

Threatify-Threat Detection using CCTV

FYP Team

Muhammad Abdullah (17I-0038)

Haasha Bin Atif (17I-0183)

Muhammad Ahmed (17I-0184)

Supervised by

Dr. Omer Ishaq

FAST School of Computing

National University of Computer and Emerging Sciences

Islamabad, Pakistan

2020

Contents

1. [Introduction 2](#_Toc54447331)
   1. Vision Statement [2](#_Toc54447335)
   2. Problem Statement [2](#_Toc54447335)
   3. Business Opportunity [2](#_Toc54447335)
   4. Objectives [2](#_Toc54447335)
   5. Project Scope [2](#_Toc54447335)
   6. Constraints [2](#_Toc54447335)
2. [High Level Use Cases 3](#_Toc54447333)
3. [Use Case Diagram 7](#_Toc54447333)
4. Iteration#01 [8](#_Toc54447334)
   1. Expanded Use Cases [8](#_Toc54447335)
   2. Domain Model [10](#_Toc54447335)
   3. SSD [11](#_Toc54447335)
   4. Operation Contracts [12](#_Toc54447335)
   5. Sequence Diagram [1](#_Toc54447335)3
   6. Class Diagram [14](#_Toc54447335)
5. Implementation Details [15](#_Toc54447335)
6. **Introduction**
   1. **Vision Statement: -**

To improve the overall security by providing a fast mechanism for threat detection and classification.

* 1. **Problem statement: -**

We observe criminal activities daily in our lives. Many times, the criminal can escape just because the reporting time was slow. To improve the reporting time of a crime, we are making a deep learning model that can identify and classify criminal activities as threats and report this to the associated organization as soon as possible.

* 1. **Business Opportunity: -**

According to a report [1], “*The physical security market is projected to grow from USD 93.5 billion in 2020 to USD 120.3 billion by 2025*”. Since our solution is generic, this can be used by anyone, it may be a private home or it can even be a big institution. We believe if we provide subscription services, we can get a very good number of customers. Security is a huge concern for everyone, whether it’s a person or a big industry, thus everyone is ready to pay a good price for it.

* 1. **Objectives: -**
* To capture live video feed and send it to the remote server.
* Develop a model that can detect threats and classify threats in minimum time.
* Create a system through which we can notify the user and associated authorities about the criminal activity (after threat is detected).
  1. **Project scope: -**

Our scope includes first collecting a dataset on criminal activities. The dataset must be of videos. Then we have to make a deep learning model and train it on our dataset of threat videos. We then devise a system which automatically sends a threat notification to the user and to the associated organization once the threat is detected. At the very end, we have to develop an application for user, which can be used by the user end for viewing threats observed in the video feed provided by their CCTV.

* 1. **Constraints**
* Very low-quality videos
* Angle of the video
* Resources limitations

1. **High Level Use Cases**

|  |  |
| --- | --- |
| **UC01:** | Registration |
| **Actors:** | Customer |
| **Type:** | Primary |
| **Description:** | The customer clicks register and enters all the credentials. The user enters the total number of cameras. |

|  |  |
| --- | --- |
| **UC02:** | Login |
| **Actors:** | Customer |
| **Type:** | Primary |
| **Description:** | The customer will click login and enter his username and password, and has an option to click on ‘Keep me logged in’ or not. |

|  |  |
| --- | --- |
| **UC03:** | Video Streaming |
| **Actors:** | Customer |
| **Type:** | Primary |
| **Description:** | The client system will be transmitting CCTV feed to the server continuously. |
| **UC04:** | Threat Identification |
| **Actors:** | modelController |
| **Type:** | Primary |
| **Description:** | The system will receive a series of frames from the stream. The system will classify it whether it is a threat or not. |

|  |  |
| --- | --- |
| **UC05:** | Threat Classification |
| **Actors:** | modelController |
| **Type:** | Primary |
| **Description:** | The system receives series of frames. The system classifies it into which type of threat it is i.e. Arson & Explosion, Fighting, Gun Event. |

|  |  |
| --- | --- |
| **UC06:** | Informing User |
| **Actors:** | modelController |
| **Type:** | Primary |
| **Description:** | The system sends notification to the user that threat is detected. |

