ANOMALY DETECTION IN VIDEO SURVEILLANCE

Final Year Project Report

By

Capt Zohair Shahid

Capt Muhammad Ibtisam Naseer

Capt Muhammad Hamza Javed

Capt Muhammad Imran

Supervisor:

Lt. Col Khawir Mehmood

In Partial Fulfillment
Of the Requirements for the degree
Bachelors of Engineering in Software Engineering (BESE)

Department of Computer Software Engineering
Military College of Signals
National University of Science and Technology
Islamabad, Pakistan
(June 2023)

In the name of ALLAH, the Most Benevolent, the Most Courteous

DECLARATION

We hereby declare that this project report entitled “Anomaly Detection in Video Surveillance” submitted to the “Computer Science Department”, is a record of an original work done by us under the guidance of Supervisor “Lt Col Khawir Mehmood” and that no part has been plagiarized without citations. Also, this project work is submitted in the partial fulfillment of the requirements for the degree of Bachelor of Computer Science.

Team Members	**Signature**
Capt Zohair Shahid	________________________
Capt Muhammad Hamza Javed	________________________
Capt Muhammad Ibtisam Naseer	________________________
Capt Muhammad Imran	________________________

Supervisor	**Signature**
Lt Col Khawir Mehmood	________________________

Date:

____

Place:

____

ACKNOWLEDGEMENTS

Allah Subhan'Wa'Tala is the sole guidance in all domains.

Our parents, colleagues, and most of all supervisor **Lt Col Khawir Mehmood** without whose guidance this project would not have succeeded.

The group members, who through all adversities worked steadfastly.

Table of Contents

List Of Figures

ABSTRACT

In this project, we have developed an anomaly detection system which makes use of Machine Learning to detect anomalies to include Violence, Theft, Accident, Arson, and Abuse. This would be accomplished by using deep neural networks. The approach adopted to fulfill the requirement is Multiple Instance Learning approach that considers normal and anomalous videos as bags and video segments to be the instances. Thus automatically learning an anomaly model to predict high score for anomalous video segments. The training datasets consist of a variety of videos containing normal and anomalous (Explosion, Shooting, Road accident and ten other anomalies) of approximately 128 hours containing 1800 real world surveillance videos. After the training phase, Model is then deployed using interface which takes the video as an input and displays results as graph. The Summary of anomaly detected further displayed in a GUI containing anomalous frame, threshold, mean and standard deviation. In addition to this the system has access control mechanism in the form of login and maintaining logs. The system is also used for trend analysis that will help security personnel to enhance security on ground. Hence the system provides management solution for video surveillance.

Chapter 1

1. INTRODUCTION

1.1 Background

Public areas have been found to improve public safety by employing physical security with manpower. Surveillance cameras are dovetailed with physical security for enhanced security. However, the it is beyond the capability of security individual to continuously monitor the anomalous behaviors occurring in the environ. Thus resulting in a marginal deficiency in detecting the anomalies in environment. Detecting anomalous events, such as traffic accidents, crimes, or illegal activities, is a critical task in video surveillance. Anomalous events are infrequent compared to normal activities, leading to inefficiencies in labor and time utilization. So, it is vital to develop smart algorithms to address this issue.

1.2 Purpose

The objective of a video anomaly detection management system is to quickly detect activities that diverge from normal behaviors. The system must also ascertain the time for which abnormal event has occurred. Consequently, abnormality detection can be viewed as a system that differentiates the normal video behavior from abnormal ones. After the detection of event, it can be classified as normal or abnormal event.

1.3 Scope

Surveillance cameras have become a necessity in any organization or vicinity sensitive to security, they have proven to be highly useful in the domain of security. However, constant monitoring of the real time surveillance videos to detect any sensitive situation needs manpower resources and is tiresome and hectic if done over a long period of time. With the advancements in technology such systems can be automated by use of machine learning. Anomaly Detection in Video Surveillance System aims to achieve this with maximum accuracy. In this system we’ll be automating the surveillance system for different set of anomalies using computer vision algorithms to notify in case of a set of predefined possible anomalies such as fighting, accidents, robbery, burglary etc. The system will initially detect anomalies on offline set of videos, later this system will perform detection on live video feed. ADVS will be able to catch these anomalies, notify users, ring alarms if necessary and ensure maximum automation of the surveillance systems. This technology provides great advantages for dealing with unexpected situations, and it can even anticipate and prevent these events from occurring. This is particularly important for ensuring public safety.

Chapter 2

2. LITERATURE OVERVIEW

2.1 Existing solutions and their drawbacks

2.1.1 Lu et el Approach

Lu and colleagues came up with an innovative method for recognizing and learning what normal behaviors look like, and then using this knowledge to detect unusual events. The process involves analyzing thousands of cuboids (small three-dimensional shapes approximately 7000) in normal video footage, and calculating gradient-based features for each one. The team then reduced the dimensionality of the data, and used a sparse representation technique to build a dictionary that describes normal behaviors. When tested, the model accurately identified anomalies with a success rate of 65%. This dictionary-based approach is a promising way to improve anomaly detection and could be applied in various fields to enhance security and safety.

2.1.2 Hasan et al Approach

Hasan and colleagues introduced a new technique for identifying local features and classification using a fully convolutional feed forward deep auto-encoder. In this approach, the network was trained on normal videos by analyzing a 40-frame temporal window. Reconstruction error was then used to identify any anomalies. When tested, the accuracy of the model was found to be 50%. This innovative approach could be useful in various applications where detecting anomalies is crucial, such as security systems or medical diagnosis.

2.1.3 Binary Classifier

Binarized Neural Network is a category of neural network that uses binary values (-1 and 1) for anomalous and normal videos instead of continuous values for weights and activations. Although the algorithm is fast but its accuracy on such huge dataset was only up to 50%.

2.1.4 Convolution Neural Network (CNN)

In anomalous behaviour detection, Convolutional Neural Network (CNN or ConvNet). This network has multi layer perceptron which refers to a Fully Connected Network (FCN) in which all neurons of one layer are connected to other neurons in the next layer.

2.1.5 Mask RCNN

RCNN structure designed and assembled to solve instant segmentation problems in various image and video applications. It is capable to separate various objects in video or image.It generates region proposals based on objects in an image and capable to predict the various class of objects by markers in pixel level. This acts as a backbone for Feature Pyramids Networks (FPN) to detect objects at different scales.

2.1.6 Semantic Segmentation

Understanding a video at minute level i.e frame by frame is a core computer vision constrains which is prominent in increasing number of applications. Some of those applications are automatic driving cars, human and computer interaction with each other, virtual reality. With many semantic segmentation changes problems are solved using convolutional neural networks that have produced promising results outmatching other approaches with regards to efficiency and accuracy.

2.1.7 Anomaly detection

In this approach then frames are extracted at 20 fps and then features are extracted from a video. The video frame is divided into foreground and background region. The methodology does not changes background region information, while the foreground region contains moving objects. Features of both regions are extracted. and given as input to mask – RCNN. Faster R-CNN (mask RCNN) has three outputs produced for each different object, one is a class label, second is a bounding-box and third output is an object mask. Hence due to this approach the extraction of information is much finer in order to construct a spatial layout of the object. The Pattern detection phase used in this model to identify patterns in the video sequence. The system can also be programmed to take some decisions upon pattern detection.

Some of the assumptions and constraints made during implementation are:

a. The object brightness must always remain constant.

b. The source of video is stationary..

c. Video should be in RBG frame structure.

d. Nearby objects must have smooth change in velocity.

e. This camera feed must be given input to computer.

2.1.8 VGG 16

VGG16 is a Convolutional Neural Network model proposed by K. Simonyan and A. Zis-serman from the University of Oxford in the paper "Very Deep Convolutional Networks for Large-Scale Image Recognition". The model has 92.7% accuracy in ImageNet, which contains over 14 million images belonging to 1000 classes. It has three fully connected layers along with thirteen convolution. Every hidden layer has ReLU activation fucntion applied inside and a 3x3 size of kernel is set. These layers are further divided into five blocks. There are two layers on first block whereas it has 64 channels. Block 2 contains a total of 128 channels. Block 3 contains 512 channels and three convolutional layers, and. The final two blocks comprise of 3 convolutional layers with 512 channels inside. Max-pooling layer of 2x2 is applied after each block. Afterwards, after every fifth block 3 fully connected layers are applied. The first two has 4096 channels each. Finally, VG 16 results prove that the efficiency of a CNN is affected by its depth.

2.1.9 Dense Convolutional Neural Network (DenseNet)

This model employs dense connections between layers and it is a variant of Convolutional Neural Network . DenseNet is centering on the features extracted. In orthodox CNNs, every layer is connect to the next layer. For example, in the VGG16, the 1st convolutional layer can not be connected to the 8th layer or 12th layer. As the input data increases, there is a problem called the disappearing gradient that can affect the overall performance of a model. In the DenseNet structure, multiple dense blocks are used, each containing several convolutional layers. Unlike VGG16, the layers within a dense block are closely connected to each other. This means that each layer in a block receives input from all the preceding layers. This arrangement strengthens the relationship between different layers in the DenseNet.

The advantage of this model is that it requires fewer input features compared to other models, which makes the network slimmer and more compact. Additionally, the enhanced layer-to-layer connection allows more information to be gathered within a dense block, resulting in a stable training process with fewer parameters and input features.

In DenseNet, every layer directly accesses the gradients from the loss function and the original input signal, which provides implicit deep supervision.

2.1.10 Recurrent Neural Network (RNN)

Recurrent Neural Networks (RNNs) are commonly used for tasks involving sequential or time-series data like NLP and video processing. RNNs differ from traditional networks due to their memory capability, allowing them to influence current outputs based on previous inputs. This is achieved through hidden states that store past information and recurrent connections that pass this information between time steps. Unfolding the RNN through time enables it to consider the impact of previous inputs on the current output, making RNNs effective for processing sequential data.

2.1.11 Long Short-term Memory (LSTM)

Recurrent Neural Networks (RNNs) struggle with long sequential data due to the problems of gradient disappearance and explosion. To overcome this, Long Short-term Memory (LSTM) was introduced as an improved version of RNNs. LSTM incorporates a cell state (Ct) along with the hidden state to address the issue. It uses gates to decide what information to keep, update, or output, allowing it to handle inputs and hidden states for sequences of any length. This solves the limitations of traditional RNNs and enables LSTM to effectively process long sequences. By incorporating LSTM, the problems of gradient vanishing and exploding can be mitigated in handling sequential data.

2.1.12 Two-stream Based Model

The two-stream model is an alternative to RNNs and LSTM for extracting temporal features. It uses optical flow to capture motion information. The spatial stream processes randomly sampled video frames using a simple CNN. The temporal stream utilizes optical flow displacement fields as input and employs a ConvNet structure. Both streams contribute Softmax scores for fusion. This approach combines spatial and temporal information to make predictions or decisions.

Chapter 3

3. PROBLEM DEFINITION

Surveillance cameras are becoming vital in modern day scenario because of the overwhelmingly heinous nature of crimes and terrorist's activities being committed on day-to-day basis. Keeping pace with monitoring of these cameras and making utilization to the full extent has unfortunately not been possible. This has led to an increase in crimes and confidence gaining of these criminals and terrorists. Another aspect of these cameras is there is a huge ratio deficit between cameras and human monitoring operators. Therefore, it is not humanly possible to monitor all of them with accuracy and efficiency. There is also an element of human error which reduces the already insufficient efficiency of human monitoring operators. Hence, a software system is required that can intelligently detect and categorize the threat type in a video feed and aid the security agencies to take appropriate steps avoid further damage to lives, property and environment.

Chapter 4

4. METHODOLOGY

4.1 Multi Instance Learning Approach (MIL)

This technique only uses labeled videos which specify the existence of an anomalous behavior in a video. An anomalous video is labeled as positive and a normal video is labeled as negative. The ADVS solution considers the video surveillance a regression problem. The abnormal video frames have high score than the regular frames. This score of video data is ranged between 0 and 1. In our approach the extraction of features from videos is done using C3d i.e. extracting 3D convolutional features by first re-sizing the image to 240x320 pixels with frame rate of 30 fps. Now we make segments of video, each segment contains 16-frames. Here every 16-frame video clip is applied with Euclidean normalization as it is calculated as Euclidean distance from the origin. Finally, features are extracted for a segment of video by taking average (16-frames per segment). Extracted features are given as input to a fully connected neural network which has 3 layers. The first layer of this network has 512 units, second layer has 32 units and final layer has single unit. All of these layers are fully connected with each other. Dropout regularization of 60% is employed between layers to avoid overfitting. ReLU activation function is used in first layer and Sigmoid activation for the last layers. Learning rate which is initially used in our model is 0.001.

4.2 Dataset

The set we opted for is UCF crime dataset which consists of 13 anomalies mentioned as under:

a. Abuse.
b. Arrest.
c. Arson.
d. Assault.
e. Burglary.
f. Explosion.
g. Fighting.
h. Normal Videos.
i. Road Accidents.
j. Robbery.
k. Shooting.
l. Shoplifting.
m. Stealing.

