Software Requirements Specification

for

Ai Invigilation System

Version 1.0

Prepared by Zicheng Guo, XXXX XX, XXXXXXX XXXX

Department of Computing and Software, McMaster University

Supervisor: Dr. Rong Zheng

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

The AI Invigilation system helps the supervisors of in-person exams by setting up exam timers, detecting and recording suspicious behaviors of examinees during the exams. The system also allows authenticated supervisors to access recorded videos of past exams.

1.2 Document Conventions

Some abbreviations used in this document are defined in Appendix A.

1.3 Intended Audience and Reading Suggestions

The intended audience for this document is the software developers and testers. They will use this document to know the specific set of functional requirements to implement, and design the system. This document also includes environmental requirements indicating OS and hardware. For the testers, they will use it to understand the environment and run tests in it.

This document will be very technical so that the software engineers have clearly laid out measurable features to implement and test the software against.

1.4 Product Scope

The AI Invigilation system helps the supervisors of in-person exams by setting up exam timers, detecting and recording suspicious behaviors of examinees during the exams. For some large-scale examinations, it's hard for the supervisors to pay attention to each and every examinee. At the same time, detecting cheating behaviors usually requires a period of time to observe that specific suspicious examinee, which makes it harder to fairly supervise all examinees. The AI Invigilation system can monitor several examinees at the same time and once their behaviors meet some pre-set criterion, the corresponding examinees will be highlighted with explanations for the supervisors to make further decisions. Besides, the criterions and factors are customizable for different examinations by the supervisors.

The system will store the videos on local machines to reduce disputes in the future.

1.5 References

1. Genemo, M. D. (2022). Suspicious activity recognition for monitoring cheating in exams. Proceedings of the Indian National Science Academy, 88(1), 1–10. https://doi.org/10.1007/s43538-022-00069-2
2. Debnath, Partha & Rashed, Md. Golam & Das, Dipankar. (2018). Detection and Controlling of Suspicious Behaviour in the Examination Hall.

2. Overall Description

2.1 Product Perspective

Currently, most exams are supervised by real human-invigilators. Usually, for an exam with around 300 examinees, only 2-3 invigilators are involved. As a result, many students tend to cheat under such conditions. There are a few similar systems on the market, but they all target online exams or a computerized exam center. Our product will target in-person exams either at a high-level educational institute or professional exam center.

2.2 Product Functions

Before the exam:

- The system shall allow supervisors to log in and authenticate their identities.
- The system shall allow supervisors to input exam information and customize criteria.
- The system shall open a separate window displaying the exam information and a timer based on the previous user input.
- The system shall display a GUI that allows users to start and end sending camera feeds to the BE.

During the exam:

- The system shall display camera feeds on the screen which is the one that only the invigilators can watch.
- The system shall detect suspicious behaviors and highlight suspicious examinees based on the pre-set criteria.
- The system shall display the highlight block border and criterions met near the block.

- The system shall allow supervisors to cancel highlight blocks attached to suspicious examinees.
- The system shall send notifications with reason and show them on the interface once suspicious behavior is detected.
- The system shall record the camera video once the exam is started.
- The system shall display a timeline with texts showing when and what triggers the detection and the system shall also highlight the periods of time on the timeline.

After the exam:

- The system shall end recording automatically at the end of the exam.
- The system shall generate a report including exam information and timestamps of operations (detected suspicious behaviors, cancelled highlighted behaviors, etc.) when the exam is ended.

2.3 User Classes and Characteristics

Supervisors

Supervisors will be the primary user of the system, they will use the system during the exams to display exam information, timer and supervise the exam with the help of suspicious behaviors detection. This user group includes the leading supervisors (for example, the professor of the course or the department staff) and other supervisors (for example, the TAs of the course).

The leading supervisors are more likely to be older than others and within the age range of 30-60. For users within this age range, they are educated and can perform basic software operations. However, it's difficult for them to read small texts, perform complicated operations and especially learn something new. Besides, these users perform operations distinctly slower than others, thus they need longer time to react and respond to information.

Other supervisors are within the age range of 20-40, and they are more adaptive to technology and software. They use technologies almost everywhere and every time in daily life, thus they are more likely to have extensive experiences on using different systems. At the same time, this user group is fast-learner, which means they can easily learn how to operate a new system.