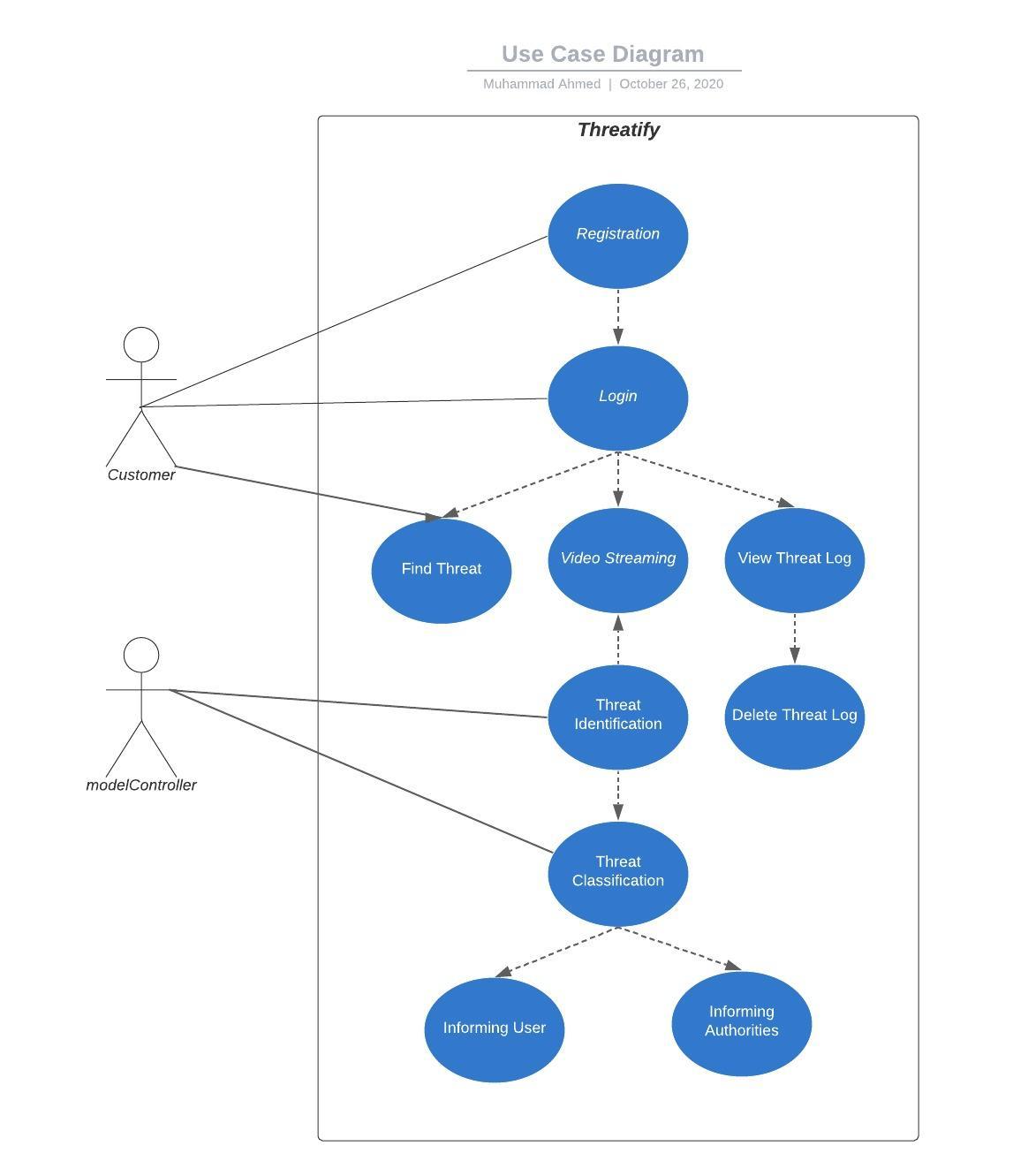
|  |  |
| --- | --- |
| **UC07:** | Informing Associated organizations |
| **Actors:** | modelController |
| **Type:** | Primary |
| **Description:** | The system sends notification to the associated organization e.g. Fire brigade in case of Arson/Explosion event, along with the location of the user. |