The dataset can be viewed category wise as under:

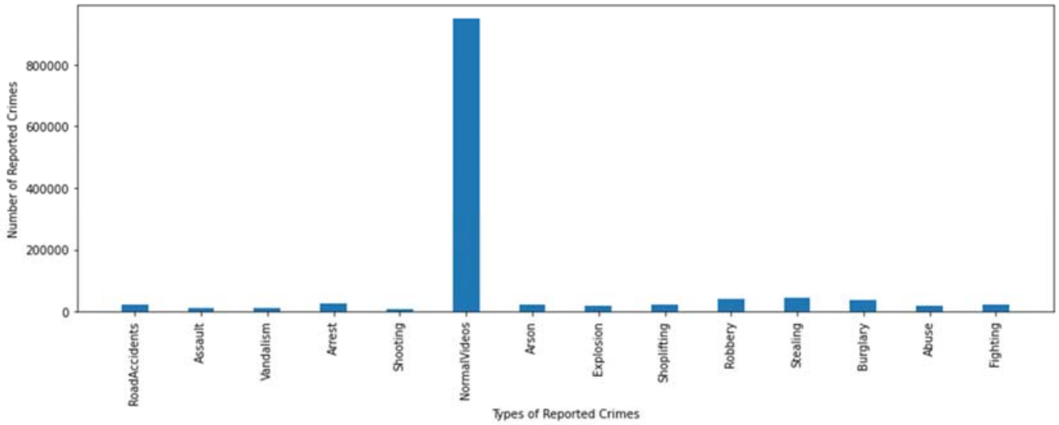


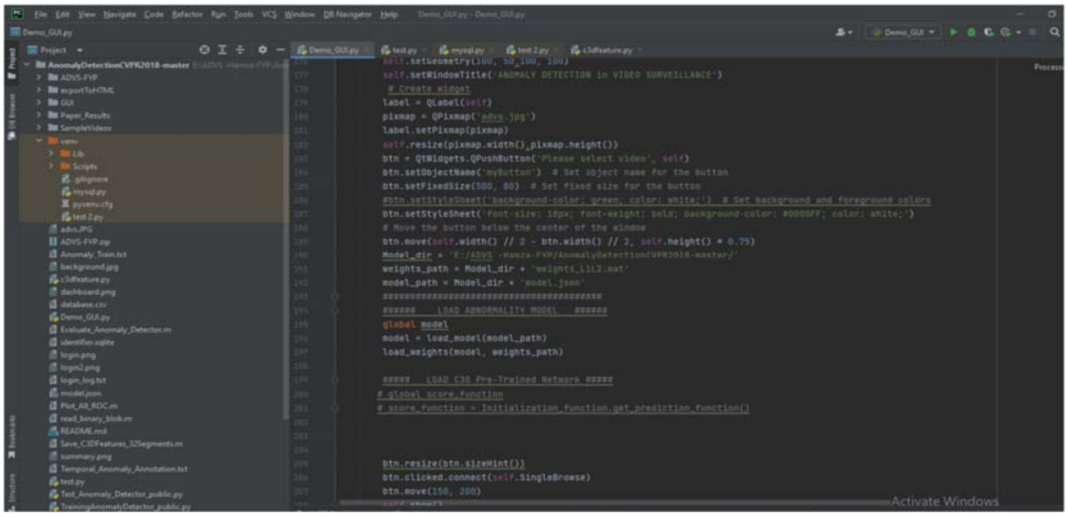
Figure 4. 1 Types of Crimes in Dataset

4.3 Tools Used

The tools used are mentioned below:

4.3.1 Pycharm

PyCharm is an IDE used for programming in Python. PyCharm comes with many useful features such as code completion, code analysis, debugging tools, version control integration, and support for various Python frameworks and libraries. It also has a user-friendly interface, which makes it easier for developers to navigate and work with their code.

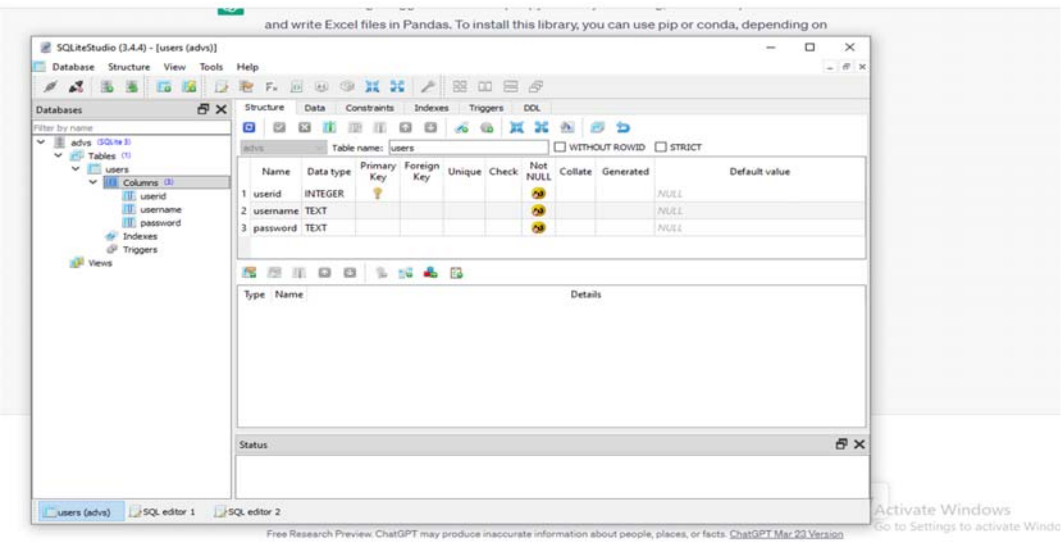


```
        self.setGeometry(100, 50, 100, 100)
        self.setWindowTitle('ANOMALY DETECTION in VIDEO SURVEILLANCE')
         # Create widget
        label = QLabel(self)
        pixmap = QPixmap('advs.jpg')
        label.setPixmap(pixmap)
        self.resize(pixmap.width(),pixmap.height())
        btn = QtWidgets.QPushButton('Please select video', self)
        btn.setObjectName('myButton')  # Set object name for the button
        btn.setFixedSize(500, 80)  # Set fixed size for the button
        #btn.setStyleSheet('background-color: green; color: white;')  # Set background and foreground colors
        btn.setStyleSheet('font-size: 18px; font-weight: bold; background-color: #0000FF; color: white;')
        # Move the button below the center of the window
        btn.move(self.width() // 2 - btn.width() // 2, self.height() * 0.75)
        Model_dir = 'E:/ADVS -Hamza-FYP/AnomalyDetectionCVPR2018-master/'
        weights_path = Model_dir + 'weights_L1L2.mat'
        model_path = Model_dir + 'model.json'
        ########################################
        ######    LOAD ABNORMALITY MODEL   ######
        global model
        model = load_model(model_path)
        load_weights(model, weights_path)

        #####   LOAD C3D Pre-Trained Network #####
       # global score_function
       # score_function = Initialization_function.get_prediction_function()



        btn.resize(btn.sizeHint())
        btn.clicked.connect(self.SingleBrowse)
        btn.move(150, 200)
        self.show()
```

Figure 4. 2 Pycharm IDE

4.3.2 SQLite Studio

It is database tool that used to manage databases. All the database tables have been created and managed through SQLite Studio.



and write Excel files in Pandas. To install this library, you can use pip or conda, depending on
SQLiteStudio (3.4.4) - [users (advs)]
Database
Structure
View
Tools
Help
Databases
Filter by name
advs (SQLite 3)
Tables (1)
users
Columns (3)
userid
username
password
Indexes
Triggers
Views
Structure
Data
Constraints
Indexes
Triggers
DDL
advs
Type
Name
Details
Status
users (advs)
SQL editor 1
SQL editor 2
Activate Windows
Go to Settings to activate Windo
Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT Mar 23 Version

Table name: users ☐ WITHOUT ROWID ☐ STRICT

	Name	Data type	Primary Key	Foreign Key	Unique	Check	Not NULL	Collate	Generated	Default value
1	userid	INTEGER	●				●			NULL
2	username	TEXT					●			NULL
3	password	TEXT					●			NULL

Figure 4. 3 SQLite Studio

Chapter 5

5. DETAILED DESIGN & ARCHITECTURE

5.1 System Architecture

This system is a follow-on member of a Video Surveillance Systems for detection of anomalies. Subsystems like image extraction, Model training and Anomaly categorization are incorporated to fulfil software requirements. ADVS can have external interface with live feed of CCTV camera. ADVS will use local storage (workstation storage) to store videos for testing and training purposes. The diagram below shows the subsystems and eternal interface of the system.

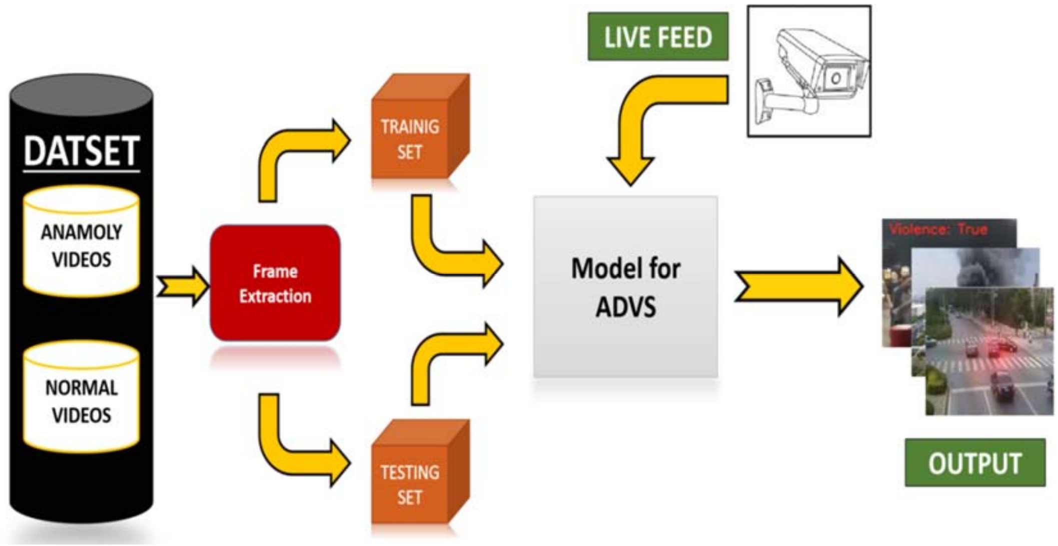


Figure 5. 1 System Architecture

5.1.1 Architectural Design

The ADVS system has a layered architecture there two layers of architecture. First layers consist of database, Controller and User (user specific functionalities) and second layer consists of anomaly detection. Controller is the main component between two layers the integrates them and delegates different tasks to components.

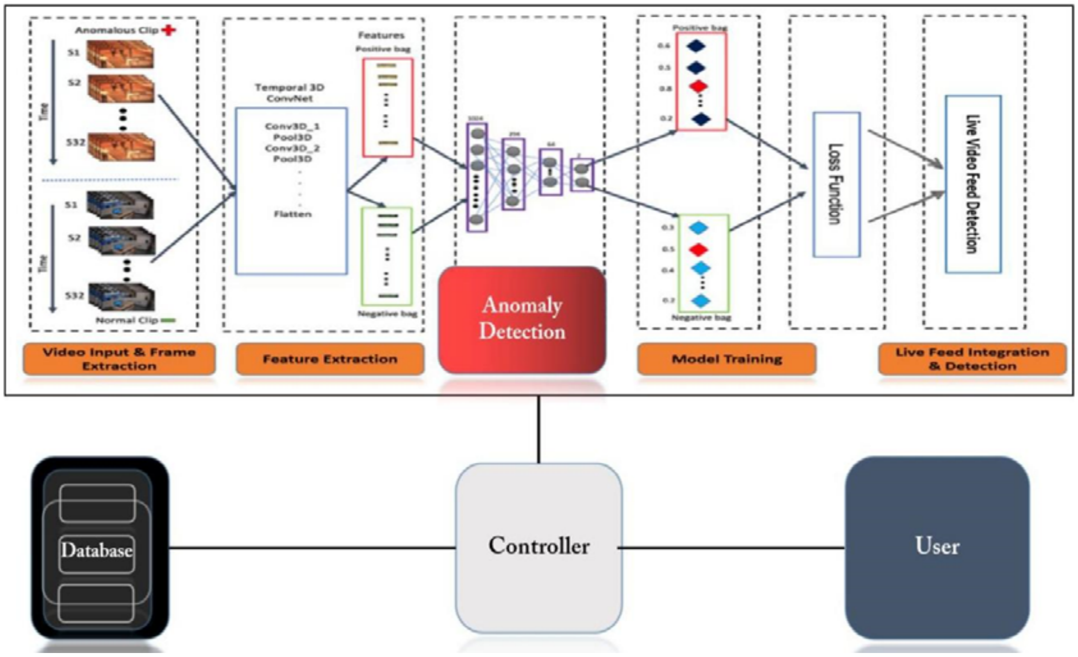


Figure 5. 2 Architectural Design

5.2 Detailed System Design

The system is divided into two main layers. The detailed system design is explained as under:

5.2.1 Classification

5.2.1.1 Layer 1

a. **Database:** The component deals with the database related functions which are mainly manage and viewing logs, user login, user management in SQLite Studio.

b. **Controller:** This is the main component of the system that controls the system. It is the central point of interaction and integration of all the components. This component will delegate responsibilities to different components based on the operation selected by user in User component.

c. **Manage User:** This component contains all the functionalities performed by the system users. Our system has two types of user Admin and the operator.

5.2.1.2 Layer 2

This component mainly works on the anomaly detection on live feed of video. It is again sub divided into four layers namely Video Input & frame extraction which takes video data set as in put and extract frames from videos at 30 fps, Feature extraction from the available frames into features for further use in model training, Model training(training and loss function) that trains the model and performs the optimization and Live feed Integration and detection that takes video input from IP camera integrates it with the model and gives real time anomaly detection and alarm generation.

5.2.2 Constraints

a. Simplicity over enhanced and lucrative user interface to improve system response.

b. Usability over security, as only username password will be used to authenticate the user.

c. Time duration to detect anomaly is directly proportional to length of the video.

d. The lengthier the video, resulting in more number of frames extracted. This increases the calculation of score and plotting the score frame by frame in a graph form. Hence it will consume more RAM.

