Hazard Analysis
Hairesthetics

Team 18
Charlotte Cheng
Marlon Liu
Senni Tan
Qiushi Xu
Hongwei Niu
Bill Song

April 2, 2023

Table 1: Revision History

Date	**Developer(s)**	**Change**
Oct 11	All	Initial Draft
Jan 13	Marlon Liu	Change based on reviews
Apr 2	Hongwei Niu	Resolved problems according to feedback
...	...	...

Contents

List of Tables

1 Introduction

This document provides the hazard analysis of the Hairesthetics application. Hairesthetics is an application that simulates 3D hairstyles. The definition of a hazard used throughout this document is based on Nancy Leveson's work. A hazard is any property or condition of Hairesthetics that has the potential to result in a loss in the system when paired with a condition in the environment. In Hairesthetics, there are hazards in safety (storing data), and security (restricting access to data).

2 Scope and Purpose of Hazard Analysis

The scope of this document is to state any critical assumptions about the project, as well as to identify possible hazards within the system components, the effects and causes of failures, mitigation steps, and resulting safety and security requirements.

3 System Boundaries and Components

The system referred to in this document that the hazard analysis will be conducted on consists of:

1. The ~~iOS~~ web application including both the front-end and back-end made up of the following four major components:
    - Facial Recognition System
    - Hair Modification System
    - Hair Salon Recommendation System
    - ~~Authentication System~~
2. User Device, ~~iPhone~~
3. ~~MongoDB database where all data will be stored~~
4. ~~Cloud database backup programs~~

The system boundary in this case includes the entire application, user device, ~~the database, and the data backup program.~~ The user device and cloud hosting, hardware, ~~and down-time of the database~~ are elements that are not controlled by this project. The user device is controlled by the user ~~and portions of the database are controlled by MongoDB~~. However, they are still critical elements of the system and were thus included in this hazard analysis.

4 Critical Assumptions

The application will be tested on ~~Apple-provided iPhone simulators as well as developers' devices (iOS 14 and above)~~ different browsers using different devices. It is assumed that all physical devices are in good condition to be used under good internet condition for the project and if the application is compatible with ~~Apple-provided iPhone simulators, then it is compatible and functions properly on actual iPhones with iOS 14 and above~~different browsers.

The scope and specifications of the project will not change when the project takes place. However, when conducting the project, there might be cases where the scope and specifications need to

be altered to cater to clients' requirements and needs of the project.

~~The data will be automatically updated in the database, and all information in the database is synchronized.~~

5 Failure Mode and Effect Analysis

5.1 Hazards out of scope

The out of scope hazards falls into the following categories:

- User's Camera
- User's mobile phone hardware
- ~~ArKit~~AR library

User side's hardware conditions is something that the team does not have control over. Besides, the ~~ArKit~~ AR library is also out of the scope since it is a third party library. The hazards can not be handled completely through our development, however we will try our best to minimize them.

5.2 Failure Mode and Effect Analysis Table

The failure modes & effects analysis (FMEA) was chosen as a tool to identify and analyze the hazards within the system so that requirements can be made to mitigate them.

[Include your FMEA table here —SS]

Component	Failure Mode	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
Facial Recognition System	The facial landmarks aren't computed properly	Inaccurate simulation results	User might not input proper image / video	Ask the user for inputs again	~~FR5,~~ ~~FR6~~ IR6	H1-1
	System Crash	~~Overall application crash~~ Inability to use the facial recognition feature	Model execution failure	~~Display error message to prevent further actions~~ Display error message, log the error, and prompt the user to try again or contact support	~~RAR1~~ IR7	H1-2
Hair Modification System	Failed to load hairstyle models	Virtual hair simulation won't appear on the screen	~~Database failure~~ File not exist, incorrect file format, file broken	~~Backup data or reboot~~ manually check the file validity and replace if it's in bad condition according to error message	~~HM6~~ IR7	H2-1
	Algorithm failed to detect hair coordinates	User's hair color fails to change as selected Hair coordination data failed to be retrieved.	~~Hair coordination data failed to be retrieved.~~ Facial recognition system crash	~~Refer to H1-1~~ Refer to H1-2	~~HM3~~ ~~HM4~~ IR7	H2-2
Hair Salon Recommendation System	~~Failed to compute recommendations, Invalid user input~~ Location not found	~~User gets no recommendation and lose interests~~ User gets no recommendation based on their location	~~Database failure~~ Invalid location input or location not in the database	~~Inform user to try again~~ Inform the user to input a valid location or try a nearby location	~~HR2~~ IR1, IR2	H3-1
	System freeze or crash	system crash or overall application crash	~~Database failure~~, ~~Invalid user input~~ workers	~~Backup data or reboot~~ reboot	~~HR1,~~ ~~SLR1~~ IR7	H3-2