|  |  |
| --- | --- |
| **UC08:** | View Threat Log |
| **Actors:** | Customer |
| **Type:** | Secondary |
| **Description:** | The user clicks on view threat log, threat log shows all threats that have occurred in the past along with the clip. |

|  |  |
| --- | --- |
| **UC09:** | Delete Threat entry |
| **Actors:** | Customer |
| **Type:** | Secondary |
| **Description:** | The user clicks on a single entry in threat log and clicks ‘delete’. The entry is deleted from threat log. |

|  |  |
| --- | --- |
| **UC10:** | Find Threat |
| **Actors:** | Customer |
| **Type:** | Primary |
| **Description:** | Customer will request the model controller to find the threat. |

1. **Use Case Diagram**

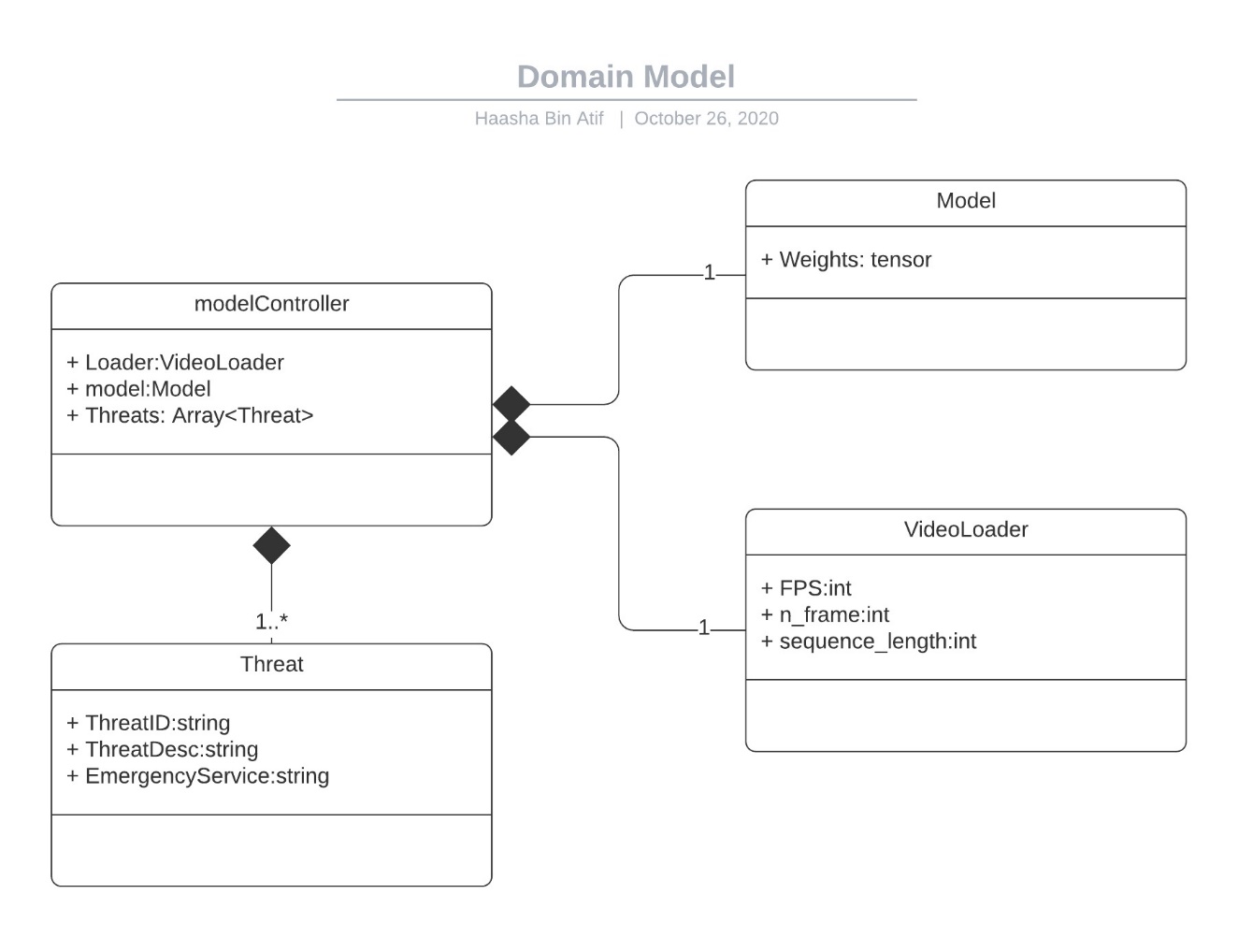


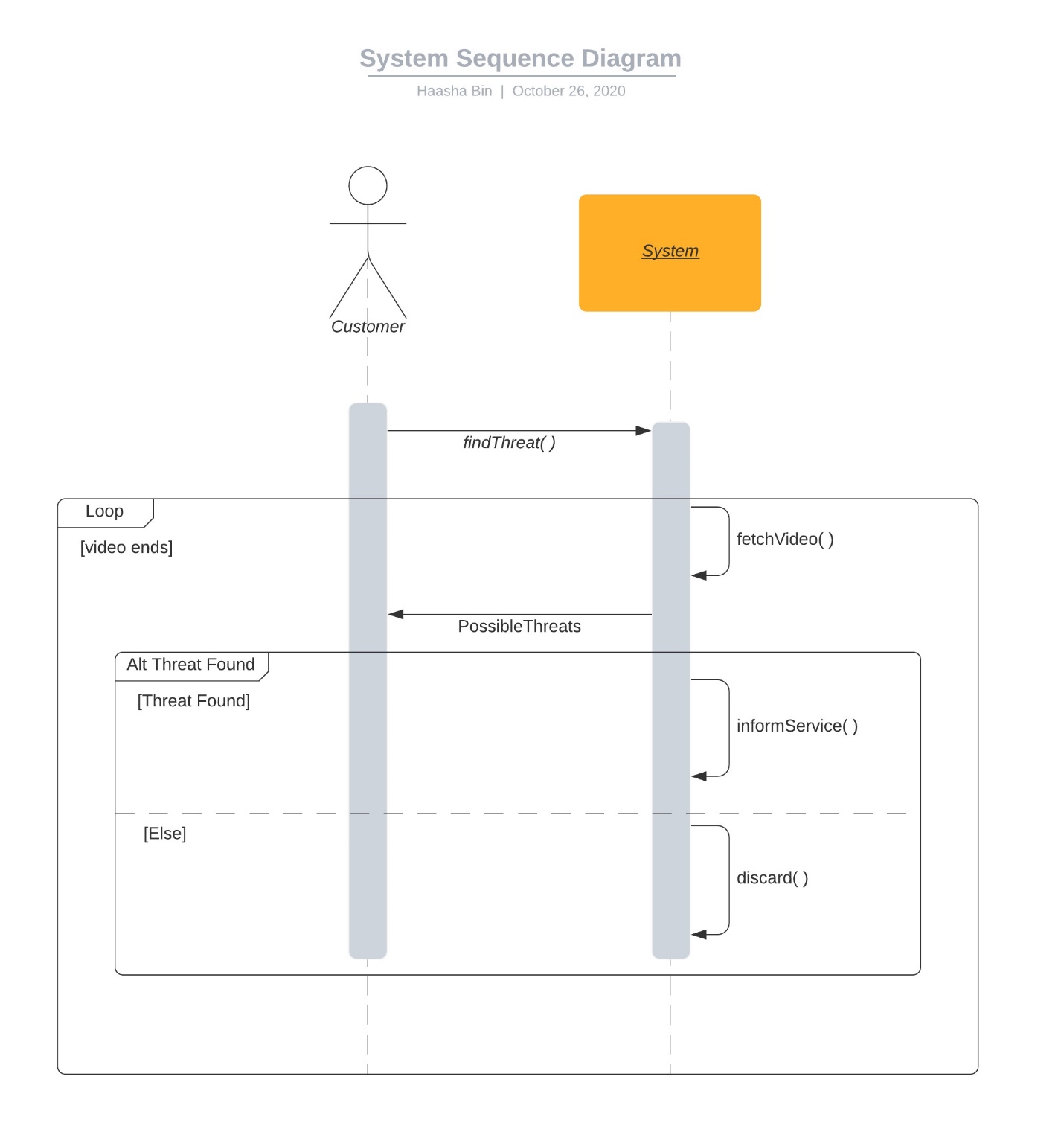
1. **Iteration#1**
   1. **Expanded Use Cases:**