5.2.3 Uses and Interaction

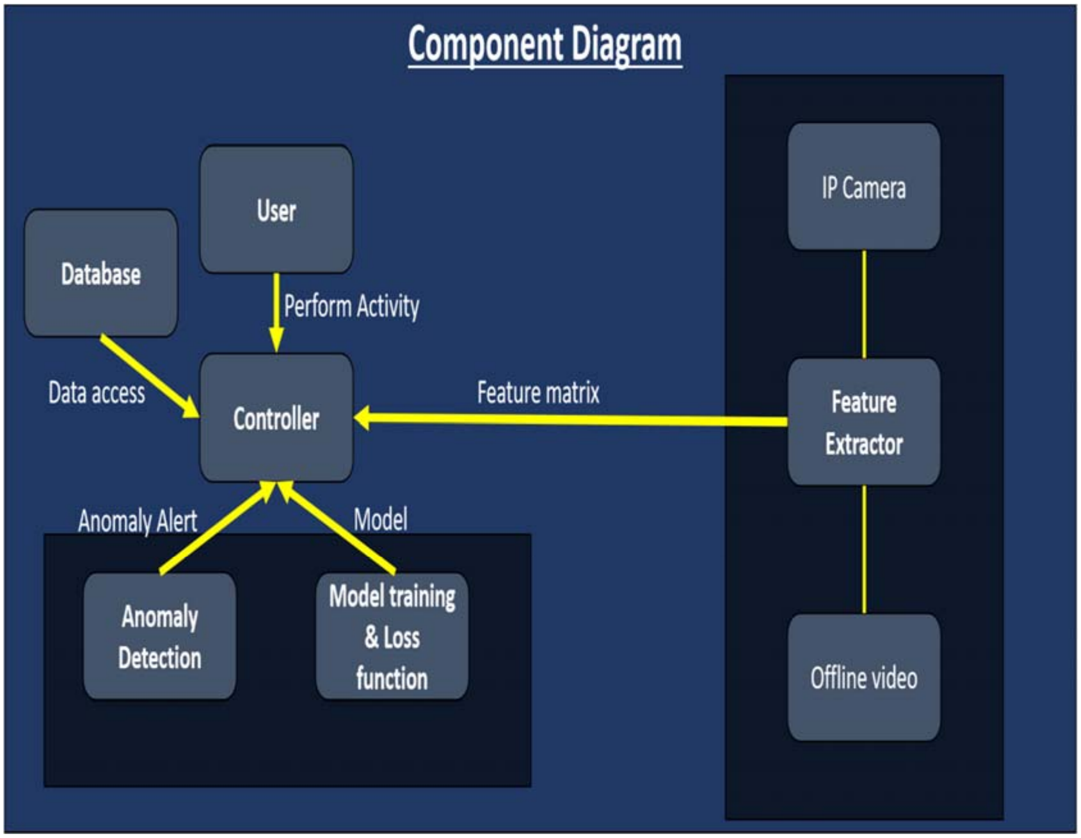


Figure 5. 3 Component Design

5.2.4 System Features

5.2.4.1 Dashboard

This is the main screen of the application and helps the user to navigate through the system. This feature of the system provides video analysis, login logs, anomaly logs and manage user. The priority of this feature is high because it gives the access to other features of the system.

5.2.4.2 Video Analysis

This feature of the system provides offline video analysis. User can use this feature to upload a video on which the user wants to perform analysis. The priority of this feature is high because it detects the anomaly in an offline video.

5.2.4.3 Login Logs

The system facilitate the management of logs related to the system. Login Logs, contains login details, date time and logout details of all users.

5.2.4.4 Anomaly Logs

The system facilitates the management of anomaly logs. When system detects an anomaly it logs that anomaly name, anomaly timings with all other necessary details in to the system.

5.2.4.5 Manage Users

The Admin and developers must be able to manage user accounts. The operations supported in this feature are:

a. Create new User.

b. Update User information.

c. Remove User.

d. Unblock User (For blocked users because of invalid login attempts).

5.2.4.6 User Login/ Logout

The users of the system able to login and logout to the system using this feature. Only registered is able to perform video analysis and check logs. The user is able to logout from the system when required.

5.2.4.6 Trend Analysis

Trend analysis is one of the core functionality, enabling users to identify patterns and anticipate potential anomalies. Moreover, it incorporates user login log monitoring, ensuring accountability and providing a comprehensive overview of system access. Furthermore, the software facilitates the visualization of previously detected anomalies, allowing users to analyze and understand abnormal events in relation to specific dates and times. By harnessing the power of advanced anomaly detection algorithms and intuitive visualization tools, this software empowers users to proactively respond to security threats, make data-driven decisions, and improve overall safety and efficiency in various domains.

5.2.5 High level Use Cases

Use Case	Login
Actors	User, Admin
Type	Primary
Description	The User and Admin if registered must be able to enter their name, id along with their password and authenticates themselves to enter the system.
Use Case	Logout
Actors	User, Admin
Type	Primary
Description	The User and Admin if logged into the system must be able to logout of the once, they have performed the activities.
Use Case	Save Logs
Actors	User, Admin
Type	Primary
Description	The User and Admin if logged in must be able to save logs manually related to anomaly detected in videos.
Use Case	View Logs
Actors	User, Admin
Type	Primary
Description	The User and Admin if logged in must be able to view logs related to videos in the database.
Use Case	View User Logs

Actors	Admin
Type	Primary
Description	The User and Admin if logged in must be able to view logs related to user in the database.
Use Case	Set profile picture
Actors	User, Admin
Type	Primary
Description	The User and Admin if logged in must be able to set their profile picture by selecting in picture in JPG or PNG format.
Use Case	Change Password
Actors	User, Admin
Type	Primary
Description	The User and Admin if logged must be able to change password as per requirement. The password can be combination of alphabets numbers and special characters.
Use Case	Recover Password
Actors	User, Admin
Type	Primary
Description	The User and Admin if not blocked by system must be able to recover and then change password by answering secret question.
Use Case	Set Secret Question
Actors	User, Admin
Type	Primary

Description	The User and Admin if logged into the system must be able to set a secret question and its answer as a contingency. In case they forget password.
Use Case	Offline Video Analysis

Actors	User, Admin
Type	Primary
Description	The User and Admin if authorized after login must be able to select video clip for anomaly detection. The video must be in mp4 format.
Use Case	Trend Analysis
Actors	User, Admin
Type	Primary
Description	The User and Admin if logged in must be able to view the trends and graphs pertaining to user activities and types of anomalies occuring by day and time.
Use Case	Record anomaly Log
Actors	System
Type	Primary
Description	The must be able to automatically save the log of anomaly detected in a video feed.
Use Case	Create User
Actors	Admin
Type	Primary

Description	The Admin must be able to create any new user of the system.

5.2.6 Expanded Use Cases

UC01	
Use Case Name	Login
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin want to enter system to monitor video anomaly
Pre-Condition	Application must be responsive, and User must be Registered.
Success Guarantee	The User or Admin will enter the system
Main Success Scenario	**Actor Action System Responsibility** 1. The User/Admin 2. If user is registered enters the credentials and login credentials are for authentication valid the system will redirect user to Main page. 3. If invalid attempt is made the user must be prompted to re-login. 4. If 3 invalid attempts are made, then block the user.

Extensions	If user is not registered, then Admin must register user. If 3 invalid attempts are made block user.

UC02	
Use Case Name	Logout
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin want to leave system after performing activities.
Pre-Condition	Application must be responsive, User must be logged in.
Success Guarantee	The User or Admin will be redirected to login page.
Main Success Scenario	**Actor Action System** 1.The User/Admin requests to logout 2.If user session of the system by exists the destroy the pressing logout session and redirect button. the user to login page.
Extensions	The system will show login page.

UC03	
Use Case Name	Save Logs
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must be able to save logs related to anomaly in videos.
Pre-Condition	Application must be responsive, Database must be available, and User must be logged in.
Success Guarantee	The User or Admin will save logs related to anomaly and database will be updated.
Main Success Scenario	**Actor Action System** 1.The User/Admin logs of a video 2. Reads Video and on a specific time save logs containing anomaly type, start and end of video and video name.
Extensions	The saved logs can be viewed in database.

UC04	
Use Case Name	View Logs
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin

Stakeholders and Interests	User and Admin must be able to view logs related to anomaly in videos.
Pre-Condition	Application must be responsive, Database must be available, and User must be logged in.
Success Guarantee	The User or Admin must be able to view logs on user interface.
Main Success Scenario	**Actor Action System** 1.The User/Admin view logs of a video. 2.Retrieve the requested log from system.
Extensions	Logs are viewed on User interface.

UC05	
Use Case Name	View User Logs
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must be able to view logs related to User (username, Profile picture, status, activities)
Pre-Condition	Application must be responsive, Database must be available, and User must be logged in.

Success Guarantee	The User or Admin will be able to view logs related to anomaly and database will be updated.

Main Success Scenario	**Actor Action System** 1.The User/Admin requests the user 2. Reads query and log from system. View logs containing user related data.
Extensions	The user can view logs on the user interface.

UC06	
Use Case Name	Set Profile Picture
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must be able to Set profile Picture (JPG, PNG) format.
Pre-Condition	Application must be responsive, Database must be available, and User must be logged in.
Success Guarantee	The User or Admin will be able to set profile picture.

Main Success Scenario	**Actor Action System** 1.The User/Admin **Responsibility** selects the picture 2. System will save them from storage and selected picture in sets it.database.
Extensions	The selected picture will be displayed in a profile box at the top of the page.

UC07	
Use Case Name	Change Password
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must be able to change password as per requirements.
Pre-Condition	Application must be responsive, Database must be available, User must be logged in and User must enter old password.
Success Guarantee	The User or Admin’s password will be changed.

Main Success Scenario	**Actor Action System** 1.The User/Admin enters old password 2. Reads the old password and new password and match password and in database, if the old requests to change password is valid then password. Allow the user to change password.
Extensions	The user will be redirected to login page, old session will be destroyed, and user must login again with new password.

UC08	
Use Case Name	Recover Password
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must be able to recover password by answering secret question in case they forget password.
Pre-Condition	Application must be responsive, Database must be available, User/Admin must register and secret question must be set by user/admin.
Success Guarantee	The User or Admin's will be able to recover password.

Main Success Scenario	**Actor Action System** 1.The User/Admin **Responsibility** answer the secret 2. Reads the answer question. and matches in database, if match found redirect to the user to Reset password page.
Extensions	The user will be redirected to Reset password page where they must enter new password.

UC09	
Use Case Name	Set Secret Question
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	The Admin/User must be able to set a secret question and answer.
Pre-Condition	Application must be responsive, Database must be available, User must be logged in.
Success Guarantee	The User or Admin will be able to set secret question.

Main Success Scenario	**Actor Action System** 1.The User/Admin enters secret 2. Reads the question and its and answer and saves answer in the database.
Extensions	The user will be able to recover password using this secret question.

UC10	
Use Case Name	Offline Video Analysis
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must be to select a video clip and perform anomaly detection on it and generate alarm if anomaly is detected.
Pre-Condition	Application must be responsive, Video clips must be selected (.mp4 format) and trained model must be available.
Success Guarantee	The User or Admin's will be able to analyze video for anomaly, on detection of anomaly an alarm will be generated.

Main Success Scenario	**Actor Action System** 1.The User/Admin selects the video 2. Perform frame and clip for analysis. feature extraction and detects for anomalies. The system will save a log if anomaly occurs.
Extensions	The user will be alerted on anomaly and log will be saved.

UC11	
Use Case Name	Trend Analysis Analysis
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	User, Admin
Stakeholders and Interests	User and Admin must able to view the user activities and behaviour in graphical form. In addition to this the users of the system must be able to view types of anomalies that have been occurred, their frequency, time, date and day of occurring. This information must be viewed in graph form.
Pre-Condition	Application must be responsive, Ip camera must be functional and trained model must be available for anomaly detection.
Success Guarantee	The User or Admin's will be able to view different types of bar chart and graphs to perform the analysis.

Main Success Scenario	**Actor Action System** 1.The User/Admin selects the Online 2. Perform frame and video analysis feature extraction and option. Detects for anomalies. The system will save a log if anomaly occurs.
Extensions	The user will be alerted on anomaly and log will be saved.

Main Success Scenario	**Actor Action System** 1.The User/Admin checks for camera 2. If feed available, the feed. system will display the feed on user interface else an error will be shown.
Extensions	The user will be able to analyze videos for anomaly.

Main Success Scenario	**Actor Action System** 1.The Admin entre username of user 2.System searches to be blocked. The username in the database and blocks the user.
Extensions	The blocked users will not be able to login the system.

UC15	
Use Case Name	Save Anomaly Log
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	System
Stakeholders and Interests	If an anomaly in a video is detected the system must be able to save a log.
Pre-Condition	Application must be responsive, and a video must be fed to system.
Success Guarantee	The system saves a log of anomaly detected on a video.

Main Success Scenario	**Actor Action System** 1.Continously analyzes video for 2.Save a log of analysis. detected anomaly.
Extensions	The user will be to view logs.

UC16	
Use Case Name	Generate Alarm
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	System
Stakeholders and Interests	The system must be able to generate an alarm on detection of anomaly.
Pre-Condition	Application must be responsive, and a must be fed to system.
Success Guarantee	System will be able to generate an alarm.
Main Success Scenario	**Actor Action System** 1.The actor will detect an anomaly. 2. If anomaly found, generate an alarm to alert user.
Extensions	The user will be view anomaly logs.
UC17	
Use Case Name	Delete Logs
Scope	Anomaly detection in Video Surveillance

Level	Primary
Primary Actor	Admin
Stakeholders and Interests	The admin must be able to delete user and video related logs from database
Pre-Condition	Application must be responsive, and a must be fed to system.
Success Guarantee	The logs will be deleted from the database
Main Success Scenario	**Actor Action System** 1.The actor will select the log to be 2. system will delete deleted the requested log.
Extensions	The log database will be updated.

UC18	
Use Case Name	Create user
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	Admin
Stakeholders and Interests	The admin must be able to create new user
Pre-Condition	Admin must be logged in & database must be available
Success Guarantee	On success new user shall be created

Main Success Scenario	**Actor Action System** 1.The admin will enter user 2. the system will store credentials into the user credentials and system will generate a success message
Extensions	The user will be able to use the system.

