is error free. For the Usability of the system, 87.5% of the respondents give a Highly Acceptable answer. Meanwhile, for Efficiency, 92.5% of the respondents Highly Accepted the effective use of system resources. On Average, 88.25% of the respondents Highly Accepted the Performance, Usability, and Efficiency of the system.

Table 8. Responses to Maintainability, Portability, and Design by IT Professionals

	Mean	**Interpretation**
Easy to expand and modify to adapt to new changes	3.4	Highly Acceptable
Can run on different environments	3.7	Highly Acceptable
The GUI design used was clear, neat, and visible.	4	Highly Acceptable
Average	3.7	Highly Acceptable

In the Maintainability, Portability, and Design, ten (10) IT Professionals were asked to evaluate. 85% of the respondents give a Highly Acceptable rating for Maintainability and 92.5% for Portability of the system. While 100% of the respondents give a Highly Acceptable rating for the Design of the UI. Overall, 92.5% of the respondents rate the Maintainability, Portability, and Design a Highly Acceptable grade.

Table 9. Responses to Maintainability, Portability, and Design Barangay Authorities

	Mean	**Interpretation**
Easy to expand and modify to adapt to new changes	3.4	Highly Acceptable
Can run on different environments	3.4	Highly Acceptable
The GUI design used was clear, neat, and visible.	4	Highly Acceptable
Average	3.6	Highly Acceptable

In the Maintainability, Portability, and Design, ten (10) Barangay Authorities were asked to evaluate. 85% of the respondents give a Highly Acceptable rating for both Maintainability and Portability of the system. While 100% of the respondents give a Highly Acceptable rating for the Design of the UI. Overall, 90% of the respondents rate the Maintainability, Portability, and Design a Highly Acceptable grade.

Table 10. Responses to Maintainability, Portability and Design Barangay Citizens

	Mean	**Interpretation**
Easy to expand and modify to adapt to new changes	3.4	Highly Acceptable
Can run on different environments	3.4	Highly Acceptable
The GUI design used was clear, neat, and visible.	4	Highly Acceptable
Average	3.6	Highly Acceptable

In the Maintainability, Portability, and Design, ten (10) Barangay Citizens were asked to evaluate. 85% of the respondents give a Highly Acceptable rating for both Maintainability and Portability of the system. While 100% of the respondents give a Highly Acceptable rating for the Design of the UI. Overall, 90% of the respondents rate the Maintainability, Portability, and Design a Highly Acceptable grade.

Table 11. Overall Summary of Responses

	Total Mean	**Interpretation**
Functionality	3.76	Highly Acceptable
Performance/Usability/Efficiency	3.55	Highly Acceptable
Maintainability/Portability/Design	3.63	Highly Acceptable

Table 12

Evaluation Result and Weighted Mean Computation for Functionality

IT – IT Professionals BA – Barangay Authorities

BC – Barangay Citizen

Respondents	A. **Functionality**				
	1.1	**1.2**	**1.3**	**1.4**	**Weighted Mean**
Respondent 1 (IT)	**3**	**3**	**4**	**4**	**3.5**
Respondent 2 (IT)	**4**	**4**	**4**	**3**	**3.75**

Respondent 3 (IT)	**4**	**4**	**4**	**3**	**3.75**
Respondent 4 (IT)	**4**	**4**	**3**	**3**	**3.5**
Respondent 5 (IT)	**4**	**4**	**3**	**4**	**3.75**
Respondent 6 (IT)	**3**	**3**	**4**	**4**	**3.5**
Respondent 7 (IT)	**3**	**3**	**4**	**4**	**3.5**
Respondent 8 (IT)	**4**	**4**	**3**	**3**	**3.5**
Respondent 9 (IT)	**4**	**4**	**4**	**4**	**4**
Respondent 10 (IT)	**4**	**3**	**4**	**4**	**3.75**
Respondent 11 (BC)	**4**	**4**	**4**	**3**	**3.75**
Respondent 12 (BC)	**4**	**4**	**3**	**4**	**3.75**
Respondent 13 (BC)	**4**	**4**	**4**	**4**	**4**
Respondent 14 (BC)	**4**	**4**	**4**	**4**	**4**
Respondent 15 (BC)	**4**	**3**	**4**	**3**	**3.5**
Respondent 16 (BC)	**3**	**4**	**3**	**4**	**3.5**
Respondent 17 (BC)	**4**	**4**	**4**	**4**	**4**
Respondent 18 (BC)	**3**	**3**	**3**	**4**	**3.25**
Respondent 19 (BC)	**4**	**4**	**4**	**4**	**4**
Respondent 20 (BC)	**4**	**4**	**4**	**4**	**4**
Respondent 21 (BA)	**4**	**4**	**4**	**3**	**3.75**
Respondent 22 (BA)	**4**	**4**	**4**	**4**	**4**
Respondent 23 (BA)	**4**	**4**	**4**	**3**	**3.75**
Respondent 24 (BA)	**4**	**4**	**4**	**3**	**3.75**
Respondent 25 (BA)	**4**	**4**	**4**	**4**	**4**
Respondent 26 (BA)	**4**	**4**	**4**	**4**	**4**
Respondent 27 (BA)	**4**	**3**	**4**	**3**	**3.5**
Respondent 28	**4**	**4**	**4**	**4**	**4**

(BA)					
Respondent 29 (BA)	4	4	4	4	4
Respondent 30 (BA)	4	4	4	3	3.75

Table 13

Evaluation Result and Weighted Mean Computation for Performance/Usability/Efficiency

IT – IT Professionals BA – Barangay Authorities

BC – Barangay Citizen

Respondents	B. Performance/Usability/Efficiency			
	2.1	2.2	2.3	Weighted Mean
Respondent 1 (IT)	3	3	4	3.33
Respondent 2 (IT)	4	3	4	3.67
Respondent 3 (IT)	4	3	4	3.67
Respondent 4 (IT)	4	4	4	4
Respondent 5 (IT)	4	4	4	4
Respondent 6 (IT)	3	3	4	3.33
Respondent 7 (IT)	3	3	4	3.33
Respondent 8 (IT)	3	4	3	3.33
Respondent 9 (IT)	3	4	3	3.33
Respondent 10 (IT)	3	3	4	3.33
Respondent 11 (BC)	4	3	4	3.67
Respondent 12 (BC)	3	4	4	3.67
Respondent 13 (BC)	3	4	4	3.67
Respondent 14 (BC)	4	3	4	3.67
Respondent 15 (BC)	3	4	3	3.33
Respondent 16 (BC)	4	4	4	4
Respondent 17 (BC)	4	3	4	3.67
Respondent 18 (BC)	3	3	3	3
Respondent 19 (BC)	3	3	3	3
Respondent 20 (BC)	3	4	4	3.67
Respondent 21 (BA)	3	4	4	3.67
Respondent 22 (BA)	4	4	4	4
Respondent 23 (BA)	3	4	4	3.67

Respondent 24 (BA)	**3**	**4**	**4**	**3.67**
Respondent 25 (BA)	**3**	**4**	**4**	**3.67**
Respondent 26 (BA)	**3**	**4**	**4**	**3.67**
Respondent 27 (BA)	**3**	**4**	**4**	**3.67**
Respondent 28 (BA)	**4**	**4**	**4**	**4**
Respondent 29 (BA)	**4**	**3**	**4**	**3.67**
Respondent 30 (BA)	**3**	**3**	**3**	**3**

Table 14

Evaluation Result and Weighted Mean Computation ***for*** *Maintainability/Portability/Design*