Technical staffs

Technical staff are not the primary user of the system, but they are still relevant because they may need to use the system during equipment setup and maintenance. The staffs are relatively not educated compared with the supervisors and their ages may be various, but they are experienced using systems.

Users of this system are supervisors and technical staff, supervisors are able to start the exam or alter any information related to the exam, the time, the details or the rules of the exam. Technical staff are the only groups of people who have access to download the recording after the end of the exam. Supervisor will have access to the following stated functions, technical staff have access to all the functions.

Examinee

Examinees are tertiary users, they will not directly operate the system and interfaces, but they are the subject of the system.

2.4 Operating Environment

MM environment: A PC with multiple monitors running windows, with enough I/O ports for connecting cameras.

BE environment: A back-end server running Linux with enough computability for the AI model.

WI environment: A modern PC with a browser to access the web interface. The system will operate in the web browser, and it mainly supports services on Google chrome.

2.5 Design and Implementation Constraints

Only available in English: All of our software and manuals will be in English.

No final decision: The system shall not draw any conclusion on suspicious behavior. The system shall only detect and provide relevant footage of examinees whose behaviors meet the pre-set criteria, and act as a reminder to the leading supervisors who are in charge. Since there is no explicit cause-and-effect relationship between the pre-set criteria and cheating, the system shall never draw any conclusions.

No guaranteed runtime: Due to the competitiveness of the AI algorithms, the runtime is strongly dependent on the computability of the back-end server, which means that it may be dramatically slower if using a low level backend. The system will not perform well under such conditions.

2.6 User Documentation

For invigilators, they will be trained to use the system, and the UI guide should be clear enough for them to use the system. Besides, a simple manual will be delivered along with the product just in case.

For technical staff, a system installation and setup manual will be delivered along with the product. The manual will explain how to set up and connect the hardware (such as the cameras).

There should be no documentation needed for examinees.

2.7 Assumptions and Dependencies

- Assume the room that installs the system will have a high-bandwidth stable internet connection.
- Assume the room that installs the system will have enough lighting conditions..
- Assume the room that installs the system will have a screen of any kind in front (projector, TV, etc.)
- Assume the organization/team using the system will have a back-end server with enough computational power to satisfy the time requirements of the system.
- Assume all examinees being monitored agree to take and store their portrait.
- Assume all examinees are valid candidates for the exam, no need of authentication.
- Assume all external communications between technical staff, leading supervisors and other invigilators are safe and remain integrity all the time.
- Assume MM is installed with some kind of PCI-E card or software settings that on each restart the system will detect all files and reset to pre-set status (Is very common in high-level educational institute)

3. External Interface Requirements

3.1 User Interfaces

Front-end

The user interface (the main function of the system for supervisors) on the MM should be web-based that can be accessed via HTTP with a browser.

The user interface that connects to and controls the cameras on the MM should be GUI based.

Back-end

The interface should be command-line-based software.

3.2 Hardware Interfaces

BE: Back-end server can be a bare-metal server or cloud service. It shall have enough GPU power to execute model inference. It can be in the same room as examinees or at any other location with a stable internet bandwidth.

MM: The main machine is required to have at least one monitor, but recommend one monitor for invigilator use while another screen(projector, large screen) to display exam relevant information for examinees. It should have enough I/O port to connect cameras.

WI: There is no particular requirement for WI interface, a monitor or screen of any kind, some put method (mouse, keyboard or touch screen) is enough. A screen size greater than 13 inch is recommended.

3.3 Software Interfaces

Operating system: Using Windows operating system for its best support and user-friendliness.

Web browser: A browser which supports HTML, CSS and Javascript.

Back-end server: All backend code should run with Python 3.9.x, torch 1.13.x, CUDA 11.6 with cudnn.

3.4 Communications Interfaces

To access BE, technical staff shall only use ssh to access the backend.

To communicate between BE and MM, the computer with the software shall have a high bandwidth connection to the BE via TCP/UDP connection.

To access WI, the leading invigilator should use any system with chrome browser to access the web interface.

Communication between backend and frontend shall use HTTP connections.