UC19	
Use Case Name	Remove user
Scope	Anomaly detection in Video Surveillance
Level	Primary
Primary Actor	Admin
Stakeholders and Interests	The admin must be able to remove user
Pre-Condition	Admin must be logged in & database must be available
Success Guarantee	On success user shall be removed

Main Success Scenario	**Actor Action System** 1.The admin will enter user 2. The system will credentials into the delete user credentials system and will generate a success message
Extensions	The user will not be able to use the system.

5.2.7 Use Case Diagram

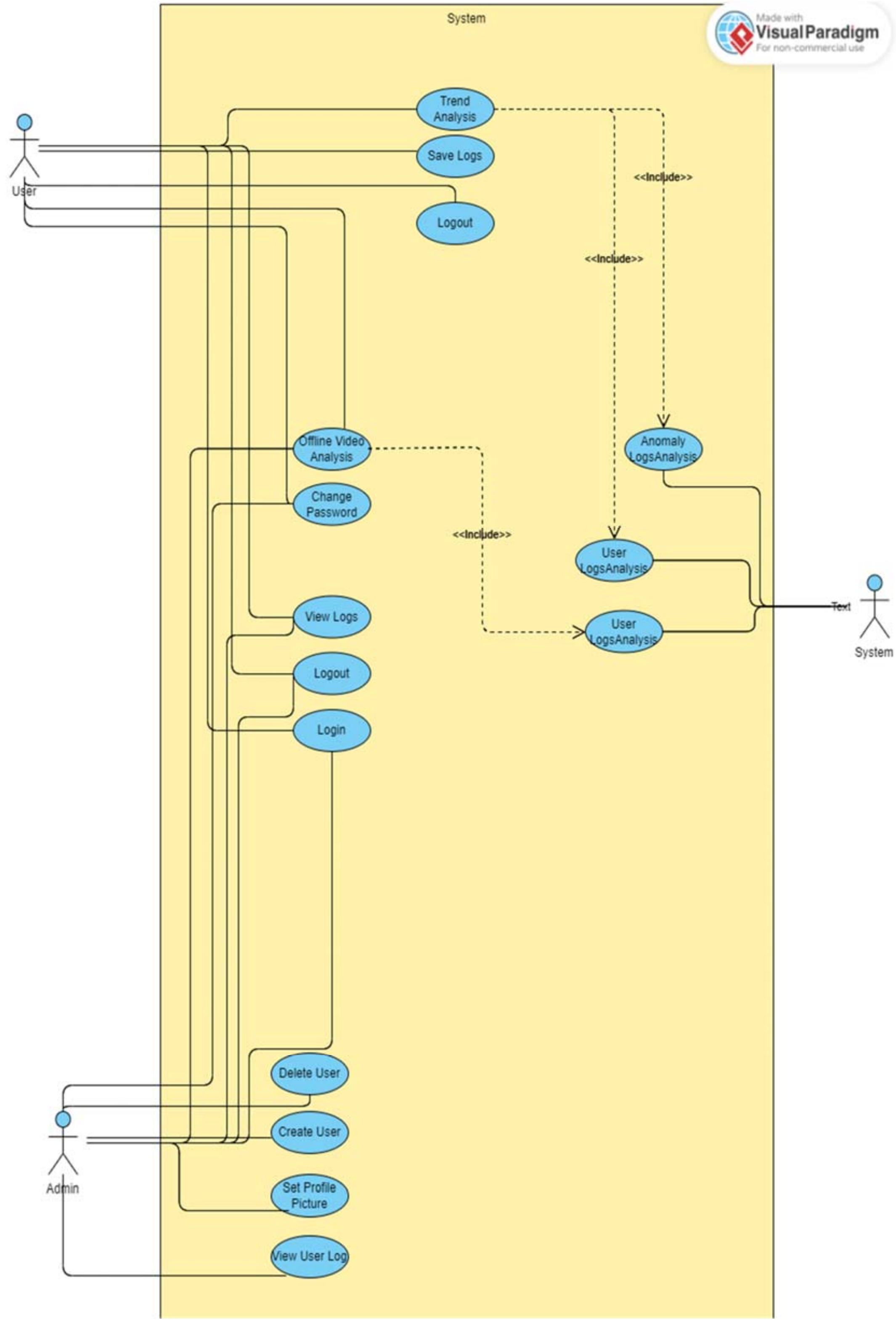


Figure 5. 4 – Use Case Diagram

5.2.8 Sequence Diagrams

i. Login

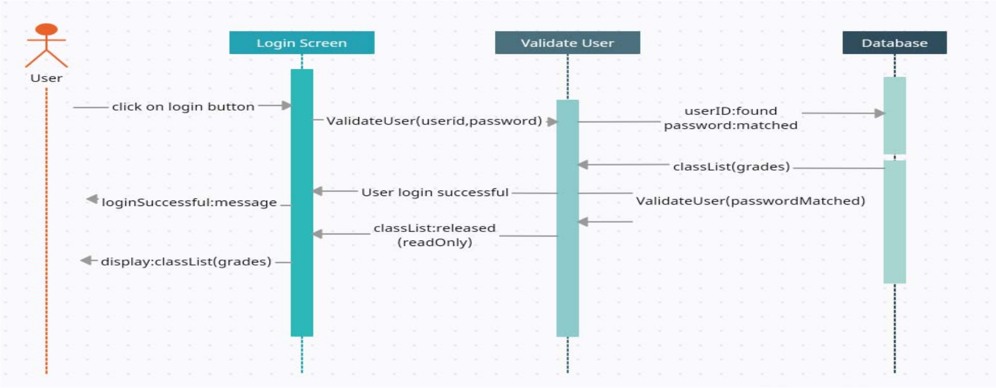


Figure 5. 5 – Login Sequence Diagram

ii. Logout

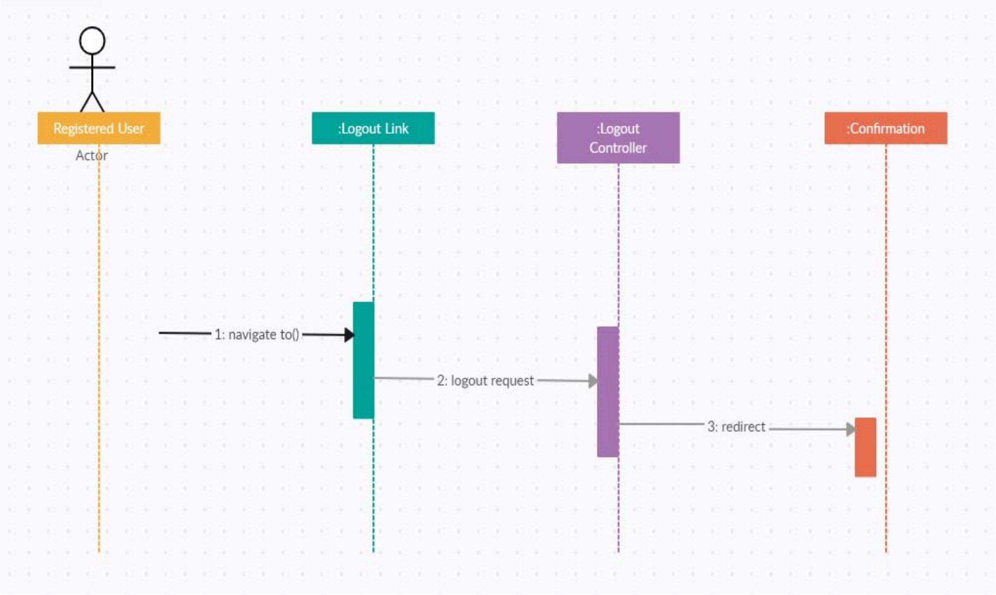


Figure 5. 6 – Logout Sequence Diagram

iii. Save Logs

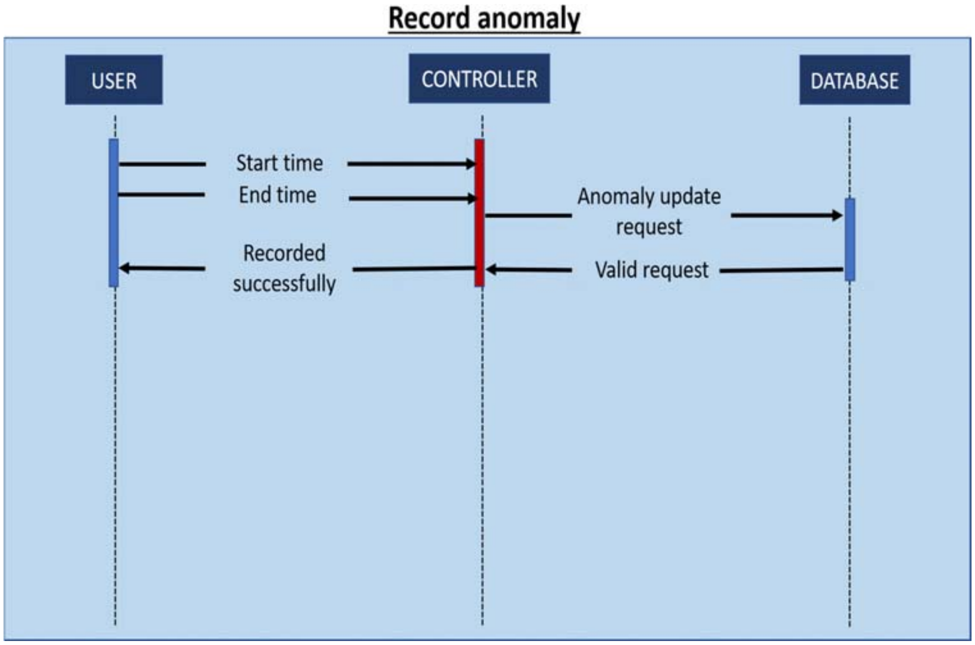


Figure 5. 7 – Save Log Sequence Diagram

iv. View Logs

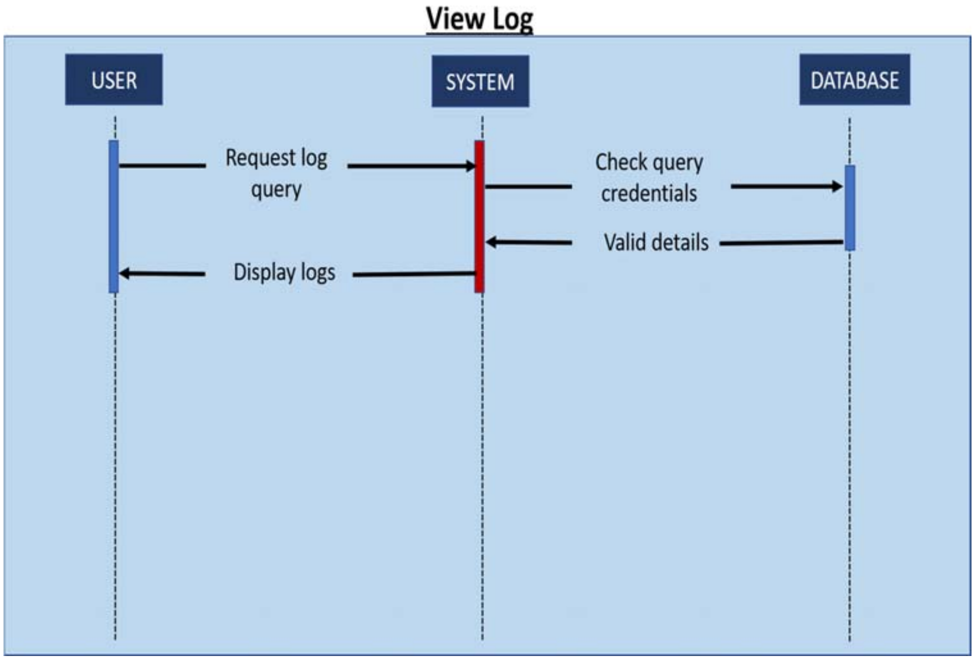


Figure 5. 8 – View Log Sequence Diagram

v. Set Profile Picture

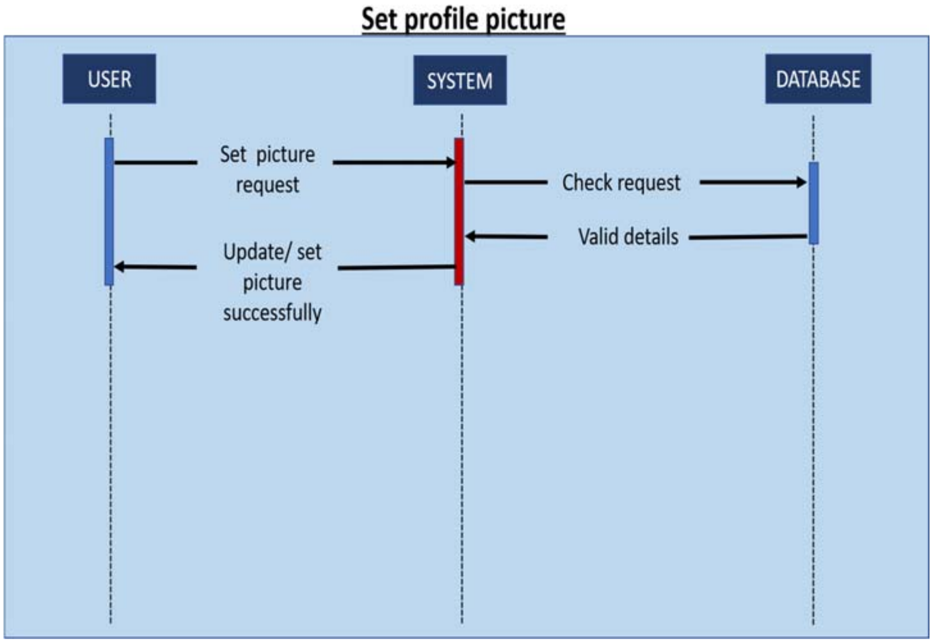


Figure 5. 9 – Set Profile Picture Sequence Diagram

vi. Change Password

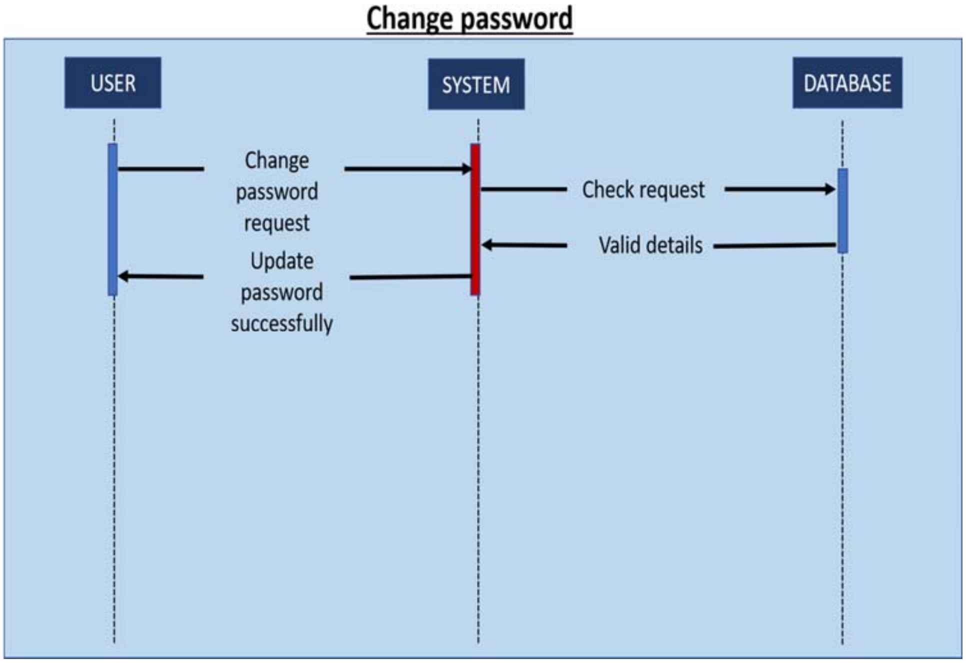


Figure 5. 10 – Change Password Sequence Diagram

vii. Offline Video Analysis

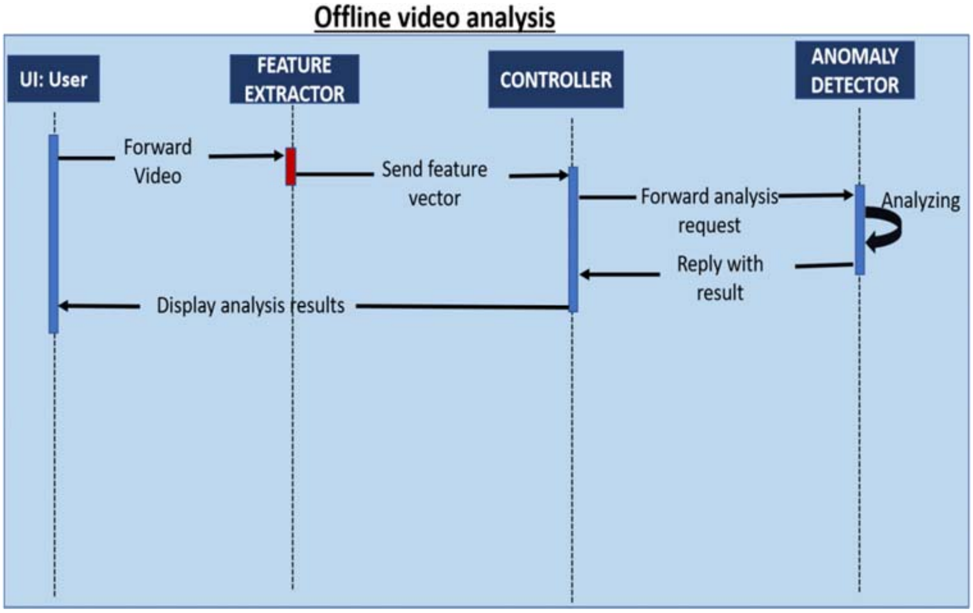


Figure 5. 11 - Offline Video Analysis Sequence Diagram

viii. View User Logs

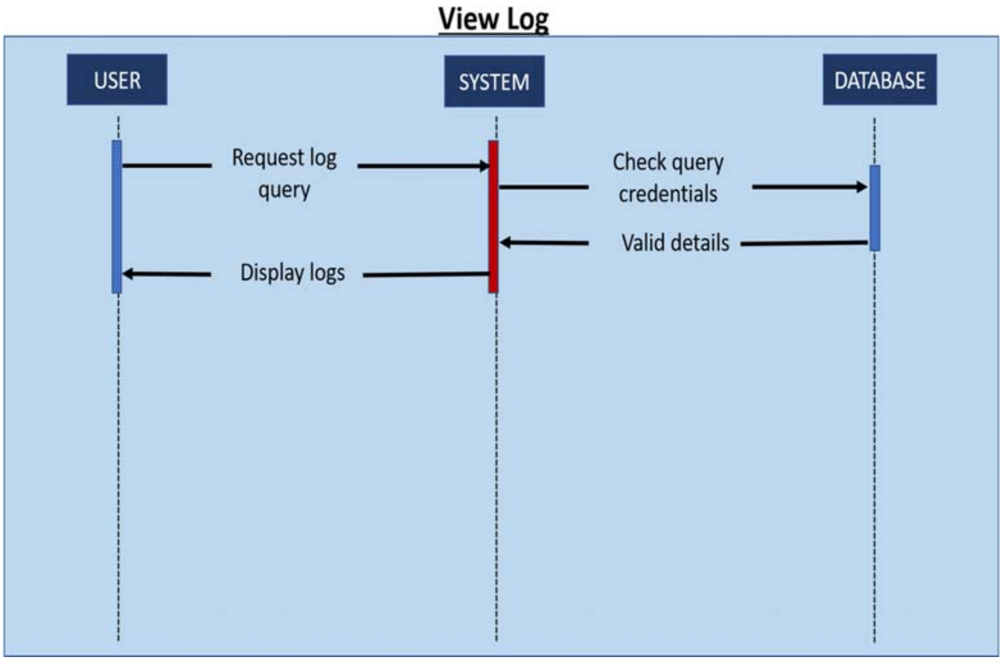


Figure 5. 12 – View User Log Sequence Diagram

ix. Create User

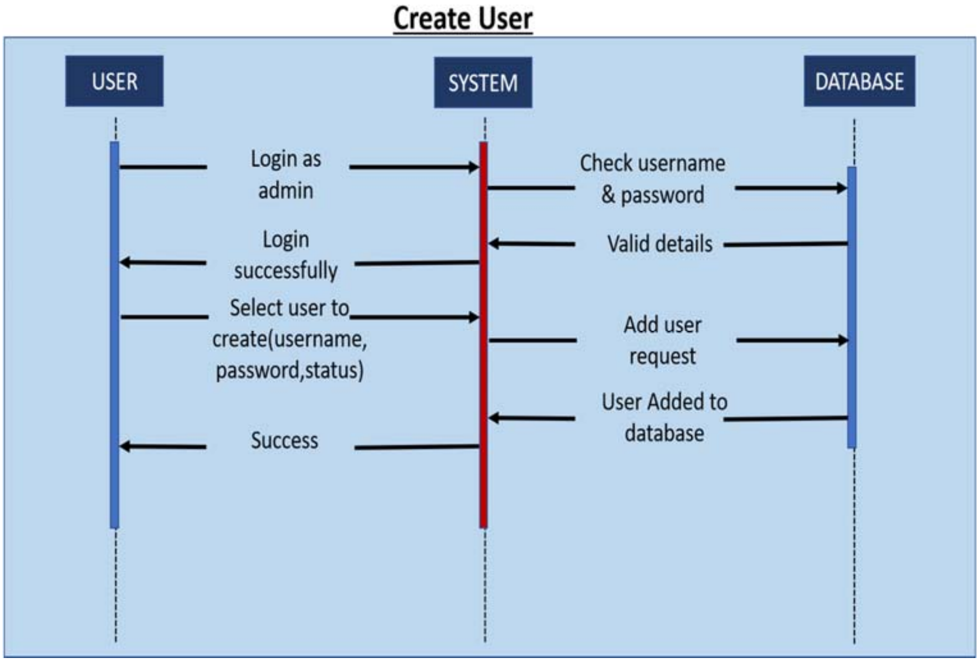


Figure 5. 13 – Create User Sequence Diagram

5.2.9 Functions and Function Parameters

i. Extract_Frames(video_name,video_extension,Number_framepersecond)

ii. Extract_Features(Frames_List) // List of Frames extracted

iii. Trend Analysis(Anomaly_logs,User_Logs)

iv. Anomaly_detection(FeatureMatrix, Model)

v. Save_Logs(anomaly_starttime,anomaly_endtime,User_id,Date_time)

vi. View_Logs()

vii. Login(Username,Password)

viii. Logout()

ix. View_UserLogs(username)

x. Set_profilepicture(image,userid)

xi. Generate_Alarm(Threshold)

xii. Offline_Video_Analysis(Videoclip, Model)

xiii. Create_User(username,password,Status)

xiv. Delete_User(username)

xv. View_User(username)

5.2.9.1 Pseudocode for Functions

i. Unblock User(username)

```
{
Connectdatabase() If Connection open
Sqlquerry= select user where username=username Get_user_record=Sqlquerry_run()
Update user status=Unblock Commitchang() CloseConnection()
Else
Error_generate()}
```

ii. Create_User(Username,Password,Status)

```
{
Connectdatabase() If Connection open
Sqlquerry= insert into user    username=username, Password=Password,Status=Status
Insert_user_record=Sqlquerry_run() CloseConnection()
Else
Error_generate()
    }
```

iii. Generate_Alarm(Threshold)

```
{ If |mean_prevframes-mean_currentframe|>Threshold