IT – IT Professionals BA – Barangay Authorities

BC – Barangay Citizen

Respondents	**C. Maintainability/Portability/Design**			
	3.1	**3.2**	**3.3**	**Weighted Mean**
Respondent 1 (IT)	**3**	**4**	**4**	**3.67**
Respondent 2 (IT)	**3**	**4**	**4**	**3.67**
Respondent 3 (IT)	**4**	**3**	**4**	**3.67**
Respondent 4 (IT)	**3**	**4**	**4**	**3.67**
Respondent 5 (IT)	**3**	**3**	**4**	**3.33**
Respondent 6 (IT)	**3**	**4**	**4**	**3.67**
Respondent 7 (IT)	**4**	**4**	**4**	**4**
Respondent 8 (IT)	**4**	**3**	**4**	**3.67**
Respondent 9 (IT)	**4**	**4**	**4**	**4**
Respondent 10 (IT)	**3**	**4**	**4**	**3.67**
Respondent 11 (BC)	**3**	**3**	**4**	**3.33**
Respondent 12 (BC)	**3**	**3**	**4**	**3.33**
Respondent 13 (BC)	**3**	**3**	**4**	**3.33**
Respondent 14 (BC)	**3**	**4**	**4**	**3.67**
Respondent 15 (BC)	**4**	**3**	**4**	**3.67**
Respondent 16 (BC)	**4**	**4**	**4**	**4**
Respondent 17 (BC)	**3**	**3**	**4**	**3.33**
Respondent 18 (BC)	**4**	**4**	**4**	**4**
Respondent 19 (BC)	**4**	**4**	**4**	**4**
Respondent 20 (BC)	**3**	**3**	**4**	**3.33**

Respondent 21 (BA)	**3**	**3**	**4**	**3.33**
Respondent 22 (BA)	**4**	**4**	**4**	**4**
Respondent 23 (BA)	**3**	**3**	**4**	**3.33**
Respondent 24 (BA)	**3**	**3**	**4**	**3.33**
Respondent 25 (BA)	**3**	**3**	**4**	**3.33**
Respondent 26 (BA)	**3**	**3**	**4**	**3.33**
Respondent 27 (BA)	**4**	**3**	**4**	**3.67**
Respondent 28 (BA)	**4**	**4**	**4**	**4**
Respondent 29 (BA)	**3**	**4**	**4**	**3.67**
Respondent 30 (BA)	**4**	**4**	**4**	**4**

CHAPTER 5

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

This chapter wraps up and summarizes the research results from the earlier chapters. This chapter contains a synopsis of results, concluding remarks, and further suggestions for individuals intending to conduct research related to the RESPOGUARD: DEVELOPMENT OF AN ANOMALY DETECTION SYSTEM FOR REAL-TIME SURVEILLANCE IN BARANGAY 294 USING MACHINE LEARNING

Summary of Findings:

In this section, the key findings from the research on RespoGuard an anomaly detection can be outlined. The aim is to present insights into the significance of the study among barangay. Through particular data analysis, important trends and visions have been identified. This summary aims to provide a clear understanding of the findings and their relevance to related surveillance system.

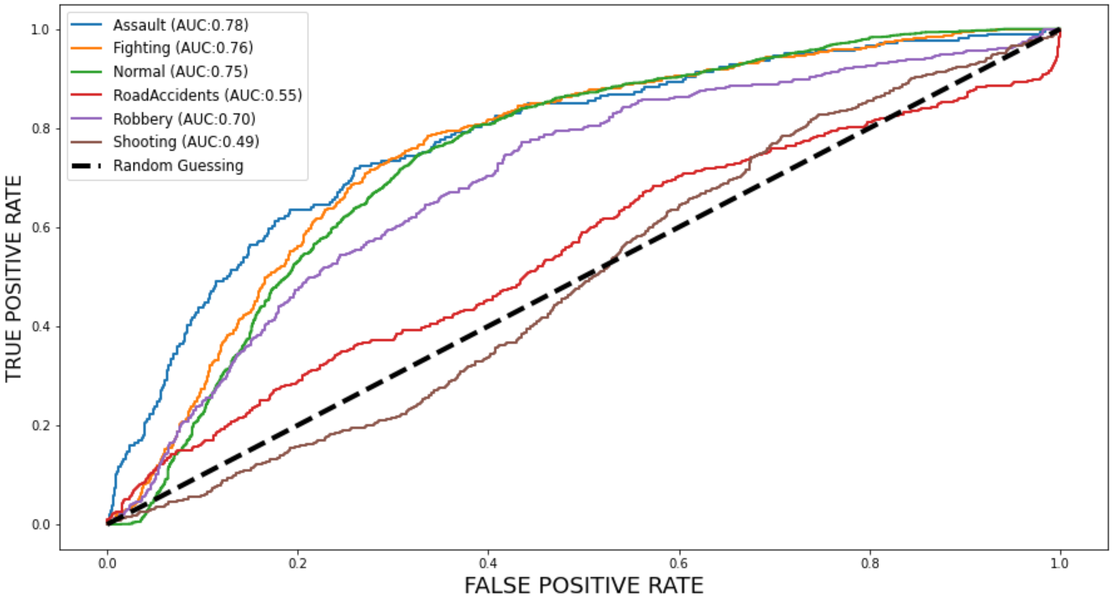
The system achieved an amazing 3.76 out of 4 for functionality, where a higher number indicates better performance. This outcome highlights the system's stability and efficiency in achieving its goal.

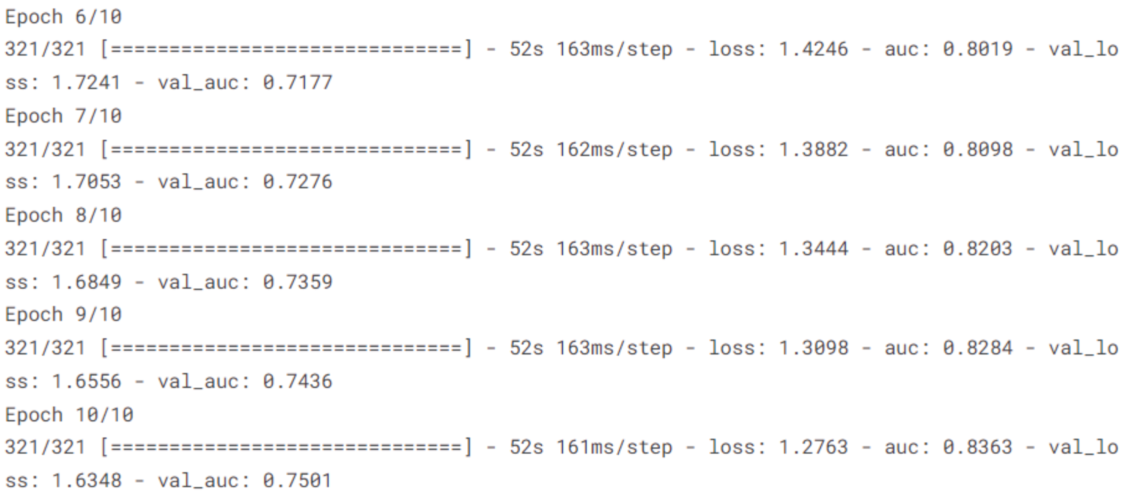
With a 3.55 performance, usability, and efficiency score, the system exhibits a respectable degree of efficacy and user-friendliness. Although this grade is a little bit below the perfect four, it nevertheless represents a significant improvement in the effectiveness and performance of the system. Expect a seamless user experience from the system, which is distinguished by its capacity to fulfill user needs and complete jobs effectively. Although there are some small areas that might be improved, the system performs brilliantly across important usability and efficiency parameters, as indicated by the interpretation of this score as highly satisfactory. This demonstrates how well it can optimize workflows, boost output, and eventually improve user happiness. The system can be further improved going ahead by utilizing the insights gained from this evaluation, guaranteeing ongoing optimization and even better performance.

