Software Requirements Specification

for

Multimodal Biometrics

Version 3.5

Brian Tan

Davina Doran

Fulya Kocaman

Konnor Gutierrez

California State Fullerton

CPSC 362 SOFTWARE ENGINEERING

09/28/2020

Table of Contents

Revision History

Name	Date	Reason for Changes	Version
Fulya Kocaman	9/28/20	Created	1
Fulya Kocaman	9/30/20	Changed iris and hand scans to retinal and palm	2
Konnor Gutierrez	10/3/20	Moved to Google Docs for Version Control	3
Fulya Kocaman	10/3/20	Added user cases with detailed info	3.1

Konnor Gutierrez	10/3/20	Added a user case with detailed info	3.2
Davina Doran	10/3/20	Added a user case with detailed info	3.3
Brian Tan	10/4/20	Added a user case with detailed info	3.4
Fulya Kocaman	10/4/20	Finalized formatting in a Word Doc	3.5

1. Introduction

The aim of this document is to gather and analyze and give an in-depth insight of the complete **Multimodal Biometrics Recognition System** by defining the problem statement in detail. Nevertheless, it also concentrates on the capabilities required by customers and their needs while defining high-level product features. The detailed requirements of the **Multimodal Biometrics Recognition System** are provided in this document.

1.1 Purpose

The purpose of this Software Requirements Specification (SRS) document is to provide a detailed overview of our software product which is a system that uses multimodal biometrics recognition system that can be customized based on the usage requirements, its parameters and goals. This document describes the project's target audience and its user interface, hardware and software requirements. It defines how our client, team and audience see the product and its functionality. Nonetheless, it helps any designer and developer to assist in software delivery lifecycle (SDLC) processes.

1.2 Scope

Since biometrics has become a key technology for identity management and security, the U.S. Army has growing need to improve access control of its many systems, both in wartime and in peacetime. [1]

- This project’s goal is to use multimodal biometrics recognition systems that can be customized based on the usage requirements to provide access to secure locations/rooms/systems for authorized personnel in military facilities.
    - The advantage of multimodal over single modal biometrics is that if fingerprint or voice recognition fails, a retinal scan, face recognition or palm scanning could still produce a match to validate that individual.
    - The multiple biometric modalities improve the accuracy of identification and to cope with people in the army that are missing a finger, or have disability problems that prevent use of retina or face recognition.[3]
    - Military security is crucial, so multimodal biometric systems are very difficult to spoof as compared to unimodal systems. Even if one biometric modality could be spoofed for example fingers made of gelatin, contact lenses, etc., the individual can still be authenticated using the other biometric identifiers.

- Another aspect of this project is to make biometrics completely contactless for hygienic reasons due to the COVID-19 pandemic.
    - Instead of touching a pad for fingerprint and palm scanning of personnel, cameras and microphones will capture their retinal, face scans and/or voice in a matter of seconds without an operator present in the screening area.
    - This project also aims to make facial recognition technology more advanced by including masked face detection and recognition technology.
- However, the mobile application of this multimodal biometrics system will be outside the scope of this project.

1.3 Definitions, Acronyms, and Abbreviations

Spoofing	The act of fooling biometric systems to either impersonate someone else, or falsely go undetected. Sometimes achieved with false biometrics
COVID-19	Coronavirus disease 2019
CISO	Chief Information Security Officer
CAC	Common Access Card. A smart card about the size of a credit card used as the standard identification for Active Duty United States Defense personnel
Environment Types	**Severe** - Environments considered abnormal or dangerous, and in climates that cannot be controlled. **Normal** - Everyday environments that civilians could interact with, and is temperature controlled.

1.4 References

The references used in this document are:

[1] https://www.rand.org/pubs/monograph_reports/MR1237.html
[2] https://neurotechnology.com/megamatcher-large-scale-AFIS-and-biometric-identification-systems.html
[3] https://en.wikipedia.org/wiki/BioAPI
[4] https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/

1.5 Overview

The remaining sections of this document provide a general description, including characteristics of the users of this project, the product's hardware, and the functional and data requirements of the product.

- Section 2 contains General description of the project.
- Section 3 gives the functional requirements, design and implementation constraints and assumptions made while designing the multimodal biometrics. It also gives the user viewpoint and the specific requirements of the product.
- Section 4 is for external interface requirements.
- Section 5 is for detailed description of non-functional requirements such as performance, security, cost, time and much more.
- Section 6 is for other requirements.

2. Overall Description

The customers and stakeholders of this project are U.S. Military, defense contractors, the CISO and their IT staff who are responsible for monitoring, running and supporting the Biometric system technologies. Here is the overall list that illustrates their needs and wants:

The objectives of the system are to:

- Have a system that uses multimodal biometrics recognition system that can be customized based on the usage requirements.
- Provide access to secure locations/rooms/systems for personnel who are authorized to be there.
- Reduce instances of intrusion
- Avoid redundancy in authorization

The things that need to be accomplished are to:

- Increase security through the use of unique identifiers (**retina**, **fingerprint**, **voice**, **face**, **palm**)
- Add additional security authorization in the event another fails
- Log of events of who accesses
- Mitigate intrusion of unauthorized personnel.
- Make biometrics completely contactless for hygienic reasons due to the COVID-19 pandemic
- Recognize a person wearing a mask

The ways that this project fits into the needs of the military are to:

- Secure valuable data/high clearance buildings and rooms
- Allow for biometric tracking of who has accessed these secure locations/devices
- Mitigate intrusion via stolen credentials.

The product is going to be used to:

- Access secure locations (weapons, administrative, “war rooms”)
- Access secure data (secret/top secret information, confidential information and medical records)

3. Specific Requirements

3.1 Product Perspective

Controlling access to facilities, computer systems, and classified information depends on fast and accurate information. The Army also operates a vast set of human resources services involving health care, retiree and dependent benefits, troop support services and many others. These services create the need for accurate identification to prevent fraud and abuse. [1]

The U.S. Army currently uses a combination of a CAC card and personal identification numbers (PINs) for traditional means of access control. This project’s perspective is to use the multimodal

biometrics in conjunction with the CAC cards to

- improve accurate identification and security,
- reduce operational and administrative costs and
- increase user convenience.

The figure 1 below shows our model in a nutshell.