    Call(alrm.mp3)
}
```

iv. Trend_ANalysis(Anomaly_logs,User_Logs)

```
{
Plot1=ReadAnomalylogs()
Plot2=ReadUserLogs()
Generate(Plot1,PLot2)
}
```

v. Offline_Video_Analysis(VideoClip,Model)

```
{
While(VideoClip==True)// Run compelete video and read frames
{
Extract_Frames(video_name,video_extension,Number_framepers
econd)
Extract_Features(Frame_List) Anomaly_Detction(FeatureMatrix,Model)
}
}
```

vi. Extract_Frames(video_name,video_extension, number_framepersecond)

```
{
Read_video(video_name, video_extenion) If video exist
While(true)
Extract frames using cv2 library
Save the extracted frames as jpeg format by frame name End while
Else
        Generate_error()}
```

vii. Extract Features Function Pseudo code

```
Extract_Features(Frame_list)
{
While (Frame_list !=NULL)
Extract features from frames using Scikit-Image library While end
Return feature matrix
}
```

viii. Anomaly Detection Function Pseudo Code

```
Anomaly_Detection(featurematrix,model)
{
Model.fit(Feature_matrix) If(Model.results()!=NULL)
Generate alarm Return Model.results()
}
```

ix. Save Logs Function Pseudo Code

```
Save_Logs(anomaly_stattime,anmaly_endtime,user_id,Date_time)
{
Anomaly_name=fetch.current_anomaly() Open database connection
Run database insert query of anomaly log table Close database connection
}
```

x. View Logs Function Pseudo Code

```
View_Logs()
{
Open database connection
Fetch logs from anomaly log table Start While (logs.next!=NULL)
Display results End while
Close database connection
}
```

xi. Login Function Pseudo Code

```
Login (username, password)
{
```

```
Open database connection Result=Run Select query on user table
While(result.next!=NULL)
If(result[0]==username && result[1]==password) Access granted
Deny access, Try again
se
Close database connection
}
End while
```

xii. Logout Function Pseudo Code

```
Logout()
{
Destroy current session Redirect to home page
}
```

xiii. View User Log Function Pseudo Code

```
View_UserLogs(username)
{
Open database query
Result=Run select query on user log table where name=username
While (result.next!=NULL)
Display user log While end
Close database connection
}
```

xiv. Set Profile Picture Function Pseudo Code

```
Set_profilepicture(image,userid)
{
Open database query
Run Update query on user user table where Uid=userid Close database connection
}
```

xv. Change Password Function Pseudo Code

```
Change_Password(username,password)
{
Open database connection
Run Update query on user table where name=username && pass=password
Close_database_connection}
```

5.2.6 Interface Design

ADVS has a very user friendly and simple interface. After initializing, user enters login id and password. The main dashboard has functions like manage users, view logs, detect anomaly on videos. An admin has the rights add, or delete a user and delete logs.