Maintainability, portability, and design all received 3.63, indicating that the system performs exceptionally well in a number of crucial areas. It excels at being adaptable to new requirements and changes, with ease of expansion and modification. Its adaptability and accessibility across multiple platforms are further ensured by its capacity to operate in diverse situations. Additionally, the user experience and interaction are improved by the excellent GUI design that is used. It is distinguished by its clarity, neatness, and visibility. These characteristics add to the system's overall design, portability, and maintainability, which makes it a dependable and flexible solution for a range of situations and demands.

The system displays a highly acceptable performance across various parameters, as evidenced by the assemble score of 3.98. The system's functionality, which includes its fundamental features, was rated well, demonstrating how well it satisfies user needs. The system's capacity to provide a positive user experience while preserving efficiency was demonstrated by the respectable score received by the performance, usability, and efficiency component. Additionally, the system's adaptability, ease of maintenance, and well-designed user interface were highlighted in the respectable rating for maintainability, portability, and design.

The system also shows the accuracy of the Anomaly Detection System using machine learning. The Anomaly Detection System's capabilities and effectiveness in practical situations are demonstrated by the table that follows, which includes important performance metrics and discoveries. These metrics provide information on the correctness, dependability, and performance of the system through methodical testing and evaluation, underscoring its importance in improving security and operational effectiveness. It gained a total average of 75% based on the system’s performance.





```
Epoch 6/10
321/321 [==============================] - 52s 163ms/step - loss: 1.4246 - auc: 0.8019 - val_lo
ss: 1.7241 - val_auc: 0.7177
Epoch 7/10
321/321 [==============================] - 52s 162ms/step - loss: 1.3882 - auc: 0.8098 - val_lo
ss: 1.7053 - val_auc: 0.7276
Epoch 8/10
321/321 [==============================] - 52s 163ms/step - loss: 1.3444 - auc: 0.8203 - val_lo
ss: 1.6849 - val_auc: 0.7359
Epoch 9/10
321/321 [==============================] - 52s 163ms/step - loss: 1.3098 - auc: 0.8284 - val_lo
ss: 1.6556 - val_auc: 0.7436
Epoch 10/10
321/321 [==============================] - 52s 161ms/step - loss: 1.2763 - auc: 0.8363 - val_lo
ss: 1.6348 - val_auc: 0.7501
```

Figure 34. *Model Training Result using the Local Dataset Gathered by the Researchers*

Conclusion:

Based on the objectives of the study, several conclusions can be drawn regarding the functionality and efficiency of the developed system:

1. Design and implement a web application with an anomaly detection have been successfully deployed and created. The web application found to be effective and capable of assessing

the whole system configuration. The system provides a user-friendly interface and offering insights to enhance decision-making and monitoring procedures, improving operational security and efficiency. The system detects anomalies with an acceptable level of accuracy, establish a notification/alert mechanism to promptly inform Barangay officials about detected anomalies, create and implement a web application for live surveillance, develop a user-friendly interface tailored for the monitoring of multiple cameras, and implement a feature for generating comprehensive reports.

2. The system capabilities have been successfully assessed with the use of Python programming language as the primary development framework. hardware such as Digital Video Recorder (DVR), Closed-Circuit Television (CCTV), and Computer/Laptop. Vue.js framework for the user interface of the web application.
3. The study highlights the effectiveness and efficiency of the proposed system, which has undergone extensive evaluation and improvement based on factors such as accuracy, dependability, and usability. Through thorough examination, it has been demonstrated that the system meets the specified levels of accuracy, continuously giving dependable results.
4. The evaluation of the system using the ISO 25010 standard has proved it complies to established software quality attributes, validating its effective design. By methodically testing essential areas such as functionality, Performance, Usability, Efficiency, Maintainability, Portability, and Design, the system has shown to meet the demanding criteria set out by the ISO 25010 standard.

In conclusion, the advancement and effective execution of the inconsistency discovery speak to a critical improvement in the field of machine learning. The system's user-friendly interface had made it valuable in assessing the setup of the total framework, giving smart data to progress decision-making and checking forms, eventually expanding operational security and productivity. The framework shows solid capabilities in coordination different innovations with the offer assistance of the Vue.js system for the client interface and equipment like DVRs, PCs, and closed-circuit tv (CCTV) that are utilized in conjunction with the Python programming dialect as the fundamental advancement system. The framework appears an effective precision rate of 75%.

Recommendation

The recommendations for the system are the following:

- Choose high-quality hardware with real-time processing and enough storage capacity to handle a large amount of data for an efficient anomaly detection system.
- Develop an auto-captured face image system for incident identification. The system then employs advanced technology to explore the captured data.
- Use a hybrid algorithm for the detection system, also add different detection system such as weapon, object and face detection.
- For the user experience, the proposed option was to add a user-friendly option for reviewing videos and playback of recorded footage, accompanied by the existing built-in functions of the Digital-Videorecorder (DVRs).
- Integration of standalone systems such as: desktop and android applications are also needed for future research purposes so there is no conflict between the storage from the browser to the system.

REFERENCES

Alajrami, E., Tabash, H., Singer, Y., & Astal, M.-T. (2019). *). On using AI-Based Human Identification in Improving Surveillance System Efficiency*. Retrieved from IEEE Explore: https://doi.org/10.1109/ICPET.2019.00024

Alsubayhin, A., Ramzan, M., & Alzahrani, B. (2023). *Crime Prediction Using Machine Learning: A Comparative Analysis*. Retrieved from Journal of Computer Science: https://doi.org/10.3844/jcssp.2023.1170.1179

Arora, S., Bhatia , K., & Amit. (n.d.). *Storage optimization of video surveillance from CCTV camera*. Retrieved from 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2016, pp. 710-713: https://doi.org/10.1109/NGCT.2016.78775

Ashby, M. P. (2017). *The Value of CCTV Surveillance Cameras as an Investigative Tool: an Empirical Analysis*. Retrieved from European Journal on Criminal Policy and Research: https://doi.org/10.1007/s10610-017-9341-6

Asor, J. R. (2020, June 25). *Implementation of Predictive Crime Analytics in Municipal Crime Management System in Calauan, Laguna, Philippines*. Retrieved from International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3), 150–157: https://doi.org/10.30534/ijatcse/2020/2291.32020

Basimanyane, D., & Gandhi, D. (2019). *STRIKING A BALANCE BETWEEN CCTV SURVEILLANCE AND THE DIGITAL RIGHT TO PRIVACY IN SOUTH AFRICA CONSIDERATIONS FOR THE INFORMATION REGULATOR*. Retrieved from https://apcof.org/wp-content/uploads/027-cctvsurveillanceanddigital-dorcasbasimanyanedumisanigandhi-1.pdf.