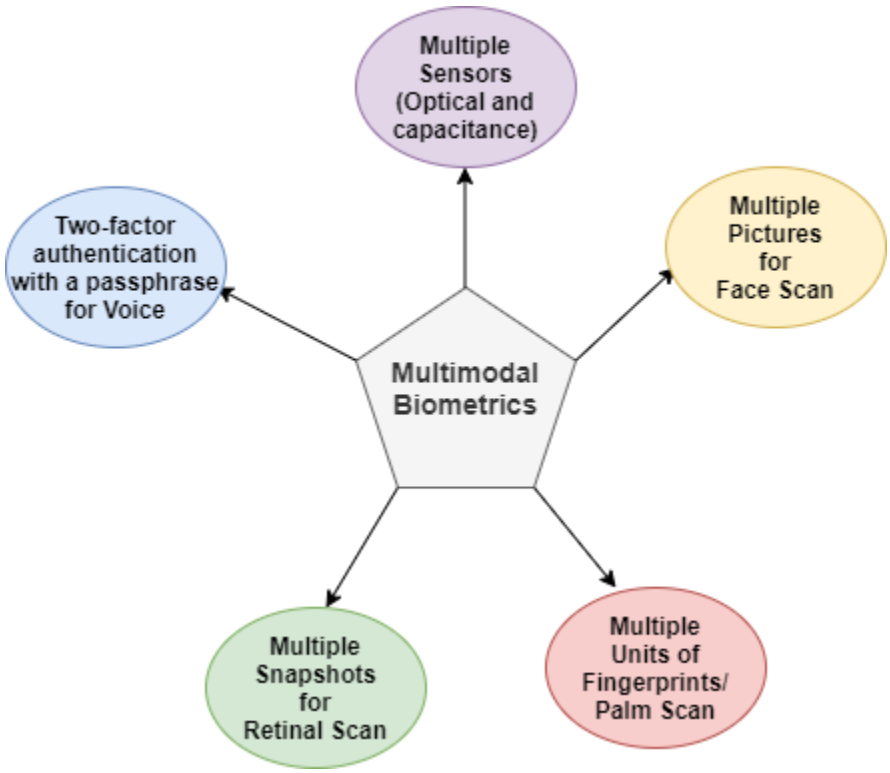

Figure 1: Basic scenario in a multimodal biometrics system

3.2 Functionality

- The server shall provide system data processing and storage capabilities.
- The system shall be able to extract and match the user biometrics data which has already been stored on the database side.
- Only the authorized user shall be able to use the system.
- The system shall allow administrator employees to enroll the new employee.
- The system shall not allow general employees to access the administrator employee options.
- The administrator employee shall be able to manage employees.

- The system shall be able to capture the biometrics of the new employee on employee registration phase.
- The system shall be attached to multiple sensors and cameras to capture the biometrics.
- The administrator employee shall be able to delete the employee record form the system.
- The system shall not allow employees to clock in, who are already clock in to the system.
- The system shall not allow employees to clock out who is already clock out to the system.
- The administrator employee shall be able to generate log reports.
- The system shall recognize a person wearing a mask with more advanced facial recognition by identifying face features as forehead, face contour, eyes, cheekbones, etc.

The figure 2 below shows a flow diagram of our multimodal biometrics system.