|  |  |
| --- | --- |
| **Section:** Main | |
| **Use case:** Find Threat | |
| **Actors:** Customer | |
| **Purpose:** To find threats which occurred in a video. | |
| **Overview:** The system will have a whole video which it will process and find threats. | |
| **Type:** Primary | |
| **Cross References:**  \* Functions: N/A  \*Use cases: N/A | |
| **Typical Course of Events** | |
| **Actor Action**   1. Customer will request system to find threat. 2. User will select video to be checked. | **System Response**     1. System will prompt user to select video. 2. System will start finding threats in the video and send all possible threats on competition. |
| **Alternative Courses:**  Line 2: If there is no video available, system should throw an error message to the project controller | |

|  |  |
| --- | --- |
| **Section:** Main | |
| **Use case:** Threat Identification | |
| **Actors:** modelController | |
| **Purpose:** Detection of threat | |
| **Overview:** The system will receive a series of frames from the stream. The system will classify it whether it is a threat or not | |
| **Type:** Primary and essential | |
| **Cross References:**  \* Functions: N/A  \*Use cases: Find Threat | |
| **Typical Course of Events** | |
| **Actor Action**   1. Project controller will request the video from the system 2. Project controller will do request to the system to provide result | **System Response**     1. System will fetch video from the server 2. After fetching, system will send videos to the project controller 3. System will inference result after applying Deep learning model 4. System will inform the project controller about the result |
| **Alternative Courses:**  Line 2: If there is no video available, system should throw an error message to the project controller | |

* 1. **Domain Model:**



* 1. **System Sequence Diagram:**
  2. **Operation Contracts:**
     1. **findThreat( )**

|  |  |
| --- | --- |
| **Name** | findThreat( ) |
| **Responsibility** | start finding threat in the video stream |
| **Type** | Customer |
| **Use Case** | Find Threat |
| **Pre-Condition** | Video is selected. |
| **Post-Condition** | Possible threat will be identified |