Bhatti, M. T., Khan, M., Aslam, M., & Fiaz, M. (2021). *Weapon Detection in Real-Time CCTV Videos Using Deep Learning*. Retrieved from IEEE Access, 9, 34366–34382. : https://doi.org/10.1109/access.2021.3059170

Chackravarthy, S., Schmitt, S., & Yang, L. (2018, October 1). *Intelligent Crime Anomaly Detection in Smart Cities Using Deep Learning*. Retrieved from IEEE Xplore: https://doi.org/10.1109/CIC.2018.00060

Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly Detection: A Survey*. Retrieved from ACM Computing Surveys, 41(3), 1–58: https://doi.org/10.1145/1541880.1541882

CRIMINAL DETECTION AND RECOGNITION USING ML. (2023, February 2). Retrieved from International Research Journal of Modernization in Engineering Technology and Science: https://doi.org/10.56726/irjmets33263

Dakalbab, F., Abu Talib, M., Abu Warga, O., & Bou Nassif, A. (2022). *Artificial intelligence & crime prediction: A systematic literature review*. Retrieved from Social Sciences & Humanities Open, 6(1), 100342: https://doi.org/10.1016/j.ssaho.2022.100342

DATA, C. A. (2020, September 28). *Crime Analysis and DATA*. Retrieved from IEEEConference Publication: https://ieeexplore.ieee.org/abstract/document/9245120

F. (n.d.).

Fabbri, M., & Klick, J. (2021, March). *The Ineffectiveness of 'Observe and Report' Patrols on Crime*. Retrieved from International Review of Law and Economics, 65, 105972: https://doi.org/10.1016/j.irle.2020.105972

Falangon, R. (2022). *Utilization of CCTV Cameras in Bontoc, Mountain Province*. Retrieved from https://www.journalppw.com/index.php/jpsp/article/download/3512/2290/4000.

Fuentes, L., & Velastin, S. (2004). *Tracking-based event detection for CCTV systems*. Retrieved from Pattern Anal Applic 7, 356–364: https://doi.org/10.1007/s10044-004-0236-z

Ganiyu, A. A., Olaniyan, O. S., Taye, A. V., Oyedele, O. J., Adetiran, A. A., Joseph, A. O., . . . Osinubi, O. A. (2020). *Design and Implementation of An Improved Digital Video Surveillance System. Computer Engineering And Intelligent Systems*. Retrieved from https://core.ac.uk/download/pdf/327151648.pdf

Garg, R., & Verma, G. (2016). *Multi-algorithms based visual surveillance system for human detection*. Retrieved from 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 1155-1160: https://doi.org/ 10.1109/CCAA.2016.7813891

Glowacz, A., Kmieć, M., & Dziech, A. (2013). *Visual detection of knives in security applications using Active Appearance Models*. Retrieved from Multimedia Tools and Applications, 74(12), 4253–4267: https://doi.org/10.1007/s11042-013-1537-2

Gorr, W., & Harries, R. (2003, October). *Introduction to crime forecasting. International Journal of Forecasting, 19(4), 551–555. https://doi.org/10.1016/s0169-2070(03)00089-x*. Retrieved from International Journal of Forecasting, 19(4), 551–555: https://doi.org/10.1016/s0169-2070(03)00089-x

Grega, M., Matiolański, A., Guzik, P., & Leszczuk, M. (2016). *Automated Detection of Firearms and Knives in a CCTV Image*. Retrieved from Sensors, 16(1), 47. : https://doi.org/10.3390/s16010047

Hollis-Peel, M. E., Reynald, D., Van Bavel, M., Elffers, H., & Wels. (2011, May 26). *Guardianship for crime prevention: a critical review of the literature*. Retrieved from Crime, Law and Social Change, 56(1), 53–70: https://doi.org/10.1007/s10611-011-9309-2

Kipāne, A., & Vilks, A. (2023, October). *Crime Forecasting in the Digital Age: A Theoretical Framework. SOCRATES*. Retrieved from University Faculty of Law Electronic Scientific Journal of Law, 2(26), 1–9: https://doi.org/10.25143/socr.26.2023.2.01-09

Kooij, J., Liem, M., Krijnders, J., Andringa, T., & Gavrila. (2016, March). *Multi-Modal Human Aggression Detection*. Retrieved from Computer Vision and Image Understanding, 144, 106–120: https://doi.org/10.1016/j.cviu.2015.06.009

Luu, P. V., Weed,, J., & Rodriguez, S. (2019). *Akhtar an AI-based web surveillance system using Raspberry Pi.* Retrieved from Journal of Advances in Technology and Engineering Research, 5(6).: https://doi.org/10.20474/jater-5.6.2

Matczak, P., Wójtowicz, A., Dąbrowski, A., Leitner, M., & Sypi. (2021, September 20). *Effectiveness of CCTV Systems as a Crime Preventive Tool: Evidence from Eight Polish Cities.*

McClendon, L., & Meghanathan, N. (2015, March 31). *Using Machine Learning Algorithms to Analyze Crime Data.* Retrieved from Machine Learning and Applications: An International Journal, 2(1), 1–12.: https://doi.org/10.5121/mlaij.2015.2101

NVR vs DVR: what's the difference and which is better? . (n.d.). Retrieved from https://www.calipsa.io/blog/nvr-vs-dvr-whats-the-difference-and-which-is-better.

Palanivinayagam, A., Gopal, S., Bhattacharya, S., Anumbe, N., & Ibeke. (2021, November 13). *An Optimized Machine Learning and Big Data Approach to Crime Detection.* . Retrieved from Wireless Communications and Mobile Computing, 2021, 1–10. : https://doi.org/10.1155/2021/5291528

Perlman, A. (2019). *The Growing Role of Machine Learning in Cybersecurity.* Retrieved from Security Roundtable:: https://www.securityroundtable.org/the-growing-role-of-machine-learning-in-cybersecurity/

PSA. (2023). *Third Quarter 2023 PSGC Updates: Conversion to a New City, Merging of 44 Barangays, Renaming of Five Barangays, Transferring of 10 Barangays, and Correction of the Names of 12 Barangays*. Retrieved from PSA: https://psa.gov.ph/classification/psgc

Quiroz-Vázquez, C. (2019, December). *Anomaly Detection in Machine Learning: Finding Outliers for Optimization of Business Functions*. Retrieved from IBM Blog: https://www.ibm.com/blog/anomaly-detection-machine-learning/

Saeed, U., Sarim, M., Usmani, A., Mukhtar, A., & Shaikh, A. (2015). *Application of Machine learning Algorithms in Crime Classification and Classification Rule Mining*. Retrieved from Research Journal of Recent Sciences, 4, 106–114: http://www.isca.me/rjrs/archive/v4/i3/15.ISCA-RJRS-2013-1005.pdf

Sathyadevan, S., Balakrishnan, A., Arya , S., & Athira Raghunat, S. (2014). *Identifying Moving Bodies from CCTV Videos Using Machine Learning Techniques*. Retrieved from 2014 First International Conference on Networks & Soft Computing (ICNSC2014), Guntur, India, pp. 151-157: https://doi.org/ 10.1109/CNSC.2014

Seydx. (2023). *camera.ui: NVR like user Interface for RTSP capable cameras with live streams, motion detection, image recognition and more*. Retrieved from Github: https://github.com/seydx/camera.ui

Shah, N., Bhagat, N., & Shah, M. (2021). *Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention*. Retrieved from Visual Computing for Industry, Biomedicine, and Art, 4(1).: https://doi.org/10.1186/s42492-021-00075-z

Shirsat, S., Naik, A., Tamse, D., Yadav, J., & Shetgaonkar, P. (2019, March). *Proposed System for Criminal Detection and Recognition on CCTV Data Using Cloud and Machine Learning*. Retrieved from International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). : https://doi.org/10.1109/vitecon.2019.8899441

Statista. (2023, December 19). *Global surveillance technology market size 2022-2027*. . Retrieved from https://www.statista.com/statistics/1251839/surveillance-technology-market-global/.