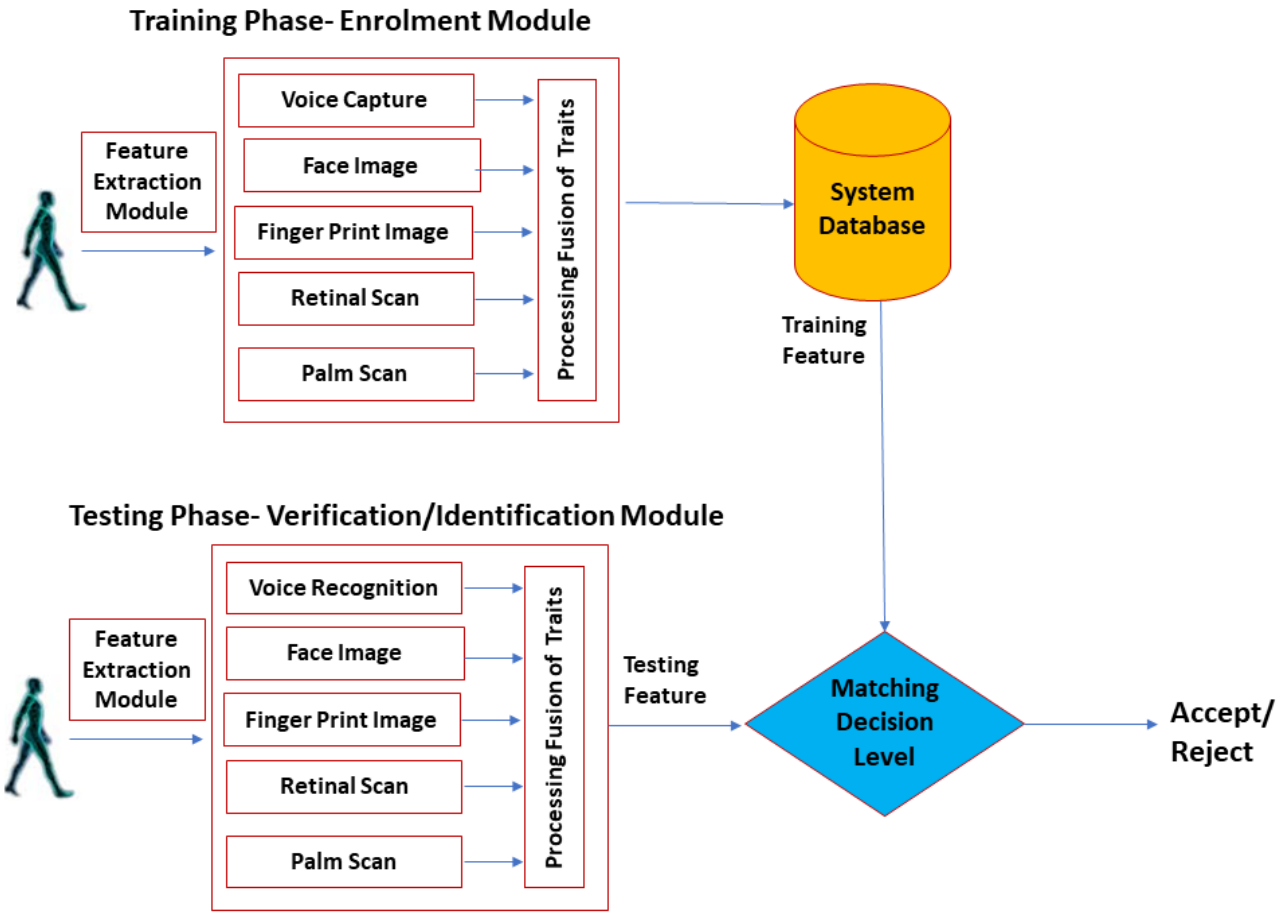

Figure 2: Flow diagram of the multimodal biometrics system

3.3 User Case Models

The customer shall choose one or more of the following models they would like to purchase. Each of them focuses on different scenarios that would benefit the customer needs in different ways:

3.3.1 User Case 1: The model in figure 3 focuses on the **high traffic areas** where a lot of users come in and out at certain times of the day. Therefore, it has to be time efficient. Instead of searching the entire database which would take longer, the user first needs to be verified by using the CAC card in this model. After the user is verified, the system will fetch the user's all of the fingerprint, face and voice data. Every time the user's images and/or scans are taken, it will try to match it with training data of the user.

In order for the user to be granted access they will need to pass two out of three biometric scans which are designed using three biometrics characteristics; fingerprint, face and voice features. Again, these three biometrics features are specifically picked for this model to be fast and efficient. There are three different paths (colored red, blue and green) a user can be identified as shown in the figure 3.

- The **red path** shows after the CAC card is verified, the user needs to pass both fingerprint and face scans and then they can be identified and granted access. The red path also covers the case where a user's card is lost, forgotten or damaged. If a user's CAC card is not verified, they need to be escorted to the ADMIN, where their fingerprint scans need to be taken and checked across the entire database to find a match. If a match is found, the system will fetch the user's face and voice data and continue with the same process with the face recognition scan in the model.

- The **blue** path shows after the CAC card is verified, the user fails fingerprint scan, so they need to pass both face and voice scans and then they can be identified and granted access.

- The **green** path shows after the CAC card is verified, the user passes fingerprint scan, but they fail face scan, so they need to pass voice scan and then they can be identified and granted access.

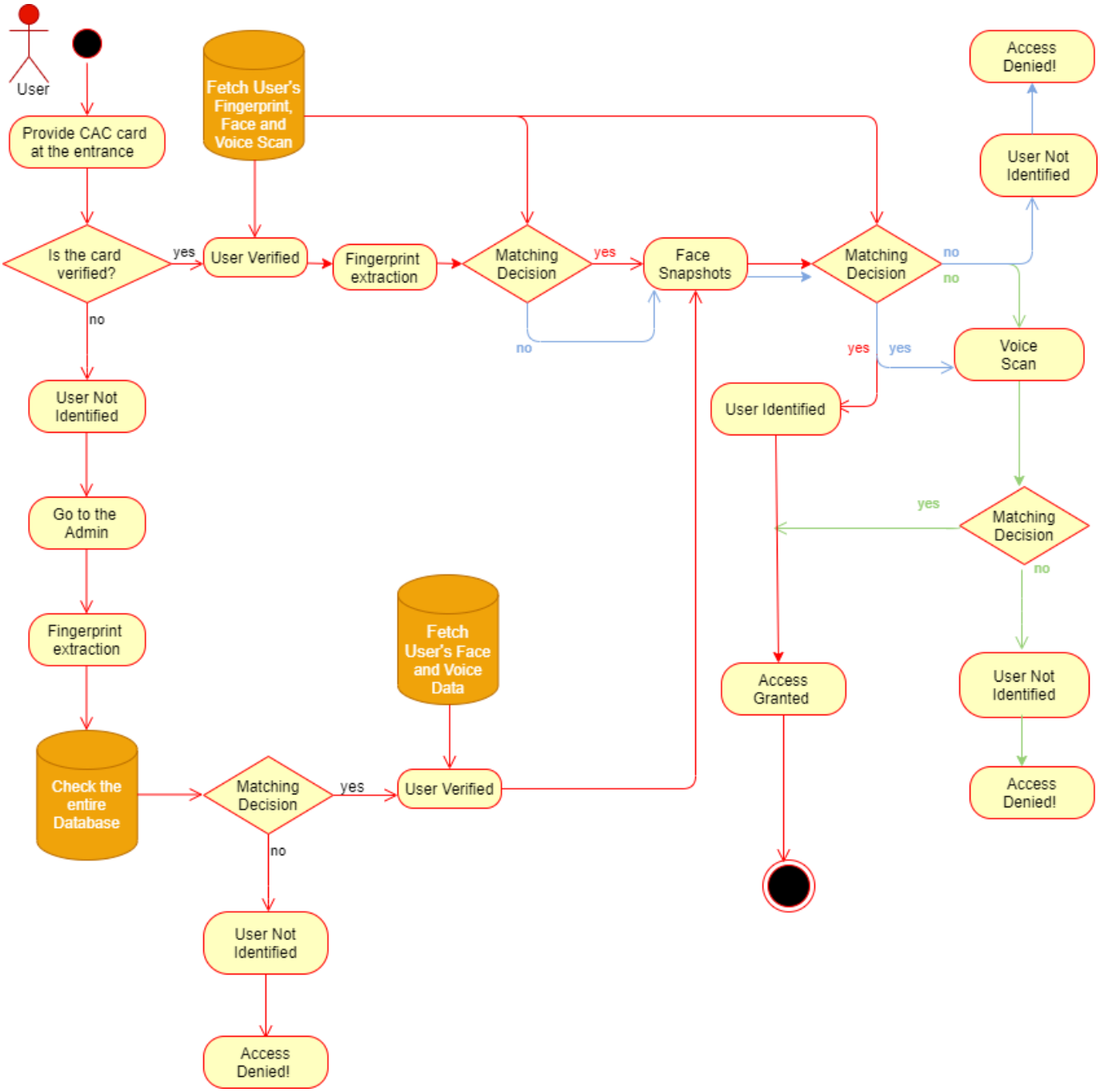

Figure 3: Activity diagram user case 1

3.3.2 User Case 2: The model in the figure 4 is designed based on the recent **Covid-19 pandemic** in mind where a user gets scanned using face, voice and retinal identification without an operator present in the screening area. Not only does this model cover cases where a user does not need to touch any screens for hygiene reasons, but also ease concerns with the users who wear masks and/or gloves and would not want to take them off. This model follows the same paths as the first user case. The only difference is that it uses retinal scan instead of fingerprint.