5.2.6.1 Login

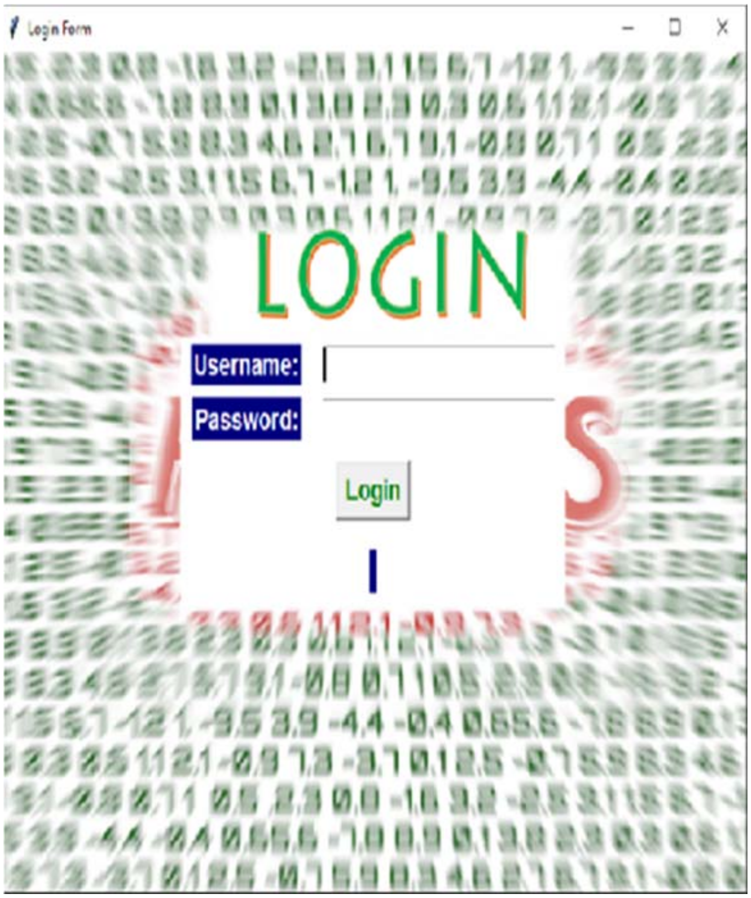


Figure 5. 14 Login

5.2.6.2 Dashboard

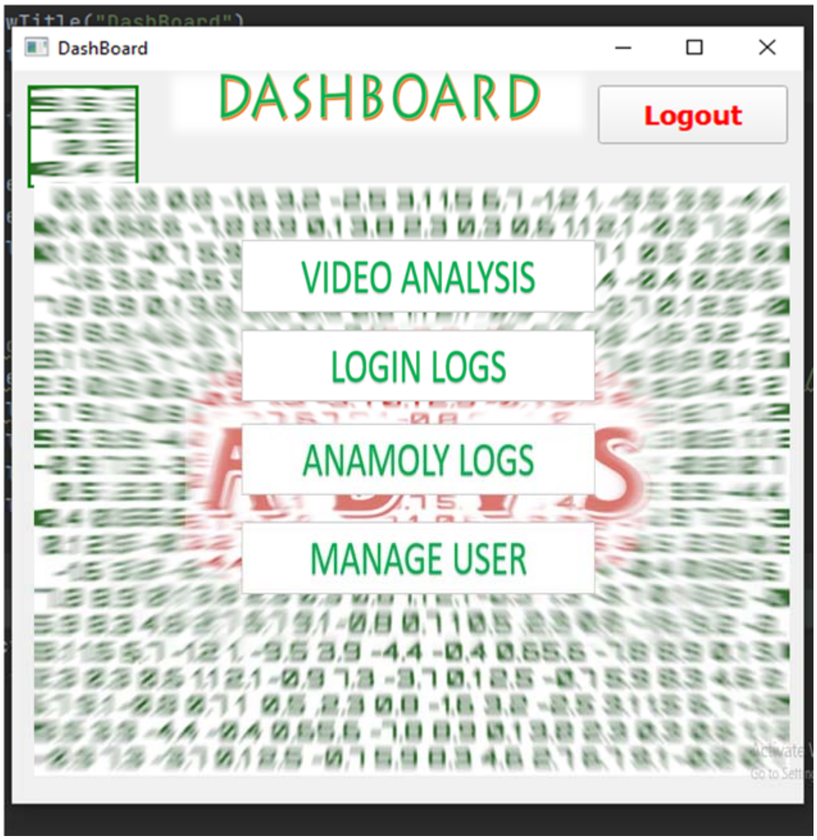
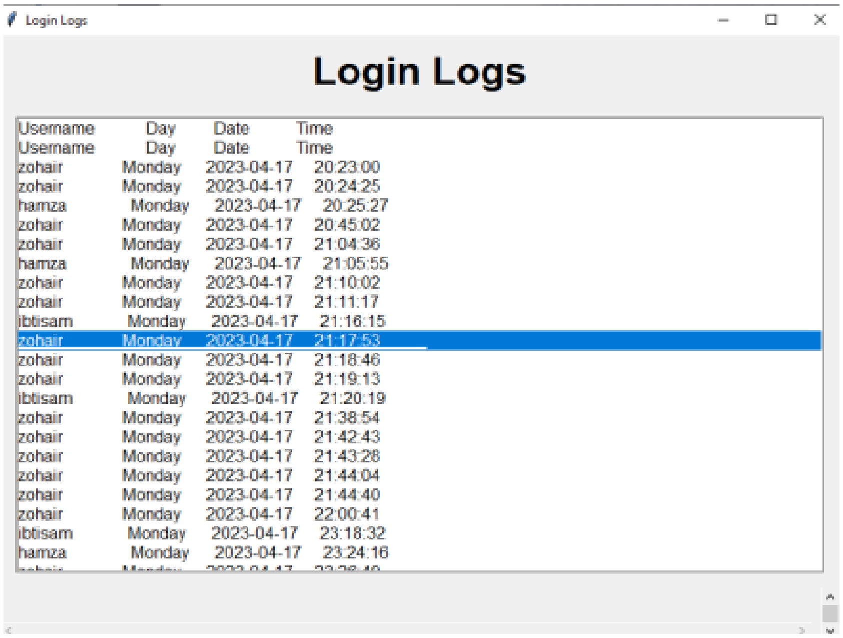


Figure 5. 15 Dashboard

5.2.6.3 Login Logs



Login Logs

```
Username        Day       Date         Time
Username        Day       Date         Time
zohair       Monday    2023-04-17    20:23:00
zohair       Monday    2023-04-17    20:24:25
hamza          Monday    2023-04-17    20:25:27
zohair       Monday    2023-04-17    20:45:02
zohair       Monday    2023-04-17    21:04:36
hamza          Monday    2023-04-17    21:05:55
zohair       Monday    2023-04-17    21:10:02
zohair       Monday    2023-04-17    21:11:17
ibtisam       Monday    2023-04-17    21:16:15
zohair       Monday    2023-04-17    21:17:53
zohair       Monday    2023-04-17    21:18:46
zohair       Monday    2023-04-17    21:19:13
ibtisam       Monday    2023-04-17    21:20:19
zohair       Monday    2023-04-17    21:38:54
zohair       Monday    2023-04-17    21:42:43
zohair       Monday    2023-04-17    21:43:28
zohair       Monday    2023-04-17    21:44:04
zohair       Monday    2023-04-17    21:44:40
zohair       Monday    2023-04-17    22:00:41
ibtisam       Monday    2023-04-17    23:18:32
hamza          Monday    2023-04-17    23:24:16
```