Tsakanikas, V., & Dagiuklas, T. (2018). *Video surveillance systems-current status and future trends.* Retrieved from Computers & Electrical Engineering, 70, 736–753.: https://doi.org/10.1016/j.compeleceng.2017.11.011

Ullah, R., Ullah, R., Hayat, H., Siddiqui, A., & Siddiqui, U. (2022). *A Real-Time framework for human face detection and recognition in CCTV images*. Retrieved from Mathematical Problems in Engineering, 2022, 1–12. : https://doi.org/10.1155/2022/3276704

Valcheva, S. (2022, November 7). *Data Flow Diagram: Examples (Context & Level 1), Explanation, Tutorial.* . Retrieved from Blog for Data-Driven Business : https://www.intellspot.com/data-flow-diagram-examples/

Vineet Pande, V. S. (2016, February 2). *Crime Detection using Data Mining*. Retrieved from International Journal of Engineering Research And, V5(01).: https://doi.org/10.17577/ijertv5is010610

Welsh, B. C., & Farrington, D. (2004, April). *Evidence-based Crime Prevention: The Effectiveness of CCTV*. Retrieved from Crime Prevention and Community Safety, 6(2), 21–33.: https://doi.org/10.1057/palgrave.cpcs.8140184

What are video surveillance systems and how do they work? (2024, March 3). Retrieved from Mammoth Security Inc.: https://mammothsecurity.com/blog/how-video-surveillance-systems-work

APPENDICES

APPENDIX A

EVALUATION SHEET

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES
Ayala Blvd, Ermita, Manila
COLLEGE OF SCIENCE

RESPOGUARD: DEVELOPMENT OF AN ANOMALY DETECTION SYSTEM FOR REAL-TIME SURVEILLANCE IN BARANGAY 294 BINONDO MANILA USING MACHINE LEARNING

EVALUATION SHEET

Name (optional): ______________________ **Position: ________________________**
Date: ________________________________

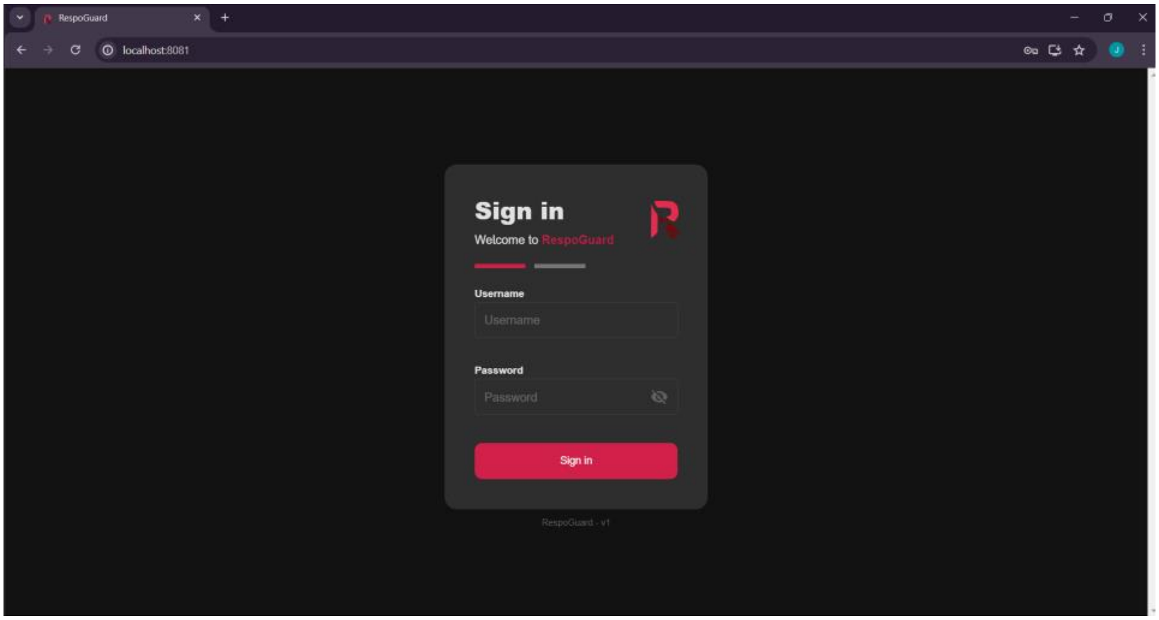
Instruction: Using the provided scale, rate the system and place a checkmark next to the corresponding number rating.

Numerical Rating	**Equivalent**
4	Highly Acceptable
3	Very Acceptable
2	Acceptable
1	Not Acceptable

Characteristics	**Rating**			
A. Functionality	**4**	**3**	**2**	**1**
1.1 Functions are required for the systems to be implemented				
1.2 The system input and output are accurate				
1.3 The system modules are working and connected properly				
1.4 There is a substantial system security				
B. Performance/Usability/Efficiency				
2.1 The system is error free (syntax, logic, runt-time error)				
2.2 Easy to operate and remember				
2.3 Allows effective use of system resources				
C. Maintainability/Portability/Design				
3.1 The system is easy to expand and modify to adapt to new changes				
3.2 The system can run in different environments				
3.3 The system Graphical User Interface design used was clear, neat, and visible enough to be seen by the user.				