* + 1. **informAgency( )**

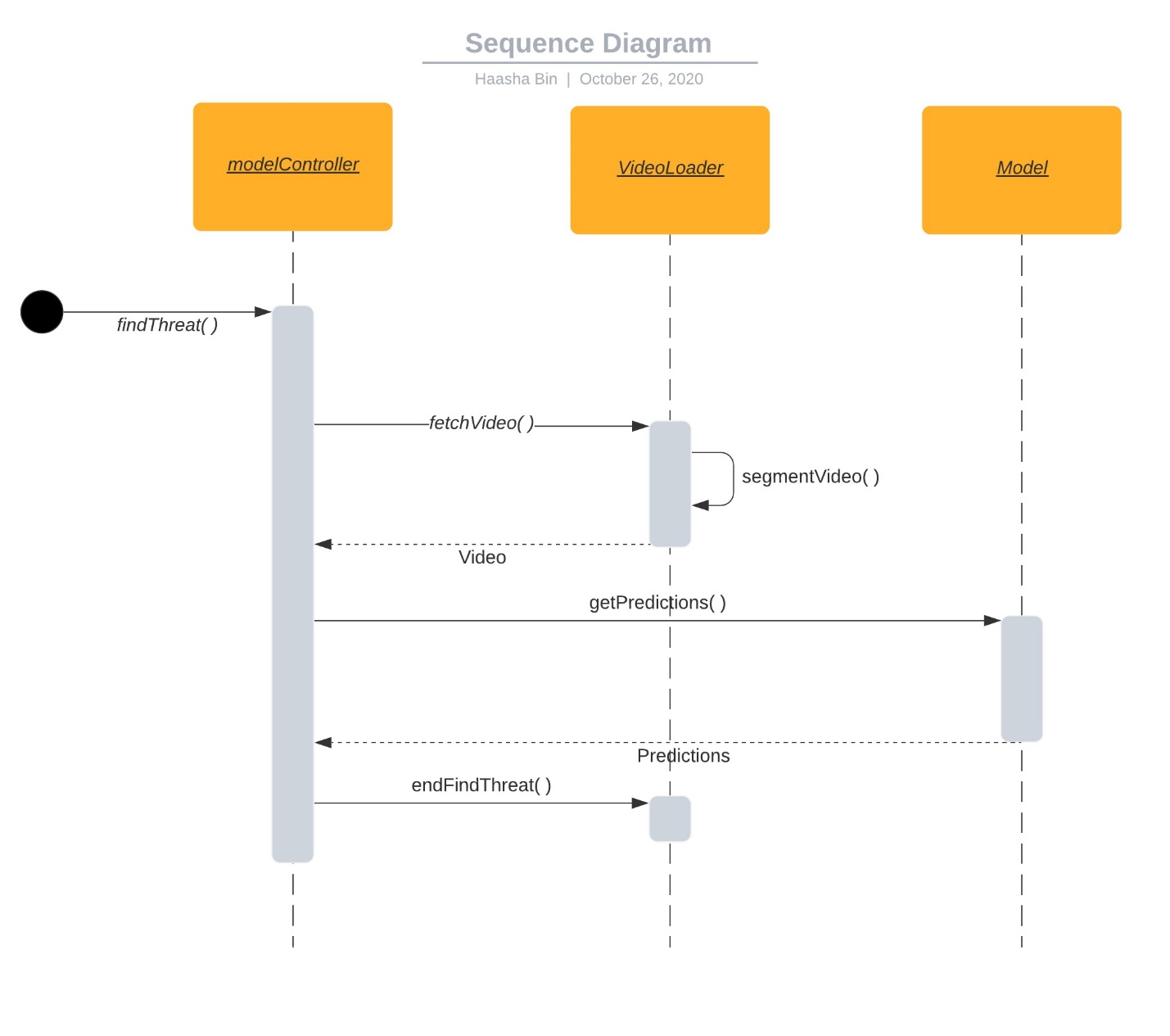
|  |  |
| --- | --- |
| **Name** | informAgency( ) |
| **Responsibility** | To inform the agency about the threat and the location. |
| **Type** | System |
| **Use Case** | inform the agency of crime. |
| **Pre-Condition** | Threat was found first. |
| **Post-Condition** | Corresponding agency would be informed |