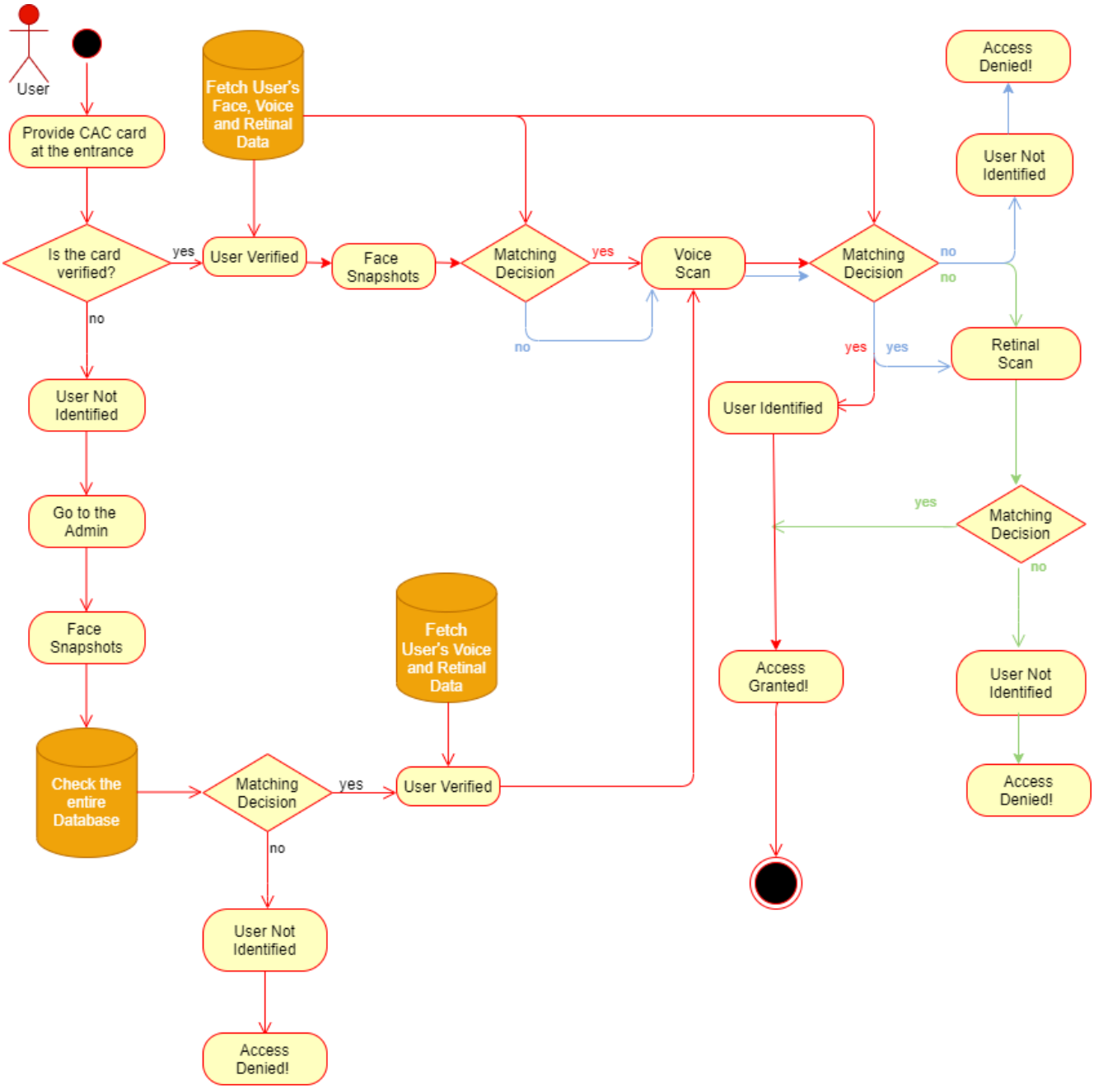

Figure 4: Activity diagram user case 2- contactless option due to Covid-19

3.3.3 User Case 3: This model in the figure 5 focuses on the **low traffic areas** where the security needs to be most accurate for the top-secret rooms/areas. It is designed to incorporate all biometrics characteristics we provide. It consists of two parts. The first part of the model consists of the scenario we proposed in the first user case to get into a Military facility. The second part of the model provides the additional security needed in certain rooms/areas where the user is trying to get access while they are in the Military facility.

Since the user is already in the facility, the system will fetch the user's biometric information from the local database where the user's biometric information has already been extracted at the entrance to the facility.

To achieve the maximum security, we added palm and retinal scans consecutively. The user needs to pass both biometric scans successfully to get access to the desired area.