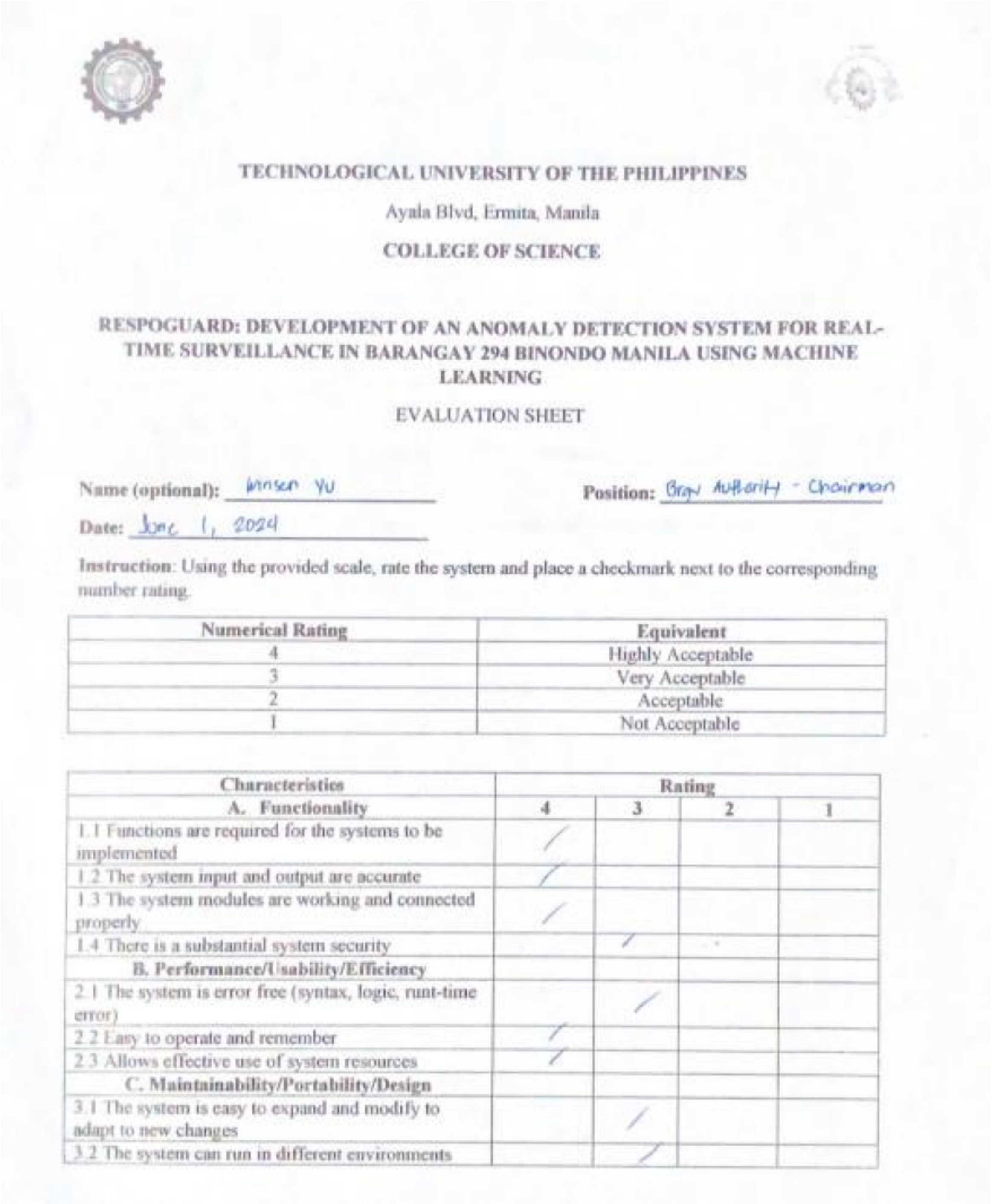
APPENDIX B

RESPOGUARD’S WEB APPLICATION



APPENDIX C

SAMPLE ANSWERED EVALUATION FORM



TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES

Ayala Blvd, Ermita, Manila

COLLEGE OF SCIENCE

RESPOGUARD: DEVELOPMENT OF AN ANOMALY DETECTION SYSTEM FOR REAL-TIME SURVEILLANCE IN BARANGAY 294 BINONDO MANILA USING MACHINE LEARNING

EVALUATION SHEET

Name (optional): Winsen Yu **Position:** Brgy Authority - Chairman

Date: June 1, 2024

Instruction: Using the provided scale, rate the system and place a checkmark next to the corresponding number rating.

Numerical Rating	Equivalent
4	Highly Acceptable
3	Very Acceptable
2	Acceptable
1	Not Acceptable

Characteristics	Rating			
A. Functionality	**4**	**3**	**2**	**1**
1.1 Functions are required for the systems to be implemented	✓			
1.2 The system input and output are accurate	✓			
1.3 The system modules are working and connected properly	✓			
1.4 There is a substantial system security		✓		
B. Performance/Usability/Efficiency				
2.1 The system is error free (syntax, logic, runt-time error)		✓		
2.2 Easy to operate and remember	✓			
2.3 Allows effective use of system resources	✓			
C. Maintainability/Portability/Design				
3.1 The system is easy to expand and modify to adapt to new changes		✓		
3.2 The system can run in different environments		✓		

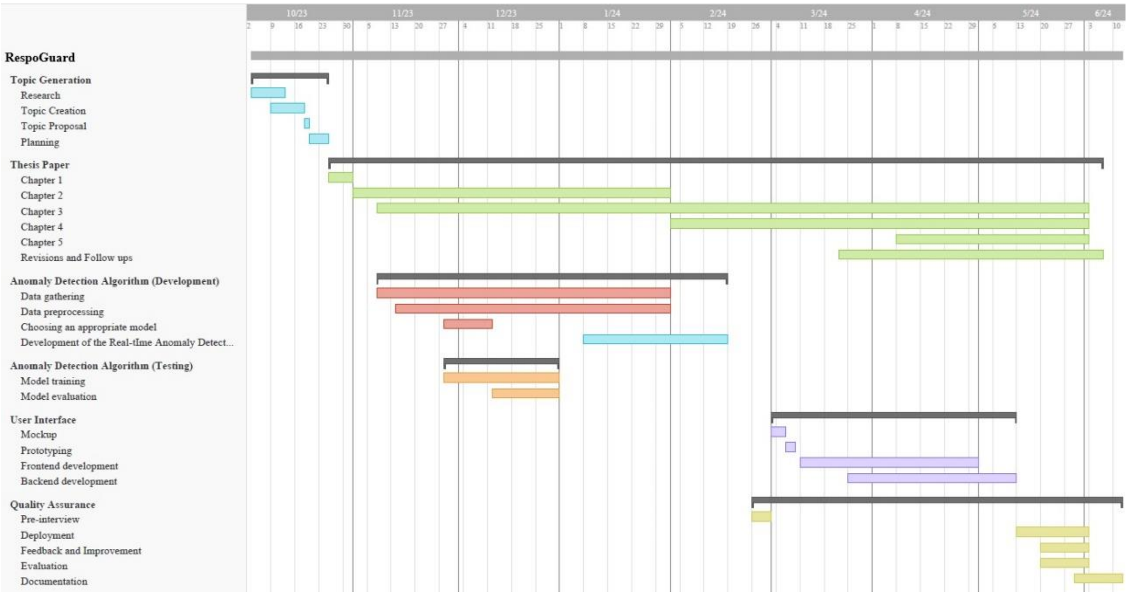
APPENDIX D

SUMMARY OF RESPONDENTS' EVALUATION

Criteria	**Scale**	
	Overall Weighted Mean	Descriptive Rating
Functionality		
Functions that are required for the systems are implemented	3.83	Highly Acceptable
The system input and output are accurate	3.77	Highly Acceptable
The system modules are working and connected properly	3.8	Highly Acceptable
There is a substantial system security	3.63	Highly Acceptable
Performance, Usability, and Efficiency		Highly Acceptable
The system is error free (syntax, logic, run-time)	3.37	Highly Acceptable
Easy to operate and remember	3.57	Highly Acceptable
Allows effective use of system resources	3.8	Highly Acceptable
Maintainability/Portability/Design		Highly Acceptable
The system is easy to expand and modify to adapt to new changes	3.4	Highly Acceptable
The system can run in different environments	3.5	Highly Acceptable
The system Graphical User Interface design used was clear, neat, and visible enough to be seen by the user	4	Highly Acceptable
Grand Weighted Mean	**3.67**	**Highly Acceptable**