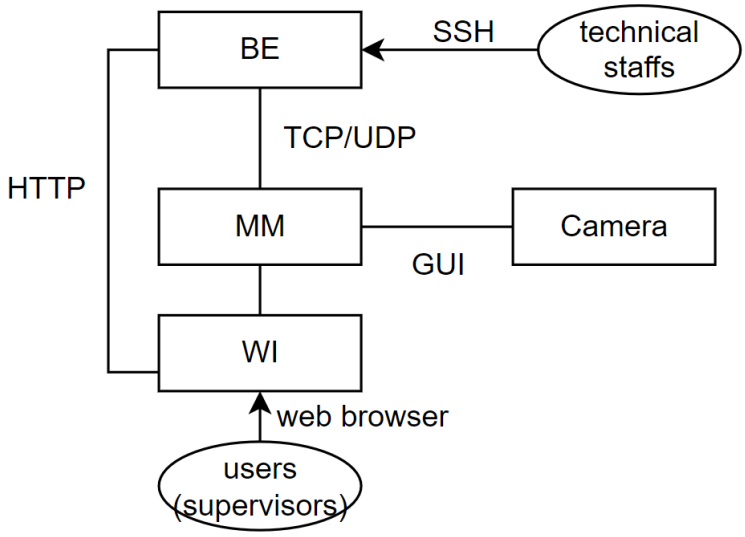

FIG1 - Communication interfaces

4. System Features

4.1 Supervisors authentication

4.1.1 Description and Priority

To ensure only the technical staff have the access to the system, the system shall provide two different auto generated hash code to the leading supervisors and other invigilators whenever an exam starts. The code only supports limited time window access. It is the main function of the software, thus is of high priority.

4.1.2 Stimulus/Response Sequences

The system shall generate hash code 30 minutes before the exam starts, and technical staff will send the auto-generated hash code to the leading supervisors through an external communication app, they will in charge to send it to other invigilators, this code only supports the use of the software in a limited time window, since there could be safety issues regarding the recordings. The code will be sent to the leading supervisors 30 minutes prior to the exam and the software is usable until 30 minutes later at the end of the exam. The supervisors will log-in to the system with the given hash code, the system will authenticate their identities. Once the supervisors are authenticated, they can use the system or access the recordings.

4.1.3 Functional Requirements

- REQ1-1 The system shall generate a hash code which will be valid 30 minutes before the exam starts.
- REQ1-2 The system shall allow technical staff to set the expiry time for the hash code.
- REQ1-3 The system shall send the generated hash code to technical staff.
- REQ1-4 The system shall complete the hash code generation and sending process in 1 min.
- REQ1-5 When the user tries to access the website, the system shall display a log-in page within 3s.
- REQ1-6 The system shall authenticate the user within 5s.
- REQ1-7 The system shall redirect authenticated users to the main page.
- REQ1-8 The system shall display an error message ("wrong code") and require users to re-enter the code if the system failed to authenticate the user.
- REQ1-9 The system shall display an error message ("expired code") and require users to re-enter the code if the code is expired.

4.2 Suspicious Behavior Detection

4.2.1 Description and Priority

Once the supervisor starts the exam, the system will detect suspicious behavior of the examinee and flag an examinee if the pre-set criteria are met. It is the main function of the software, thus is of high priority.

4.2.2 Stimulus/Response Sequences

Once the exam starts, the backend shall also start the suspicious behavior detection function. When one frame is sent through the algorithm, they have been passed to multiple computer vision models, which will be responsible for different trigger flags. If any suspicious behavior is detected, a warning message will be displayed on the WI with the reason why that is triggered. And the time stamp and that frame will be output to a log. The whole recording from the camera(s) will be saved on MM for invigilators to make backup.