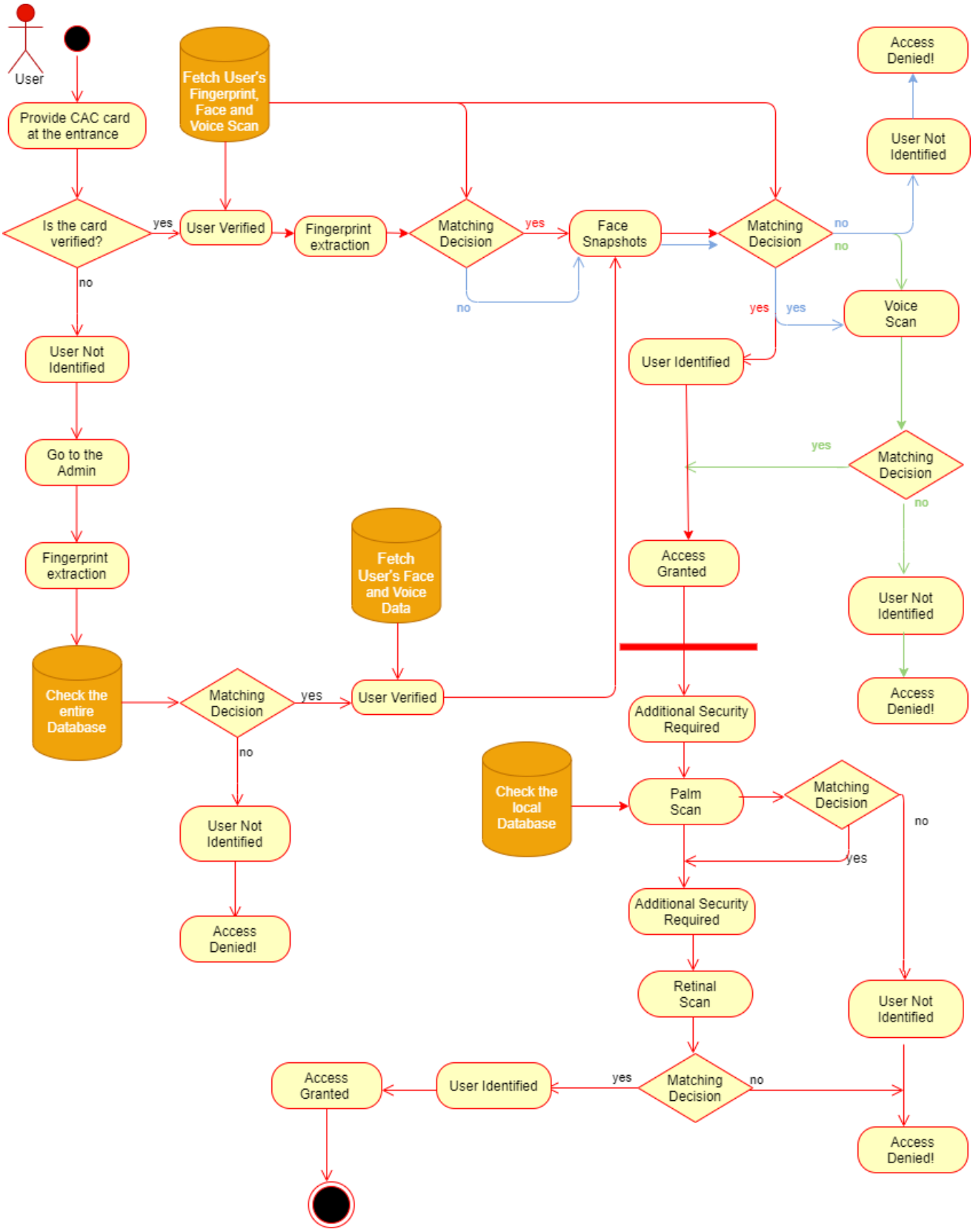

Figure 5: Activity diagram user case 3- top secure areas

3.3.4 User Case 4: The model in figure 6 focuses on **high traffic areas** where a medium security level needs to be met for secured locations and requires biometric scans. It is designed to use parallel authentication in which multiple biometric scans are taken simultaneously, validated against the database, and verified to be matching to one user.

The intended result is to process multiple biometric authentication methods in quicker real time to allow for the next person to use the system for authentication. In this configured deployment, biometric scanning modules need to be chosen for speed and simultaneous input.

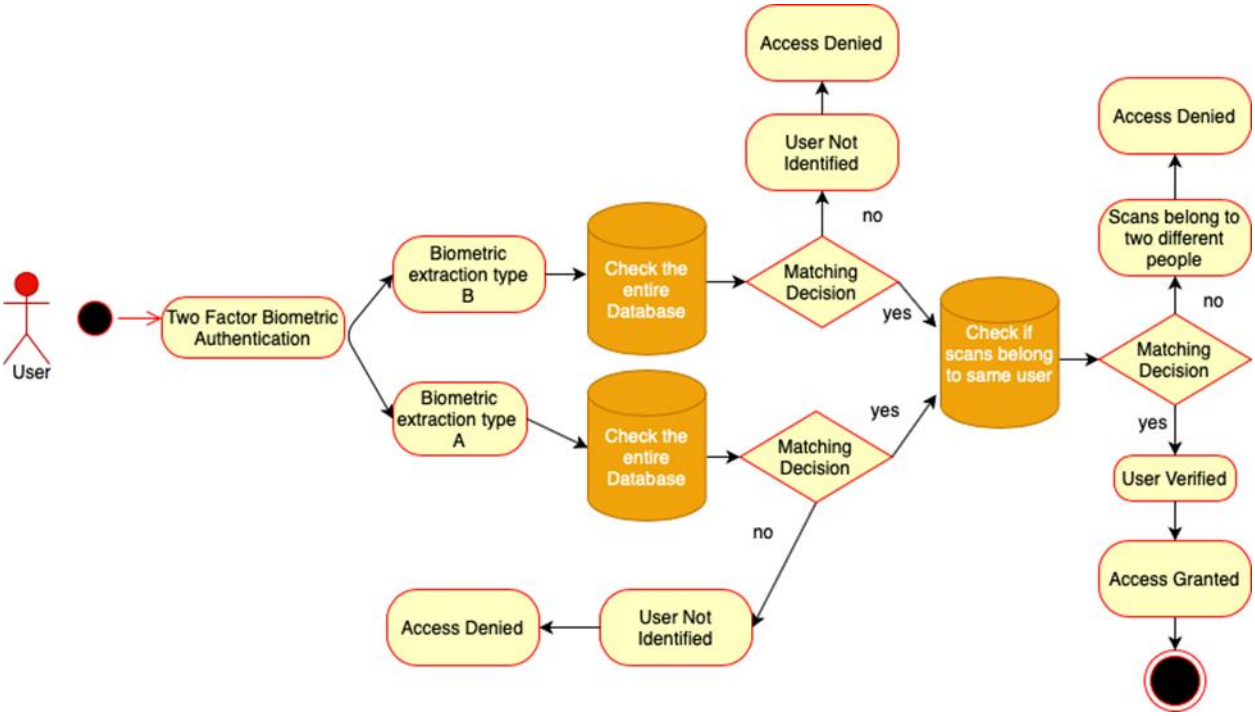

Figure 6: Activity diagram user case 4- Parallel Authentication

3.3.5 User Case 5: The diagram in figure 7 focuses on systems within **environmentally restricted** locations (i.e. extreme hot or extreme cold). These biometric systems are employable with either low or high security standards.