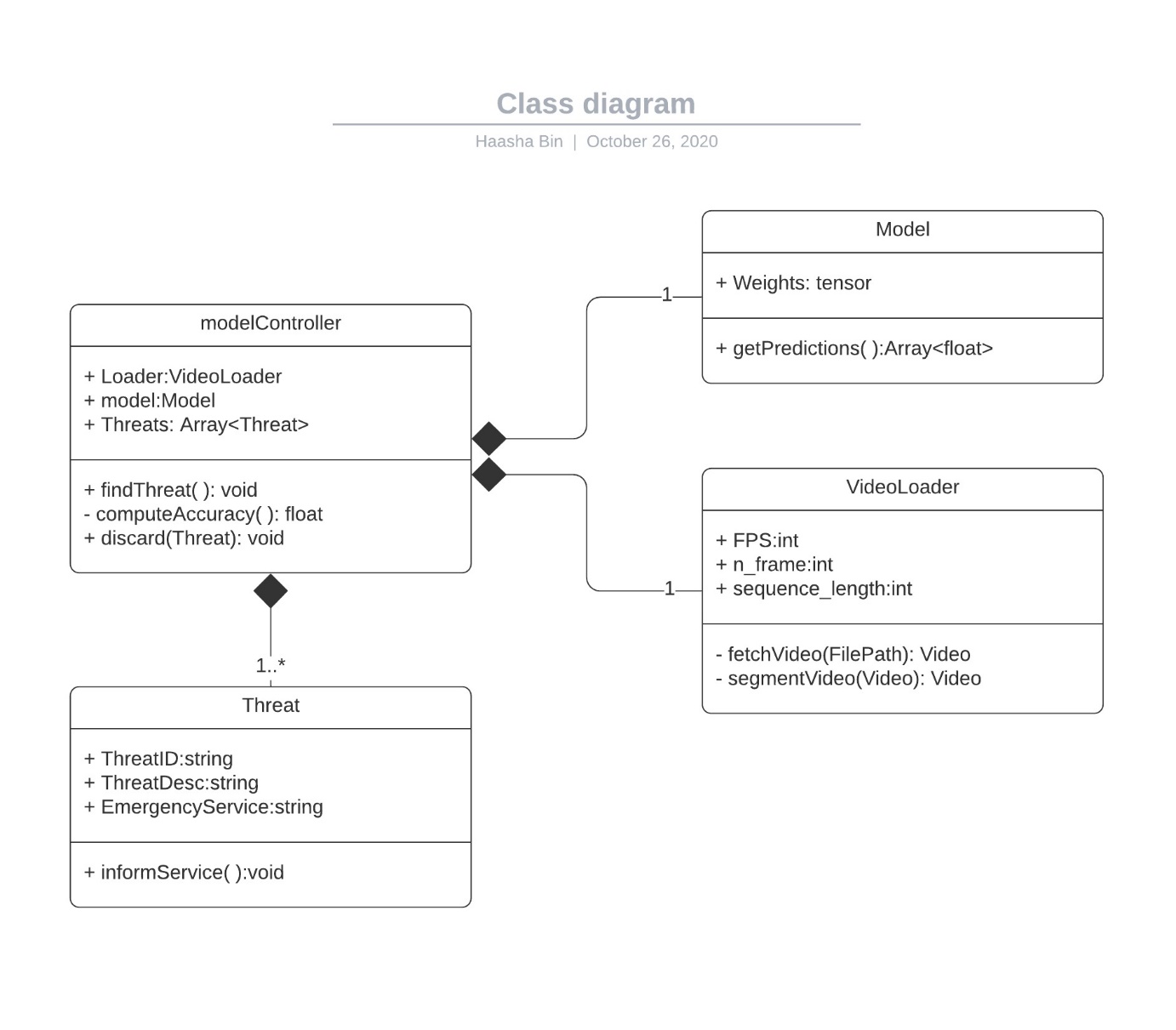
.