4.2.3 Functional Requirements

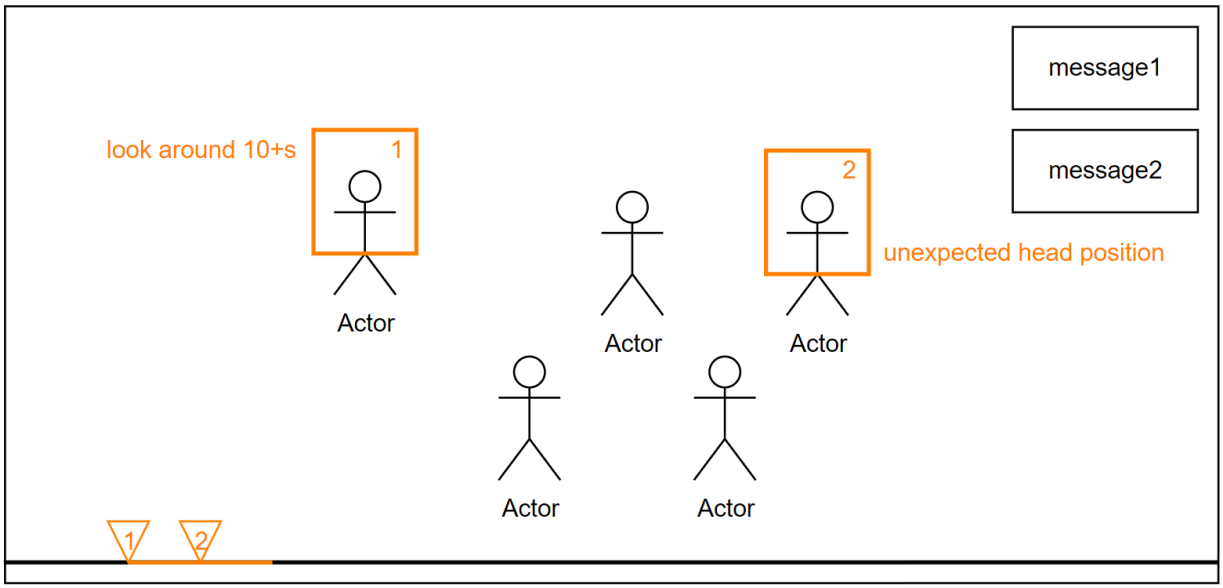

FIG2 - Suspicious behavior detection feature

- REQ2-1 The system shall display the camera feeds in the user interface.
- REQ2-2 The system shall start recording the camera video within 5s once the exam is started.
- REQ2-3 The system shall send camera feeds to the backend within 5s once the user starts the exam.
- REQ2-4 The system shall apply models to the captured feeds and detect any suspicious behaviors based on the pre-set criteria.
- REQ2-5 The system shall display the highlight block border and triggered criteria around the examinees who are detected as suspicious.
- REQ2-6 The system shall allow supervisors to select and cancel highlight blocks attached to suspicious examinees.
- REQ2-7 The system shall remove the highlight block and text once the suspicious detection is canceled in 3s.
- REQ2-8 The system shall send notifications including time and triggered criteria, and show it on the interface once suspicious behavior is detected in 5s (since the suspicious behavior is detected).
- REQ2-9 The system shall display a timeline with tags showing when and what triggers the detection and the system shall also highlight the periods of time on the timeline below the camera video.
- REQ2-10 The system shall display the triggered criteria when the user places the curser on the tag.
- REQ2-11 The system shall stop sending camera feeds to the backend within 5s once the user ends the exam.
- REQ2-12 The system shall stop recording the camera video within 5s once the exam is ended.
- REQ2-13 The system shall save the recording to the pre-set path on the local machine at user-set intervals (to prevent extremely large files).
- REQ2-14 The BE shall save each frame it received as a backup if anything uncontrollable happened in MM.

4.3 Exam Management

4.3.1 Description and Priority

The system shall allow the leading supervisors to input exam information, setup timer, change the rules and add any specification about the exam. This feature will help invigilators manage the exam, this feature has medium priority.

The system shall also allow supervisors to customize pre-set triggers that the system will detect suspicious behaviors depend on. The suspicious behavior detection is based on these pre-set criteria, thus this feature is of high priority.

4.3.2 Stimulus/Response Sequences

Before starting the exam, the leading supervisor can choose if he/she would like to display relevant information on the projector. If so, he/she will enter exam information, such as length, timer, etc. Then, the system shall pop up a separated window displaying all relevant information, and the supervisor can display it via another screen or projector.

Besides, the invigilator shall be able to enable/disable or customize different flags that can trigger the detection before the exam. The system will use these flags as the definition of "suspicious behavior" in the exam.