The intended result is to provide sufficient levels of security regardless of environmental circumstances.

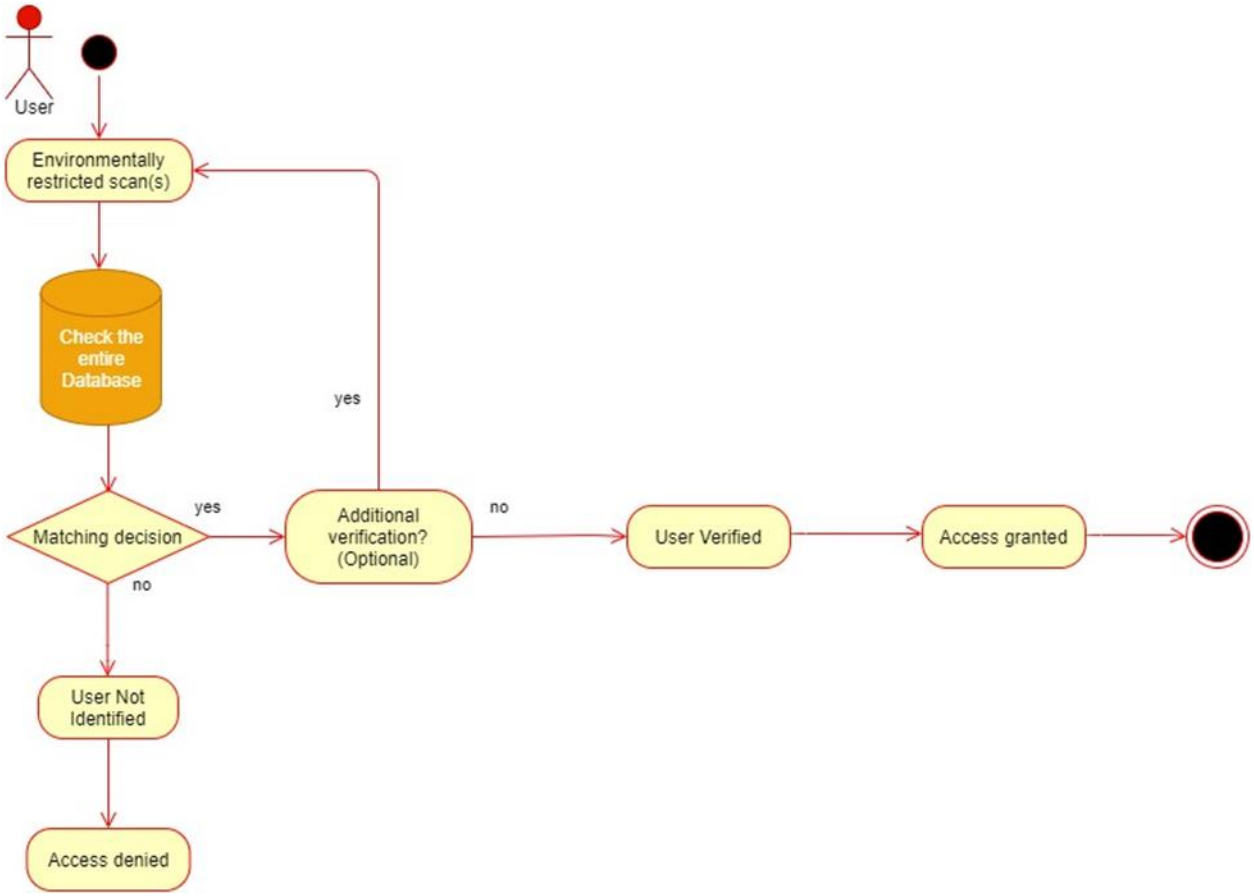

Figure 7: Activity Diagram User Case 5 - Environmentally Restricted

3.4 Environmental Requirements

The system's environment shall be very controlled both indoors and outdoors by

- Keeping it at certain temperature
- Providing proper lighting for the cameras
- Reducing glare by using anti-glare screen for the user
- Providing a quiet space for voice recognition
- For highest tier
    - Should be reinforced structurally to mitigate physical intrusion to device's internal components.
    - Modules need to be built to survive a 15-foot drop 10 times in a row.
    - Modules requiring transparent material should be using a minimum of 3mm thick acrylic.
        - Will need to be UV resistant in the event of outdoor deployment.
        - Scratch resistance will be needed due to heavy use.
    - Be able to operate in extreme temperature environments.
        - Should operate in -70F to 165F range

        - Environments like this might limit module choice to iris and voice due to attire worn in these climates, but face/hand will be supported.
- Base tier
    - Use of materials should not change from the highest tier, but reinforcements are removed as they are likely unnecessary in these deployments.
        - Minimal structural reinforcement.
        - Survive a 5-foot drop 10 times.
        - Transparent material can be made of 2mm thick glass.
        - Intended to operate in normal climates
            - Should operate in 0F to 125F range.

3.5 Detailed Requirements

- The recognition decision needs to be made in real-time, therefore computing efficiency is critical.
    - 1GHz multicore processor minimum required per system.
    - 500 MB of memory minimum required per system.
    - LAN network connectivity (100Mbps).
- **Storage Requirements:**
    - designated database system to track and log movement across the system for future referencing. Minimal data stored.
    - designated database system to store all biometric data related to base, branch, and other approved personnel. Must be large enough to retain biometric data for up to 500,000 individuals.
- **C/C#** will be the designated programming language, and the BioAPI (Biometric Application Programming Interface) will be used for development.

3.6 Design and Implementation Constraints

- **System Response Time Per Usage**
    - Severe Environments:
        - Iris: Under 3 seconds
        - Palm: Under 2 Seconds
        - Voice: Under 3 Seconds
        - Facial: Under 1 Second
    - Normal Environments:
        - Iris: Under 5 Seconds
        - Palm: Under 10 seconds
        - Voice: Under 5 Seconds
        - Facial: Under 3 Seconds

- **Frequency of system being used**
    - Severe Environments
        - Will need to be accessed by simultaneous users across a network.
            - Network infrastructure will need to support data streams for multiple end nodes.
            - System will need to support 100-1000 users simultaneously utilizing the network.
    - Normal Environments
        - Not intended to be a high-volume usage. System should be able to handle usage every 60 seconds.
            - Note: Burst usage should be supported but sustaining burst usage for over 5 minutes should impact performance.
                - Example: Start of business day and users are clocking in.