Figure 5. 16 Login Logs

5.2.6.4 Video Analysis

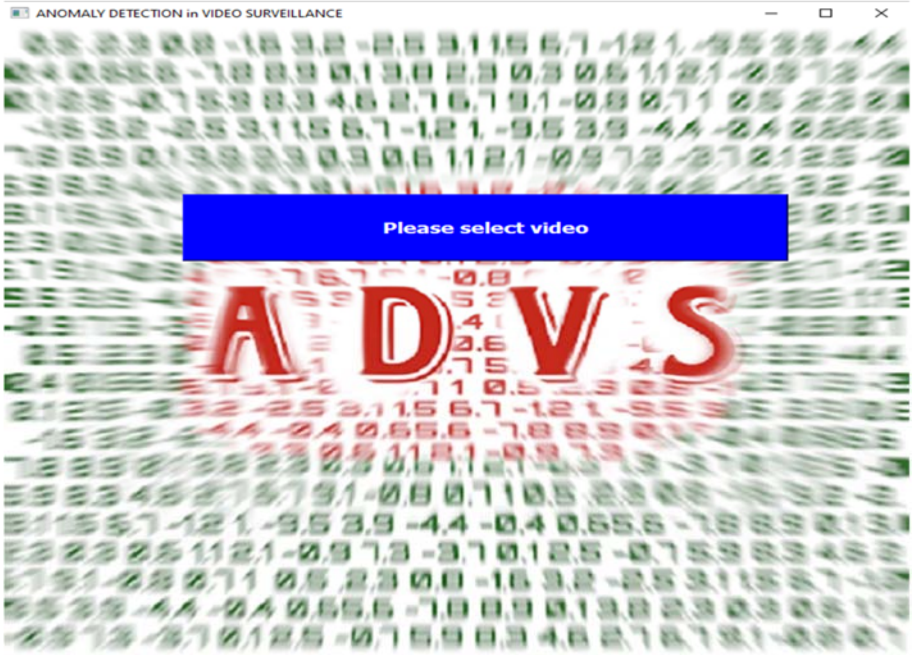


Figure 5. 17 Video Analysis

5.2.6.5 Trend Analysis

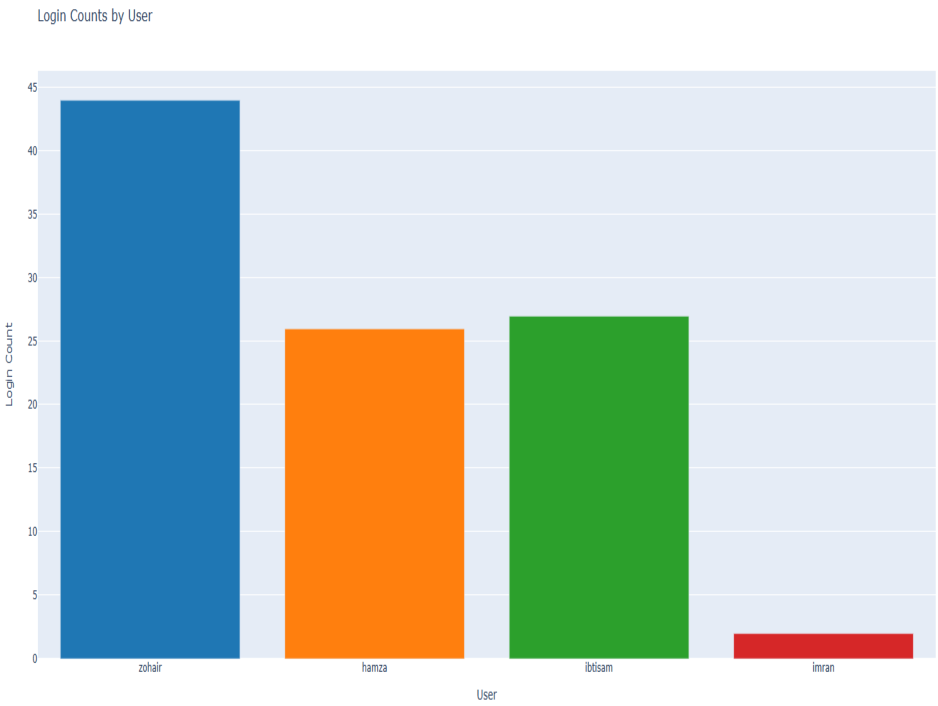


Figure 5. 18 Trend Analysis – User Count

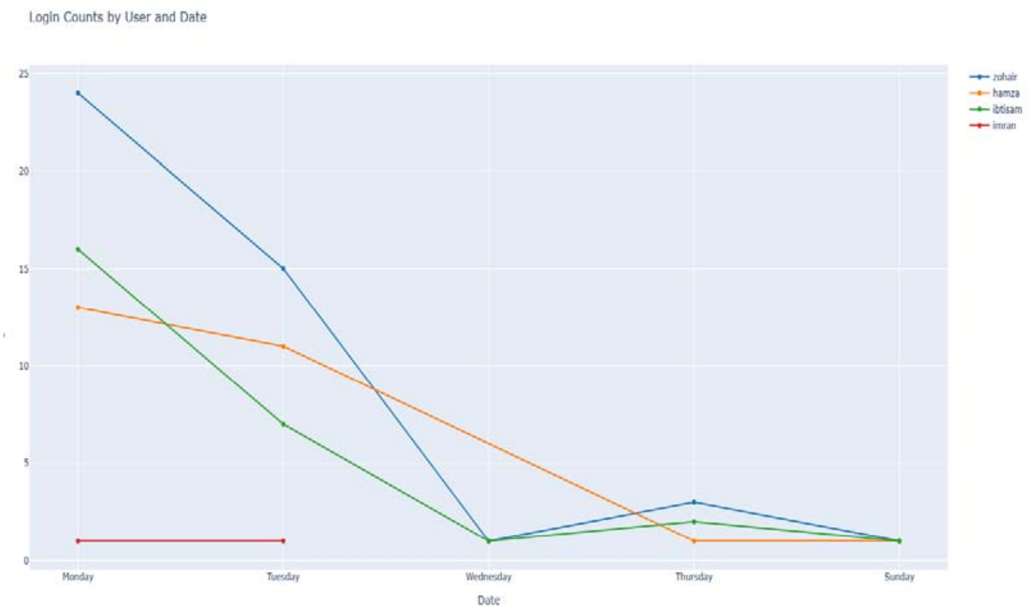


Figure 5. 19 – Login Count by User & Date

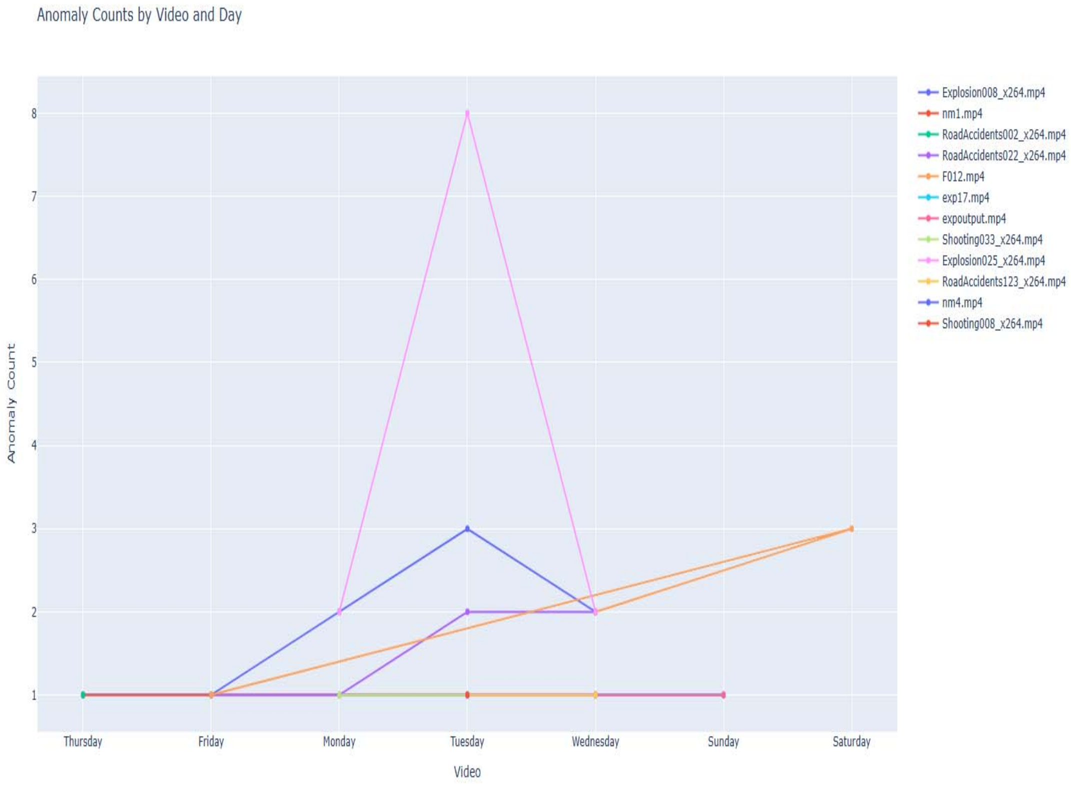


Figure 5. 20 – Anomaly Counts by Videos & Day

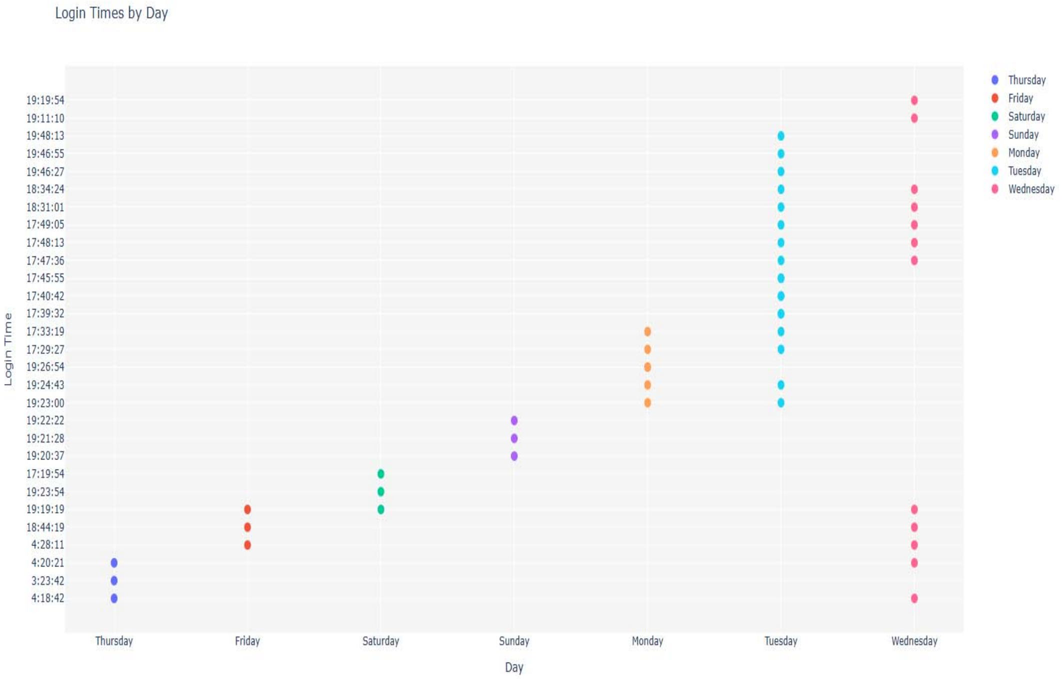


Figure 5. 21 – Login Times by Day

5.3 Class Diagram

We have three class which are app, pretty widget and model. The execution of the system starts with app class which further calls pretty widget class. Pretty widget class has login, logout and other functions in it. Model class is called by pretty widget class, after successful login. This class is responsible for loading the pre-trained model, weights and video that required to be analyzed.

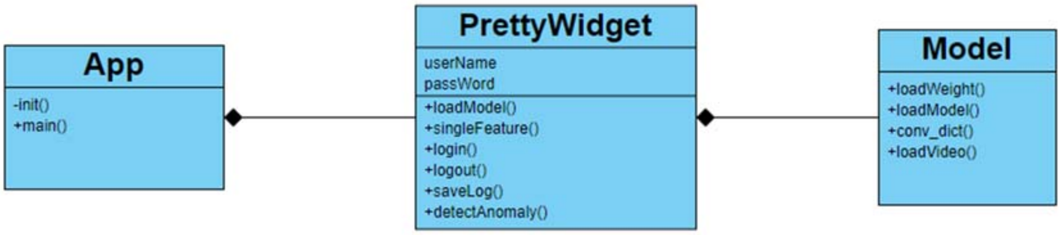


Figure 5. 22 Class Diagram

5.4 ER Diagram

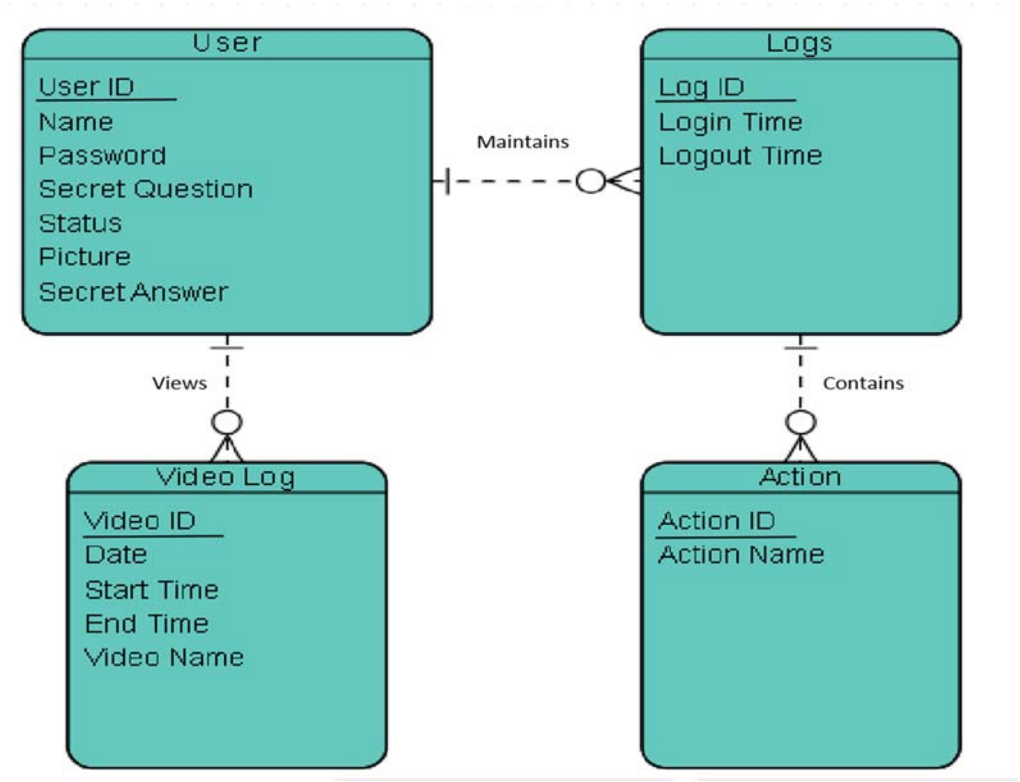
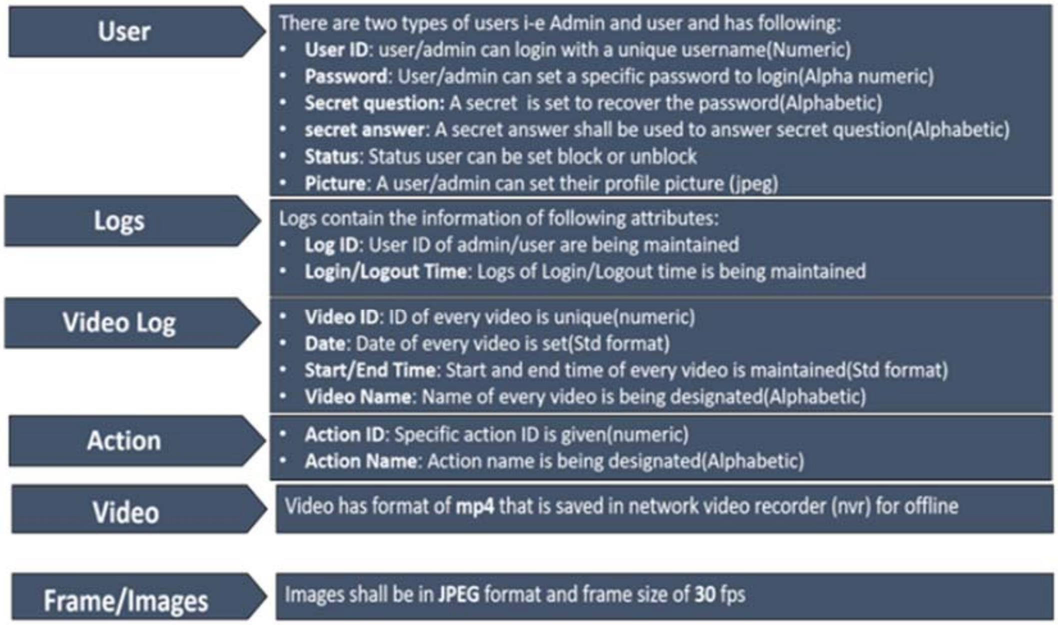


Figure 5. 23 ER Diagram

5.2.5 Detailed Subsystem



User

There are two types of users i-e Admin and user and has following:

- **User ID**: user/admin can login with a unique username(Numeric)
- **Password**: User/admin can set a specific password to login(Alpha numeric)
- **Secret question:** A secret is set to recover the password(Alphabetic)
- **secret answer**: A secret answer shall be used to answer secret question(Alphabetic)
- **Status**: Status user can be set block or unblock
- **Picture**: A user/admin can set their profile picture (jpeg)

Logs

Logs contain the information of following attributes:

- **Log ID**: User ID of admin/user are being maintained
- **Login/Logout Time**: Logs of Login/Logout time is being maintained

Video Log

- **Video ID**: ID of every video is unique(numeric)
- **Date**: Date of every video is set(Std format)
- **Start/End Time**: Start and end time of every video is maintained(Std format)
- **Video Name**: Name of every video is being designated(Alphabetic)

Action

- **Action ID**: Specific action ID is given(numeric)
- **Action Name**: Action name is being designated(Alphabetic)

Video

Video has format of **mp4** that is saved in network video recorder (nvr) for offline

Frame/Images

Images shall be in **JPEG** format and frame size of **30** fps

Figure 5. 24 Detailed Subsystem

Chapter 6

6. IMPLEMENTATION & TESTING

The first phase of implementation starts with fetching video dataset. For each video we extract C3D features, that are computed for every segment (16 frames each), along with Euclidean normalization. A single segment score is calculated by taking average of score of frames within a segment. These features are then input into a fully connected neural network with 3 layers, with the first containing 512 units, middle layer comprises of 32 units and last layer with single neuron. First layer implements ReLU activation and Sigmoid activation is used for the last layer. Once a model is trained, we then perform similar steps to extract feature from a test video load the weights of model and other configuration and feed the test video frames into model. Model then calculates scores of these frames which plotted in a graph form. To generate an alarm, we further take the statistical mean and standard deviation of the frame score. The threshold is set as a value equal to standard deviation of all frames. The mean is calculated by segmenting frames into a bracket of 30 frames each. The mean of first 30 frames segment (i.e frame 1 to frame 30) and second frames segment (frames 31 to frame 60) are subtracted and if the resultant difference is greater than threshold, we generate an alarm for anomaly. The final results are displayed as summary in a separate GUI. Furthermore, Admin can manage the users (add and remove), view logs and perform anomaly detection on videos. The testing phase consists of checking for false positive and false negatives. A sample output of false negative is attached as under. The video contains a small blast which is not detected by the system here.