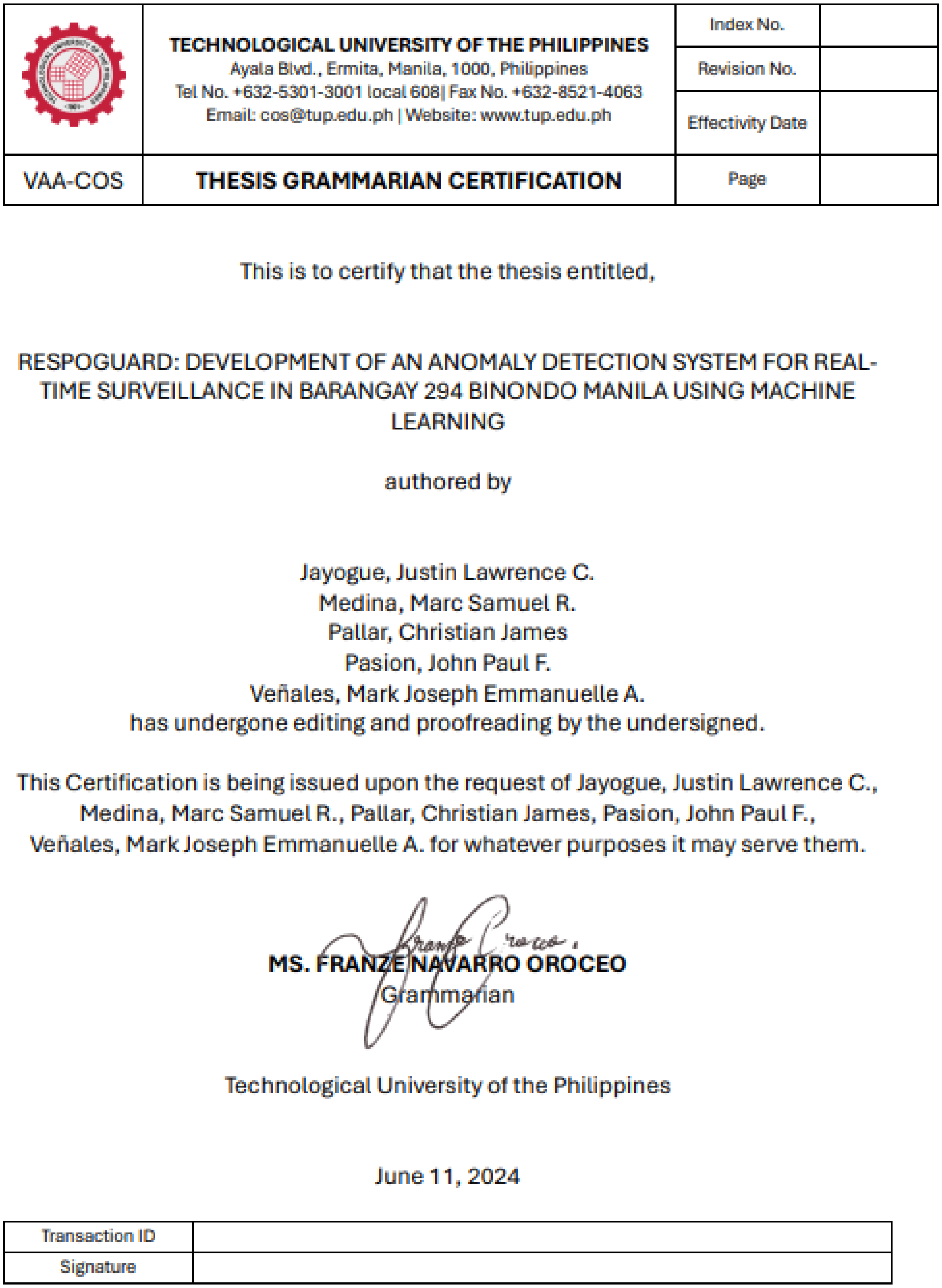
APPENDIX E

GANTT CHART



APPENDIX F

THESIS GRAMMARIAN CERTIFICATION



	TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES Ayala Blvd., Ermita, Manila, 1000, Philippines Tel No. +632-5301-3001 local 608| Fax No. +632-8521-4063 Email: cos@tup.edu.ph | Website: www.tup.edu.ph	Index No.	
		Revision No.	
		Effectivity Date	
VAA-COS	**THESIS GRAMMARIAN CERTIFICATION**	Page	

This is to certify that the thesis entitled,

RESPOGUARD: DEVELOPMENT OF AN ANOMALY DETECTION SYSTEM FOR REAL-TIME SURVEILLANCE IN BARANGAY 294 BINONDO MANILA USING MACHINE LEARNING

authored by

Jayogue, Justin Lawrence C.
Medina, Marc Samuel R.
Pallar, Christian James
Pasion, John Paul F.
Veñales, Mark Joseph Emmanuelle A.
has undergone editing and proofreading by the undersigned.

This Certification is being issued upon the request of Jayogue, Justin Lawrence C., Medina, Marc Samuel R., Pallar, Christian James, Pasion, John Paul F., Veñales, Mark Joseph Emmanuelle A. for whatever purposes it may serve them.

MS. FRANZE NAVARRO OROCEO
Grammarian

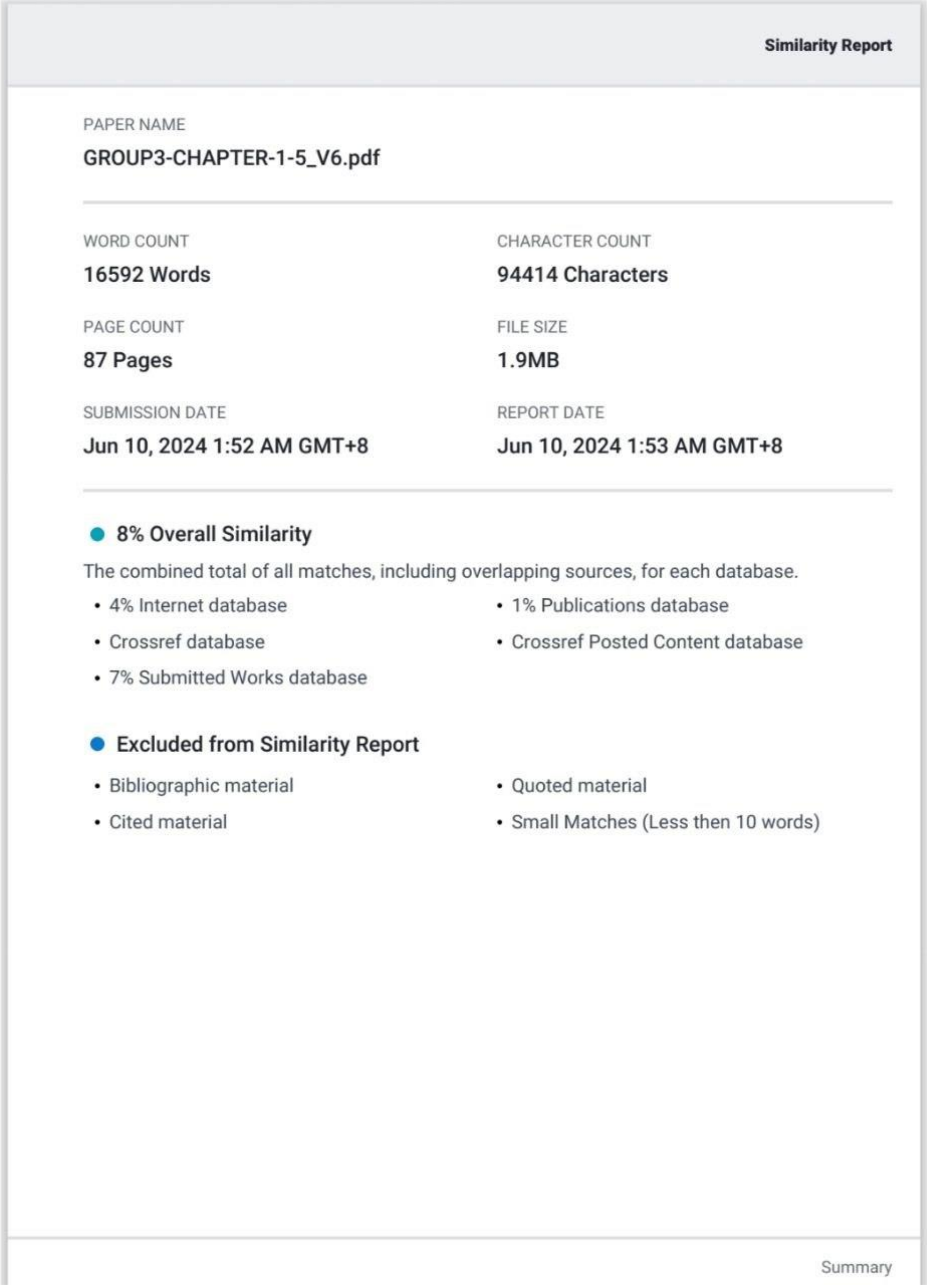
Technological University of the Philippines

June 11, 2024

Transaction ID	
Signature	

APPENDIX G

CERTIFICATION OF SIMILARITY INDEX USING TURNITIN



Similarity Report

PAPER NAME

GROUP3-CHAPTER-1-5_V6.pdf

WORD COUNT 16592 Words	CHARACTER COUNT 94414 Characters
PAGE COUNT 87 Pages	FILE SIZE 1.9MB
SUBMISSION DATE Jun 10, 2024 1:52 AM GMT+8	REPORT DATE Jun 10, 2024 1:53 AM GMT+8

● **8% Overall Similarity**

The combined total of all matches, including overlapping sources, for each database.