4.3.3 Functional Requirements

- REQ3-1 The system shall only allow the authenticated leading supervisor (empowered by the code given from the technical staff which is different from the normal invigilators) to change or set detection criteria.
- REQ3-2 The system shall display a form for supervisors to enter exam information.
- REQ3-3 The system shall pop up a separate window displaying exam information within 2s once the user clicks the "display information button" on the web interface.
- REQ3-4 The system shall display a panel for supervisors to enable/disable or customize different flags.
- REQ3-5 The system shall apply the flags (also called pre-set criteria) to the BE within 10s once the supervisor makes any change.

4.4 Generating report

4.4.1 Description and Priority

The system shall generate a report including exam information and timestamps of operations (detected suspicious behaviors, cancelled highlighted behaviors, etc.) when the exam is ended. This is of low priority.

4.4.2 Stimulus/Response Sequences

After the supervisor ends the exam, the system will generate a text file including every event that happened during the exam in a format of "timestamp - operations". Then the system will save the text file in the same path as the exam recordings but in a different directory.

4.4.3 Functional Requirements

- REQ4-1 The system shall generate a text file including every event that happened during the exam in a format of "timestamp - operations" in 10s once the exam is ended.
- REQ4-2 The system shall save the text file to the pre-set path on the local machine.

4.5 Streaming camera feeds

4.5.1 Description and Priority

The system shall display a GUI that allows supervisors to control (start and end) the stream of camera feeds to the BE and MM. This is of medium priority.

4.5.2 Stimulus/Response Sequences

During the exam preparation period, the supervisors will start the stream of camera feeds via a GUI on MM. Then, the system shall send the captured videos to the BE for analysis. After the exam, when the supervisors stop streaming, the system shall stop sending the videos.

4.5.3 Functional Requirements

- REQ5-1 The system shall display a GUI that allows users to choose "start streaming" or "stop streaming".
- REQ5-2 The system shall start sending camera feeds to the BE once receive the user input "start streaming" within 3s.
- REQ5-3 The system shall stop sending camera feeds to the BE once receive the user input "stop streaming" within 3s.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

With a consumer-level back-end setup (Gen 10 or later I7 process or equivalent, RTX 3070 or later GPU or equivalent), our model should process at least 5 frames per second. Enterprise-level

setup(Enterprise level data center CPU with A100 or similar product) will expect a much higher processing speed, at least 10 - 15 frames per second.

5.2 Safety Requirements

- No significant negative consequence to any valuable asset.
- No access to the user's personal financial information nor give permission to use it.
- Each invigilation team has to log in to the app with a valid hash code generated by the system.
- System shall not cause system or software crashes under normal circumstances. Except for human uncontrollable factors like natural disasters, bitflips etc.
- If the MM crashes, there won't be any video clips stored on the local machine, but there are still frames stored in the BE, we can still extract the frames out to fill up the holes.

5.3 Security Requirements

- For the user identity authentication, the system shall generate RSA256 or a similar level of security level hash codes.
- The system models used in the back-end server shall be secure, which means the camera's feed will not be revealed or sent to any third parties.
- The system shall not allow any unauthenticated users to access the video recordings.

5.4 Software Quality Attributes

- Availability: the user-end should be available at least 30 minutes earlier than the specific exam time and also need to be available for the re-play after the exam until the invigilation team makes sure everything is ok.
- Performance: The model should give a decision(whether the behavior is suspicious or not) and pass the message to invigilators to warn them right away, the model shall not make any decision(whether the examinee are cheating or not), they need to let the invigilation team decide.
- Security: No significant negative consequence to any valuable asset, our BE does not associate with any database.
- Usability: User-end interface should be quite easy to use, with only a few options provided with quick responses, the warning message provided should be quite concise and accurate.

5.5 Business Rules

The recording made by this product is only available to the supervisor or technical staff of the organization using the system, the development team does not have access to them. The supervisor is responsible for making copies and deleting the recordings if the system will not reset after the system restarts.

6. Other Requirements

<Define any other requirements not covered elsewhere in the SRS. This might include database requirements, internationalization requirements, legal requirements, reuse objectives for the project, and so on. Add any new sections that are pertinent to the project.>

Appendix A: Glossary

MM: The main machine is a PC with multiple monitors running windows, and it will be used as the primary monitor for supervisors.

BE: The back-end server running the AI models analyzing captured camera videos.

WI: The web interface that is used to access the system.

Supervisor: Leading invigilator of the examination.