Component	Failure Mode	Effects of Failure	Causes of Failure	Recommended Action	SR	Ref
~~Authentication System~~	~~User can not login to the app~~	~~User can not use the functionality of the application~~	~~Login credentials do not match the records in the database~~	~~Inform user to try again or reset credentials~~	~~AR1~~	~~H4-1~~
	~~System failed to use the default camera with the device~~	~~The application can not be used since there's no input source~~	~~User denied the access of the camera.~~ ~~The device has no proper camera system.~~	~~Prompt the user to allow camera access.~~ ~~Try another device with a valid camera.~~	~~AR2~~ ~~AR3~~	~~H4-2~~
General	App crashes unexpectedly	User loses the current progress	The device runs out of battery. The application crashes due to instability.	Charge the device. Reboot and restart the app.	~~RAR1~~ ~~RAR2~~ IR7	H5-1
	Failed to save the images locally	The user won't have the simulation result	User denied the system access to the local storage. The local storage is full.	Prompt the user to allow access to local storage, Prompt users to clear up local storage before retrying	~~AR2~~ IR1, IR2, IR7	H5-2

Table 3: Failure Mode and Effect Analysis Table

6 Safety and Security Requirements

Requirements that have been included in Revision 0 of the Software Requirements Specification document are written in **bold**.

6.0.1 Access Requirements

ACR1: **Users will be able to access images they previously stored.**

Rationale: Allowing users to access their previously stored images will enable them to track their hair styling choices and preferences over time.

Hazard: Unauthorized access to users' stored images, leading to privacy breaches and potential misuse of personal data.

ACR2: **Admins will be able to unlock locked resources.**

Rationale: Admins should have the capability to unlock locked resources to resolve access issues and ensure smooth application functioning.

Hazard: Unauthorized or malicious admin actions, leading to potential compromise of data integrity and application stability.

ACR3: **Only admins will be able to modify application information.**

Rationale: Restricting application information modification to admins prevents unauthorized changes and maintains application stability.

Hazard: Inadequate admin access controls, leading to unauthorized modifications and potential application vulnerabilities.

ACR4: **Users will be able to access the history of the hairs they chose.**

Rationale: Providing users with access to their hair choice history allows them to review and make better-informed decisions about their preferences.

Hazard: Unauthorized access to users' hair choice history, leading to privacy breaches and potential misuse of personal data.

6.0.2 Integrity Requirements

IR1: **The product will not modify data unnecessary.** The product will not touch or modify data/objects in the local storage.

Rationale: Ensuring that the application does not modify unrelated data or objects maintains data integrity and prevents unintended consequences.

Hazard: Unintentional data modification, leading to data corruption and application instability.

IR2: **The product will not modify any data unrelated to its execution.** The product will only access local storage for saving images, will not modify other data.

Rationale: Restricting the application to only modify data related to its execution ensures data integrity and prevents unauthorized access.

Hazard: Unintended data modification or access, leading to data breaches and application instability.

IR3: ~~**Data will be automatically backed up daily.**~~

IR4: ~~**Unsaved data will be stored locally on the user's device if it cannot be uploaded to the remote da**~~
The data will only be saved in local storage upon users' requests.

Rationale: Saving data to local storage only when requested by users ensures data privacy and control over personal information.

Hazard: Unauthorized data storage, leading to potential privacy breaches and misuse of personal data.

IR5: All locked resources will be unlocked once the user sends the request to admins and admins approves the request.

Rationale: This process ensures that access to locked resources is granted only after proper authorization and review by admins.

Hazard: Inefficient or unauthorized unlocking of resources, leading to potential data breaches and application vulnerabilities.

IR6: The application will execute fully functionally

Rationale: A fully functional application ensures user satisfaction, maintains data integrity, and prevents application errors.

Hazard: Application malfunction or failure, leading to potential data corruption, loss, and user dissatisfaction.

6.0.3 Privacy Requirements

PRR1: **Users will not be able to access data generated by other users.**

Rationale: Restricting users from accessing data generated by others maintains privacy and prevents unauthorized access to personal data.

Hazard: Unauthorized access to other users' data, leading to privacy breaches and potential misuse of personal data.

PRR2: **Users will be required to register and login to the application with their emails.**

Rationale: Requiring users to register and log in with their email addresses establishes unique user identities and helps maintain data privacy.

Hazard: Unauthorized access to user accounts and personal data, leading to privacy breaches and potential misuse of personal

PRR3: Admins will not able to access data generated by other users.

Rationale: Restricting admin access to user-generated data maintains user privacy and ensures a trustful environment.

Hazard: Unauthorized access by admins to users' data, leading to privacy breaches and potential misuse of personal data.

6.0.4 Audit Requirements

AUR1: **Requirements should be easy to read and verify against the system facilitate regular inspections.**

Rationale: Clear and easily verifiable requirements ensure that the application's compliance with these requirements can be regularly inspected, resulting in a more secure and stable product.

Hazard: Ambiguous or hard-to-verify requirements, leading to inadequate inspection, potential non-compliance, and application vulnerabilities.

6.0.5 Immunity Requirements

N/A

7 Roadmap

The hazard analysis resulted in new safety and security requirements given in section above. A number of the requirements will be implemented within the capstone timeline such as ACR1, ACR3, IR1, IR2, IR4, PRR1, PRR2, PRR3, AUR1. However, some of them will not, due to project time constraints, such as ACR2, ACR4, IR3, IR5. These will be implemented in the future. Towards the end of the project, the hazard analysis will be consulted to gain an understanding of which risks have been successfully mitigated and which one sill require work.