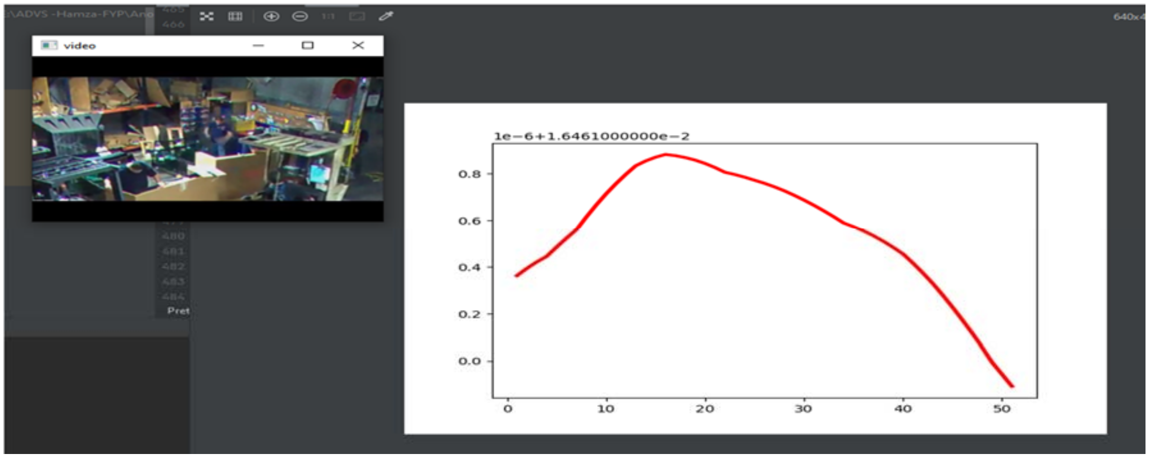
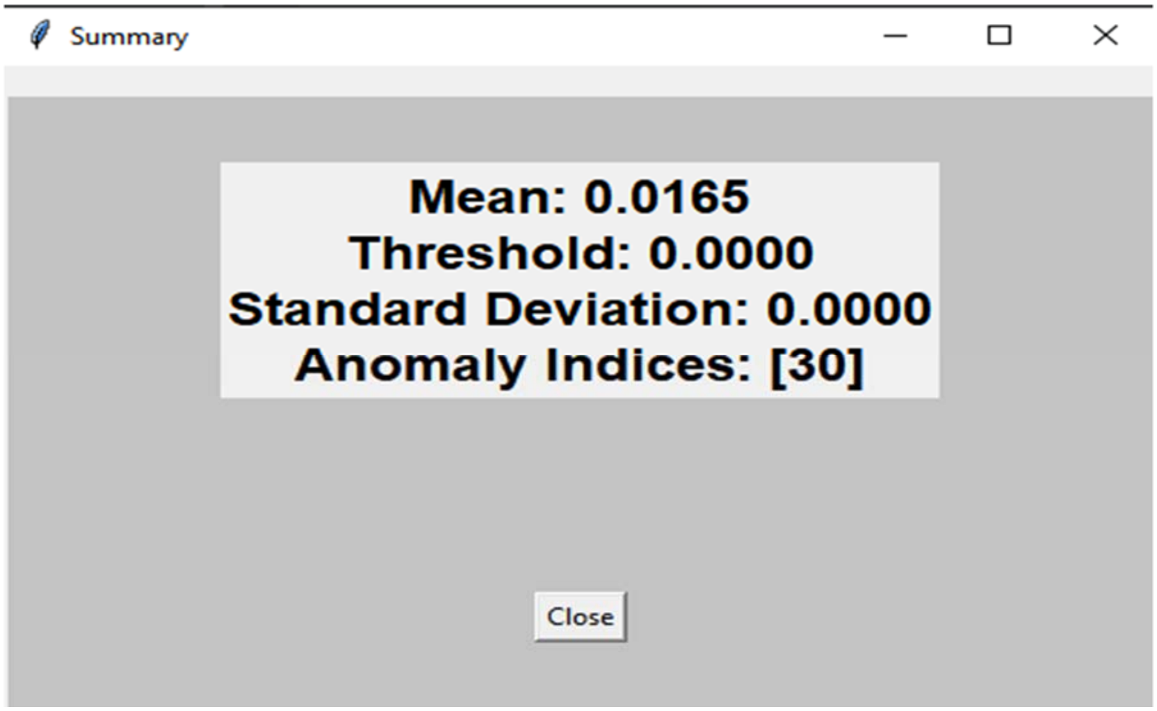


Figure 6. 1 False Negative



Mean: 0.0165
Threshold: 0.0000
Standard Deviation: 0.0000
Anomaly Indices: [30]

Figure 6. 2 False Negative Summary

Chapter 7

7. RESULTS AND DISCUSSION

During the process of training the network to detect abnormal events, it was noticed that after 3,000 iterations, the network began to produce lower scores for normal segments and higher scores for anomalous segments. With more iterations, the network was able to accurately trace the anomaly without needing any segment level annotations.

In real-world surveillance scenarios, the majority of the video footage captured is normal, so it is crucial to have a robust anomaly detection scheme that can minimize false alarms in normal videos. Our method was verified on various videos, and it achieved an accuracy of 75.4%, which is higher than previous implementations. This demonstrates the potential of our approach to improve anomaly detection in practical settings.

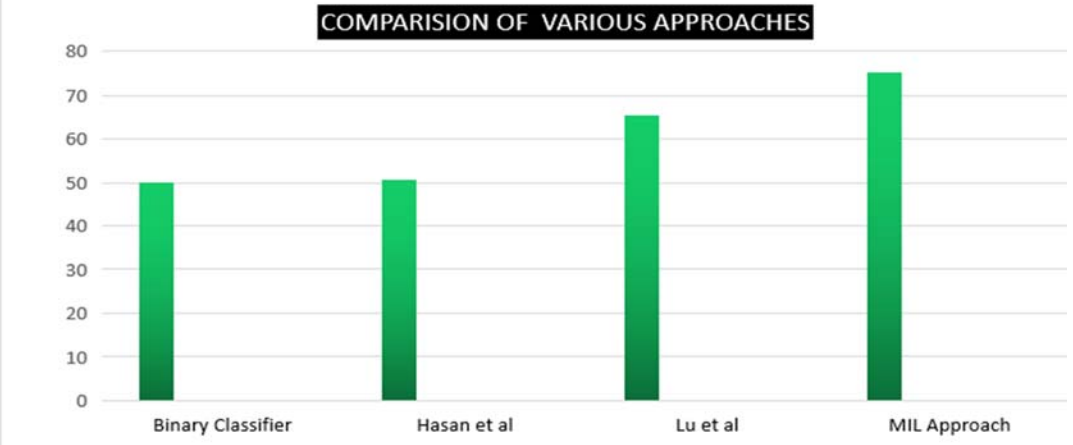


Figure 7. 1 Comparison of Approaches

7.1 Results

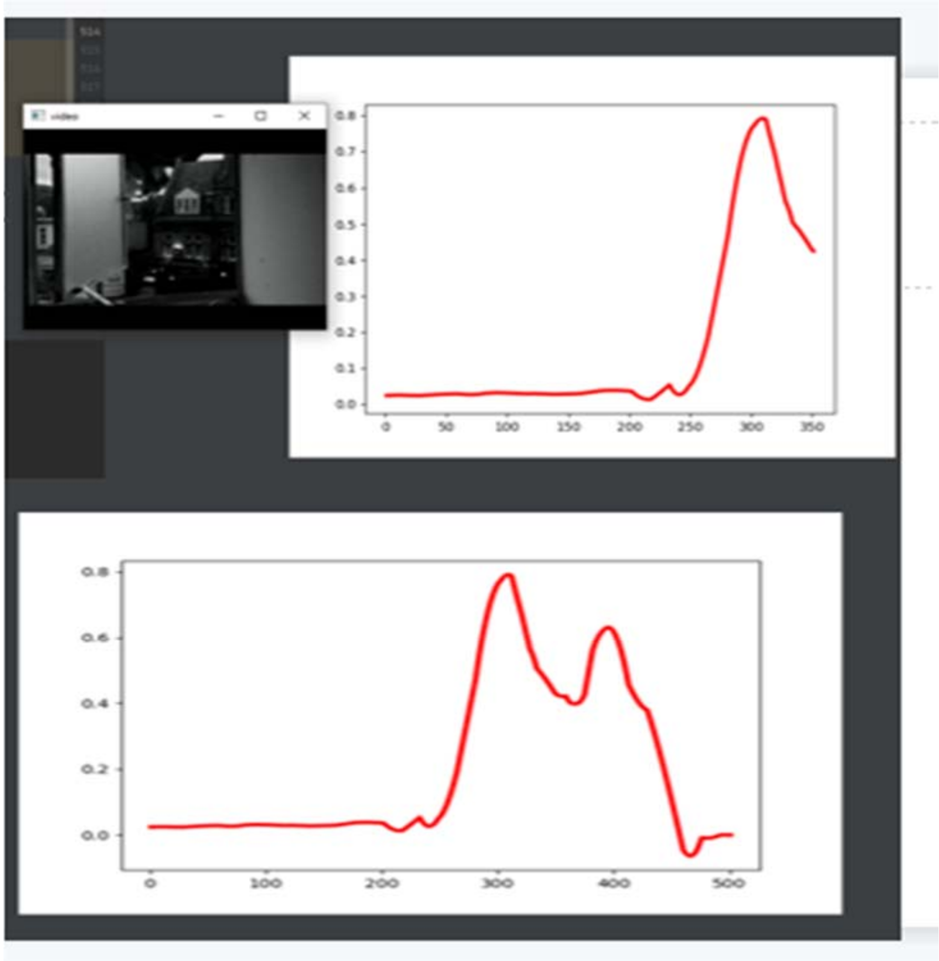
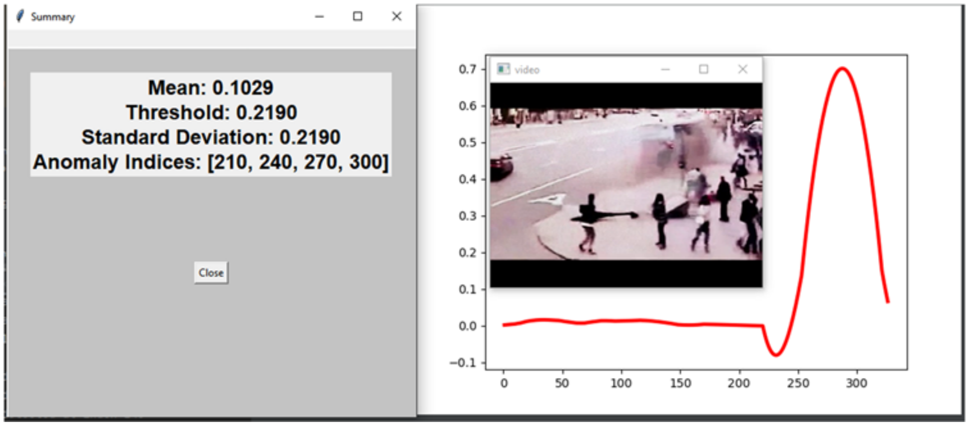
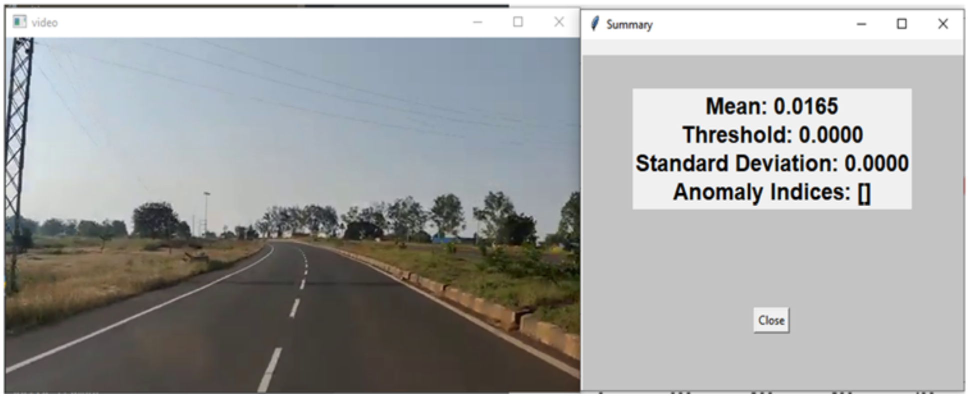


Figure 7. 2 Explosion



Mean: 0.1029
Threshold: 0.2190
Standard Deviation: 0.2190
Anomaly Indices: [210, 240, 270, 300]

Figure 7. 3 Road Accident



Mean: 0.0165
Threshold: 0.0000
Standard Deviation: 0.0000
Anomaly Indices: []

Figure 7. 4 Normal Video

Chapter 8

8. CONCLUSION AND FUTURE WORK

8.1 Conclusion

Anomalous events occur less than normal events in real world surveillance. The surveillance requires continuous monitoring which requires manpower. Therefore, this system helps us in saving time and reducing labor wastage to perform surveillance. Our approach has been trained and tested on 13 different anomalies which most algorithms lack. We have also been able to achieve a higher accuracy result as compared to her approaches. The only drawback of implementation are memory occupation and large dataset that makes the model more complicated and heavy. Detecting anomalous before is also difficult as major chunk of videos are normal and only few anomalous events occur in routine. This requires a balanced acquisition and incorporation new data with anomalous behavior to improve the accuracy. Currently, the system can detect anomalies in live feed but in that case it becomes ineffective and slow due to amplified video processing which result into a high latency.

8.2 Future Work

The system can further be developed to give early warning of anomaly even before it occurs using the existing and new dataset. But this put forwards a challenge of more powerful machine for model training and live detection or giving early warning of anomaly being occurring in environment. The model can be further used to deploy on a live feed, but its latency would increase and for these ways must be found to cater this problem which will also require upscaling of machine, processing power and computational power. This will open an avenue for more lucrative GUI for system as well. Furth more, a more efficient way of manage the memory need to be devised. The system can be integrated among different law enforcement agencies for quick and early response. The system can be used to categorize he type of anomalies or criminal activities acting in specific areas of city or country and thus helping Law enforcement agencies to take appropriate counter measures.

Chapter 9

9. REFERENCES

9.1 Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 6479- 6488).

9.2 Zhou, J. T., Du, J., Zhu, H., Peng, X., Liu, Y., & Goh, R. S. M. (2019). Anomaly net: An anomaly detection network for video surveillance. IEEE Transactions on Information Forensics and Security, 14(10), 2537-2550.

9.3 Ullah, W., Ullah, A., Haq, I. U., Muhammad, K., Sajjad, M., & Baik,S. W. (2021). CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks. Multimedia Tools and Applications, 80(11), 16979-16995.

9.4 https://pubmed.ncbi.nlm.nih.gov/18784010/

9.5 https://www.crcv.ucf.edu/research/real-world-anomaly-detection-in-surveillance-videos/

9.6 https://arxiv.org/pdf/1801.04264v3.pdf

9.7 https://pubmed.ncbi.nlm.nih.gov/23921828/

9.8 https://www.kaggle.com/code/pushkalpandey3/ufc-crime-dataset