* + 1. **discard( )**

|  |  |
| --- | --- |
| **Name** | discard( ) |
| **Responsibility** | To discard any possible threats which were found |
| **Type** | System |
| **Use Case** | discard threats and don’t log them. |
| **Pre-Condition** | The threat found was a false positive |
| **Post-Condition** | The threat alert is discarded and no one is informed. |

* 1. **Sequence Diagram:**



* 1. **Class Diagram:**

1. **Implementation Details:**
   1. **Model Details:**

The model that we are using for threat identification is not constant for now. At the moment, we are using a pretrained VGG16 model as our backbone. Our backbone serves the job of extracting features in frames, then it is sent to some fully connected layers. The data we have is in the form of videos, and to understand the relation between frames, we have 3 blocks of LSTM layer and at last we have 2 blocks of (fully connected & Batch norm) providing us confidence for each class. The optimizer we are using is ADAM and the loss function is Cross entropy.

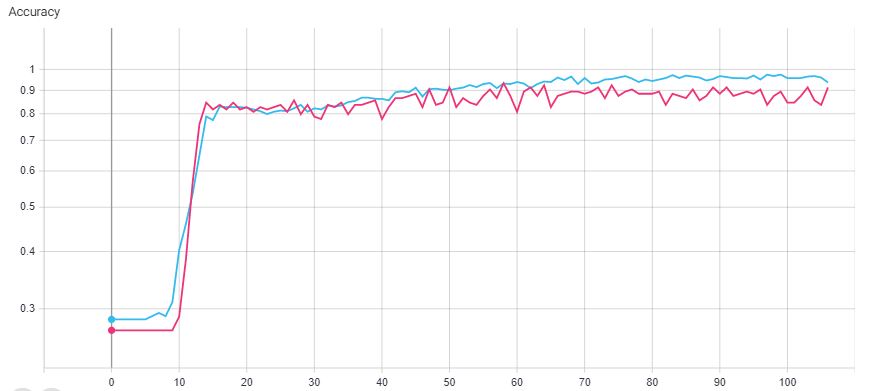
* 1. **Video Segmentation:**

To segment the moving object, we first have to obtain a mask by calculating the difference between 2 consecutive frames by simply subtracting them. We get X number of masks and simply concatenate them (X is a hyper-parameter). This is the mask we use for the 1st frame, then slide ahead by removing the oldest mask and add the latest mask. Once we have a mask against a frame, we multiply the frame with the mask and get the moving area in consecutive frames.

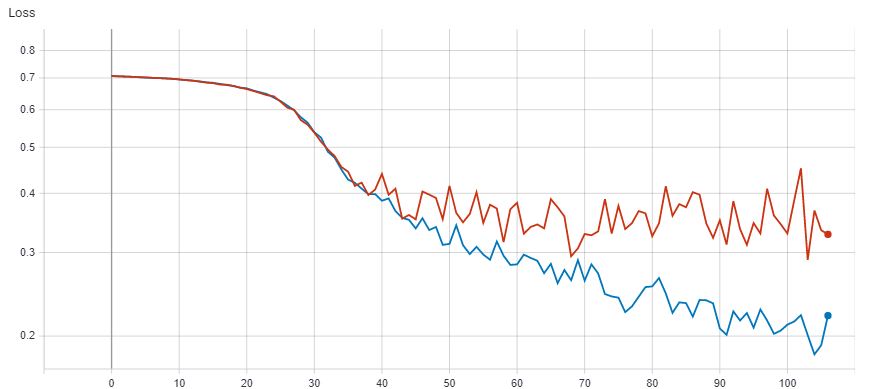
* 1. **Threat Identification:**

For threat identification, we first fetch a video and get it segmented. After segmentation, all we have to do is to pass it to our model, our model returns us the probabilities in form of [Threat, Non-Threat]. We give the label of max probability to a video.

* 1. **Results:**
     1. **Accuracy with Masking:**



* Train Set
* Test Set
  + 1. **Loss with Masking:**



* Train Set
* Test Set

**References:**

[1] https://www.marketsandmarkets.com/Market-Reports/physical-security-market-1014.html

[2] https://github.com/HHTseng/video-classification