3.7 User Documentation

- Documentation will be given to end users that have a support plan that would require spares to be left on site and to be installed by the end user.
    - Documentation should be done in two methods, “quick setup” and user manual.
        - Quick setup should be primarily pictorial, with worded instructions that last one to two sentences per step.
        - User manual will be an in-depth multi-chapter instructional book that covers everything.

3.8 Derived Requirements

- A high-resolution camera shall be required to capture the face and iris images of a person accurately when training data.
- Additional hardware (multiple sensors) and/or software (multiple algorithms) could be needed to capture the data using multiple modalities. For example, a facial recognition system might employ multiple cameras to capture different angles on a face.
- A high-quality microphone for voice recognition shall be required.
- Proprietary interface to connect biometric scanning modules.
- Networking capabilities over RJ-45 ethernet port.
- Interface to receive CAC card validation.

4. External Interface Requirements

4.1 User Interfaces

- The system interface shall require clear instructions on a digital screen prompting the user in a step by step manner; i.e. to look into the camera, speak a phrase, place hand on screen or proprietary hand scanning device, etc.
- The system shall have an analog keypad for secondary use in the event the digital interface fails.
- The interface may include a screen showing the video feed of the user, alerting the user to adjust their posture, distance, or any other objects that may obstruct the system's recognition process. i.e. hat, glasses, etc.
- Color visuals to alert the user when verification succeeds or fails.

4.2 Hardware Interfaces

Coverage: How Much Area?

- Dimensions of scanning unit: Varies depending on multimodal configuration
  - 13x10x7 inches max
  - 10x7x7 inches minimum
- Dimensions of server
  - Severe Environments
    - Should fit in a server rack. 1U to 2U spec.
      - May require SAN environment depending on scale of customer
  - Normal Environments
    - ATX to EATX form factor. Blade configuration is also an option.

4.3 Software Interfaces

- The interface that shall be used in this project is BioAPI (Biometric Application Programming Interface) which is a standard application program interface (API) that allows biometric technology modules and applications to communicate with each other by performing enrollment and verification (or identification).
  - **Enrollment** is the process of collecting biometric samples from a person and the device produces an enrollment template.
  - **Matching** is the process of comparing a submitted biometric sample against one (verification) or many (identification) templates in the system's database.

- The purpose of the BioAPI specification is to define an architecture and all necessary interfaces (using C programming language specifications) to allow biometric applications (perhaps distributed across a network) to be integrated from modules provided by different vendors.[3]

- BioAPI supports all the use cases from multiple biometric modalities (for example, retina, fingerprint, voice, face, hand geometry), both to improve the accuracy of identification and to cope with people that are missing a finger, or have disability problems that prevent use of iris or face recognition. [3]
- An API is needed to hand off validation between CAC database and biometric database

4.4 Communications Interfaces

- Communicates over existing network infrastructure.
    - Must be wired infrastructure.
        - Wireless infrastructure reduces stability, and is easily compromised in security.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

- In order for the system to perform reliable identification in terms of accuracy, multi-biometric sample shall be collected using several fingerprint images, several face samples with different angles and retinal samples etc. from a given person because biometric identification systems tend to accumulate False Acceptance Rate (FAR) and false reject rate (FRR) with database size increase.

- A **fused** algorithm shall be used to create a single identification decision based on the results of those multiple measurements to increase matching reliability. [2]

- **Quality:** Identification requests shall be processed as quickly and efficiently as possible (ideally in real-time), requiring considerable computational power.

- The system shall show high productivity and efficiency, regardless of its scale: [2]
    - System scalability is important, as a system may continue to expand and a high level of productivity should be available through the addition of units to the existing system.
    - The daily number of identification requests could be very high for certain applications.
    - Support for large databases shall be required.

- The system shall support the major biometric standards, thereby allowing the use of system-generated templates or databases across a variety of platforms, independent of the vendor source.

- The biometric software engines shall be based on deep neural networks and contain many proprietary algorithmic solutions such as fingerprint, face, palm, voice and retina that are especially useful for large-scale identification problems.[2]

- **Quantity:**
    - How many?
        - Severe Environments:
            - 50 to 500 modules per server.
        - Normal Environments:
            - Up to 50 modules per server
                - Additional modules can be purchased for a fee.
- Device should be mounted to existing physical infrastructure
    - Wall with studs
    - Secured table

5.2 Safety Requirements

- With a hand scanner, the interface will be touched a lot. Cleaning of the surface must be implemented regularly. An unclean surface poses a health risk.
- Due to the nature of highly secure access points, criminal behavior may occur. In the particular event of forced entry by coercion or threatened violence from a criminal, the user shall input a personal sequence of numbers in the keypad that initiates an emergency alert, and locks down that particular system.

5.3 Security Requirements

- System shall have an IP rating of 65 or higher; protection from entry by tools, wires, or brute force. It shall be dust tight with moisture protection. Outdoor systems shall withstand elements of the region; high temperatures, snow, rain, wind, hail.
- In the event of unauthorized tampering of the hardware, the system shall be intuitive to alert the administrators, and shut down, maintain door lockdown to protect from unauthorized access.
- In the event of a database breach or other cyber-attack, lockdown of all systems shall be initiated. In-person verification of identity shall be performed by military police.
- In the event of system failure or glitch, system shall be intuitive to perform troubleshooting and failsafe procedures, and secondary security measures. (See figure 8 below)

The diagram in figure 8 demonstrates the fail-safe procedure in the event of a software or hardware failure. The system shall be designed to perform software troubleshooting procedures that will attempt to resolve any issues. Failing which, the software shall disable that particular scanner and continue to the next verification process. Should all biometric scanners fail, verification will be done by a CAC scan and PIN input.

All issues will be logged, and system administrators will be alerted. The interface shall instruct the user next course of action by visual cues.

This design was implemented to cover every possible combination of scanners installed in any particular system and location.

The intended result is for the system to be expedient in detecting problems, preventing a complete system shut down, and transitioning to secondary verification methods in order to allow quick access to verified users.