- 4% Internet database
- Crossref database
- 7% Submitted Works database
- 1% Publications database
- Crossref Posted Content database

● **Excluded from Similarity Report**

- Bibliographic material
- Cited material
- Quoted material
- Small Matches (Less then 10 words)

Summary

APPENDIX H

CERTIFICATION OF SIMILARITY INDEX USING TURNITIN FROM URDS

RESEARCHER'S PROFILE

JUSTIN LAWRENCE C. JAYOGUE

QUEZON CITY | 09670233858 | justinelawrence.jayogue@tup.edu.ph

OBJECTIVES

My primary goal is to become a Web – Developer while simultaneously broadening my understanding of diverse frameworks and acquiring further expertise in the field of technology.

SKILL HIGHLIGHTS

- Knowledgeable in python
- Knowledgeable in web development such as HTML and CSS
- Familiar with C and C++
- Knowledgeable in multimedia using windows software

EDUCATION

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES	ERMITA MANILA
BACHELOR OF SCIENCE IN COMPUTER SCIENCE	2020-2024
OUR LADY OF FATIMA UNIVERSITY	LAGRO QUEZON CITY
SCIENCE TECHNOLOGY ENGINEERING AND MATHEMATICS	2018-2020

EXPERIENCE

Full – stack web developer, IT - Tech

TRACE ALARM AND SECURITY SYSTEM INC. Poblacion, Makati

- Created a responsive and dynamic website written in HTML, CSS and PHP back end.
- Troubleshooting and resolving issues with the security system
- Maintaining client's security system by testing and checking the devices.

SEMINARS AND CERTIFICATIONS

Modern Data Center Infrastructure (In Accordance with Global Standards)

- December 2022
- Department of College of Science
- Technological University of the Philippines

MARC SAMUEL R. MEDINA

MANILA | 09456-871-385 | marcsamuelmedina@tup.edu.ph

OBJECTIVES

To Utilize programming skills to optimize system efficiency, troubleshoot issues, and implement solutions that ensure seamless operations. Demonstrate adaptability, creativity, and a passion for lifelong learning.

SKILLS

- Knowledgeable in C, C++ and in Java
- Knowledgeable in web development (HTML, CSS, JavaScript)
- Familiar with game development (Android Studio) and software development (SQL, Firebase)

EDUCATION

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES	ERMITA MANILA
BACHELOR OF SCIENCE IN COMPUTER SCIENCE	2020-2024

EXPERIENCE

Full – stack web developer, IT - Tech

TRACE ALARM AND SECURITY SYSTEM INC. Poblacion, Makati

- Created a responsive and dynamic website written in HTML, CSS and PHP back end.
- Troubleshooting and resolving issues with the security system
- Maintaining client's security system by testing and checking the devices

SEMINARS AND CERTIFICATIONS

Modern Data Center Infrastructure (In Accordance with Global Standards)

- December 2022
- Department of College of Science
- Technological University of the Philippines

CHRISTIAN JAMES PALLAR

PARAÑAQUE | 09286621017 | christianjames.pallar@tup.edu.ph

OBJECTIVES

To develop and implement data-driven solutions to optimize business processes, improve decision-making, and drive strategic growth.

SKILLS

- Knowledgeable in C, C++, Java, Python
- Knowledgeable in Web Development (HTML, CSS)
- Proficient in MS Word, Basic Graphic Design

EDUCATION

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES	ERMITA MANILA
BACHELOR OF SCIENCE IN COMPUTER SCIENCE	2020-2024
OLIVAREZ COLLEGE	PARAÑAQUE CITY
SCIENCE TECHNOLOGY ENGINEERING AND MATHEMATICS	2018-2020

EXPERIENCE

Full – stack web developer, IT - Tech

TRACE ALARM AND SECURITY SYSTEM INC. Poblacion, Makati

- Created a responsive and dynamic website written in HTML, CSS and PHP back end.
- Troubleshooting and resolving issues with the security system
- Maintaining client's security system by testing and checking the devices.

SEMINARS AND CERTIFICATIONS

Modern Data Center Infrastructure (In Accordance with Global Standards)

- December 2022
- Department of College of Science
- Technological University of the Philippines

JOHN PAUL F. PASION

QUEZON CITY | 0966-417-3227 | johnpaul.pasion@tup.edu.ph

OBJECTIVES

To leverage my expertise in machine learning, data analysis, and software development to create innovative solutions that drive business growth and efficiency.

SKILLS

- Knowledgeable in some programming languages such as Assembly, C, C++, Java, Python
- Knowledgeable in Web development (HTML, CSS, JavaScript, jQuery, Node.js, React, Flask, Bootstrap, Tailwind, MongoDB, Express), Game Development (C#), Software Development (C#, SQL)
- Proficiency in software development tools and IDEs such as Git, Visual Studio, Visual Studio Code, Atom, Microsoft SQL Server, Unity Engine

EDUCATION

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES	ERMITA MANILA
BACHELOR OF SCIENCE IN COMPUTER SCIENCE	2020-2024
DR. CARLOS S. LANTING COLLEGE	NOVALICHES QUEZON CITY
SCIENCE TECHNOLOGY ENGINEERING AND MATHEMATICS	2018-2020

EXPERIENCE

Full – stack web developer, IT - Tech

TRACE ALARM AND SECURITY SYSTEM INC. Poblacion, Makati

- Created a responsive and dynamic website written in HTML, CSS and PHP back end.
- Troubleshooting and resolving issues with the security system
- Maintaining client's security system by testing and checking the devices

SEMINARS AND CERTIFICATIONS

Full-Stack Web Development with React Specialization

- November 2022
- Coursera (The Hong Kong University of Science and Technology)

MARK JOSEPH EMMANUELLE A. VEÑALES

MANILA | 09266863024 | markjosephemmanuelle.venales@tup.edu.ph

OBJECTIVES

To design and implement secure and scalable network architectures and apply knowledge of network protocols, security measures, and infrastructure design to develop robust and secure network systems

SKILLS

- Knowledgeable in multi-media editing using Microsoft Windows Programs
- Hardware and software
  Trouble shooting/Maintenance
- Canva
- Web design

EDUCATION

TECHNOLOGICAL UNIVERSITY OF THE PHILIPPINES	ERMITA MANILA
BACHELOR OF SCIENCE IN COMPUTER SCIENCE	2020-2024
NU – NAZARETH	SAMPALOC MANILA
SCIENCE TECHNOLOGY ENGINEERING AND MATHEMATICS	2018-2020

EXPERIENCE

Full – stack web developer, IT - Tech

TRACE ALARM AND SECURITY SYSTEM INC. Poblacion, Makati

- Created a responsive and dynamic website written in HTML, CSS and PHP back end.
- Troubleshooting and resolving issues with the security system
- Maintaining client's security system by testing and checking the devices.

SEMINARS AND CERTIFICATIONS

Modern Data Center Infrastructure (In Accordance with Global Standards)
December 2022
Department of College of Science
Technological University of the Philippines