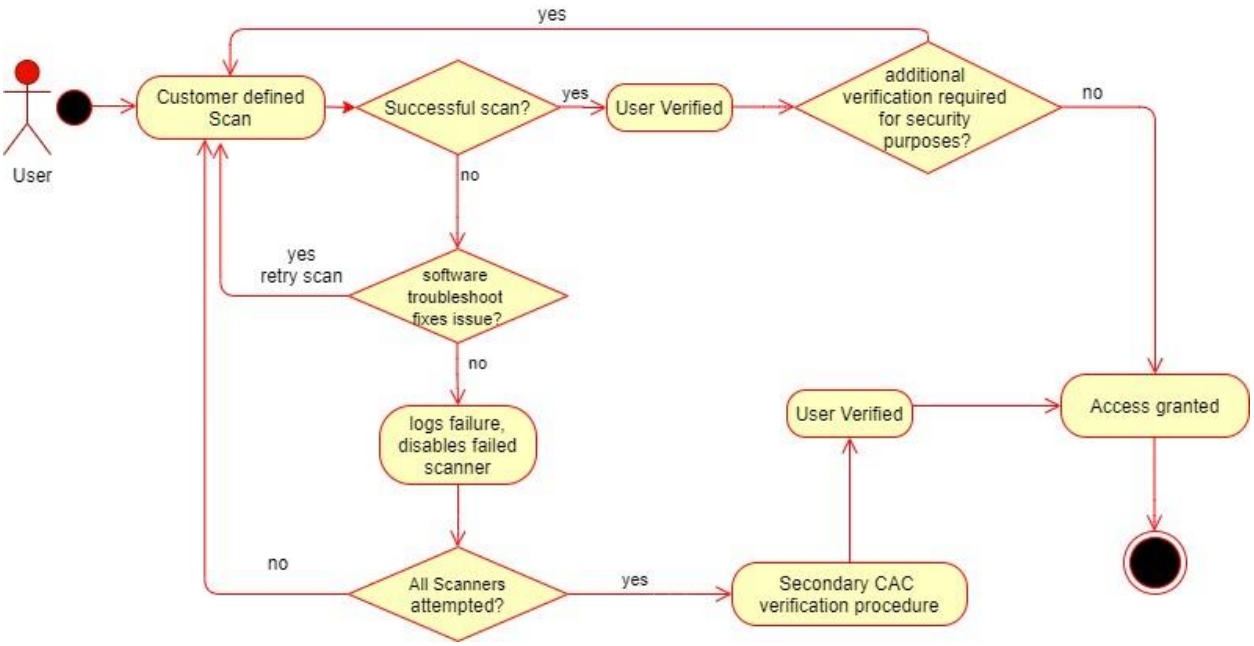

Figure 8: Fail-safe procedure

5.4 Software Quality Attributes

- The build of the system must be in compliance of aforementioned standards. Therefore, the precision engineering must be employed in order to ensure IP compliance, and in accordance with the military aesthetic.

5.5 Cost Requirements:

- The quality and accuracy must be very curial in the military, so it shall cost time and money to achieve the level of software quality requested.
- The cost of an advanced retinal scanner will be about $50,000.00, an advanced facial scanner will be about $25,800.00, a voice recognition software will be about $500.00, an advanced fingerprint scanner will be about $1,298.00, and a palm scanner will be about $1,000.00.
- How much is the customer planning to pay?

- How many units of the product is the customer planning to buy?
- How much initial investment will the customer give as an upfront payment?
- Based on the initial investment and the time frame given by the customer how much should it cost to make the project profitable at the end.
- Do I have the right to expand my customer base e.g. U.S. Airforce, U.S. Navy?
- The cost will change depending on the customer going with how many biometrics traits they would like to combine.
    - Price will be dependent on the amount of scanning modules deployed, not multimodal scanners.
        - Example: an iris/palm/voice scanner consists of three modules.

5.6 Time Requirement:

- What is the time frame required for the customer?
- The faster we develop; it may take less time to complete the project. It might also affect the cost meaning that we might be paying less to the software engineers, but we might need to pay more to get a faster response on data collection and analysis.
- How much will the initial investment be given by the customer? Initial investment is recouped in a short amount of time to achieve fast return on investment.
- Downtime Turnaround
    - Varies based upon customer
        - Severe Environments:
            - Spare parts are located on site, ready to be deployed by the end user. Guide to be included with all spares.
                - Additional spare will be sent to the customer after the issue has been logged.
                    - Should be delivered within 24 hours.
                - Failed equipment will be sent back to be refurbished.
        - Normal Environments:
            - 72-hour response time for repair.
                - Troubleshooting consists of:
                    - Swapping modules
                    - Validating module slots
                    - Validating integrity of entire scanner
                    - Replacing module
                    - Replacing scanner

5.7 Schedule Requirement:

- The schedule for this product to deploy shall be more flexible approximately 8-10 months since the security in military applications must be very accurate.
- Availability?
    - Severe Environments
        - 24x7x365 for high security deployments.
    - Normal Environments
        - 8x5 for daytime operation environments

- After hours option should be considered for select

5.8 Risk Management:

- Determining which technology to use at each access point, or a combination of technologies. If possible, develop a system to be a one-size-fits-all solution where the system will be capable of all technologies, but stakeholder may disable whichever they choose. This may run the risk of having unused components such as the hand scanner.

- With a hand scanner, the interface will be touched a lot. Cleaning of the surface must be implemented regularly. An unclean surface poses a health risk.

- In the event of system failure or glitch, the system must be intuitive to shut down.

- To protect user privacy, biometric information will be associated with an ID number, and data is encrypted.
- To mitigate network intrusions from the scanner, communications will be done only with valid MAC addresses.

6. Other Requirements

- System shall meet standards outlined in the Department of Defense Information Technology Standards Registry (DISR).
- System shall be in compliance with cyber-security mandates detailed in the National Institute of Standards and Technology 800-171 (NIST 800-171) Special Publication.
- System shall be fast and responsive. Therefore, the software must be lightweight and future-proof up to at least 5 years. The hardware must also be future-proof so as not to require constant upgrades which can be costly and may compromise security during maintenance.

Glossary

- CAC – Common Access Card
- DOD – Department of Defense
- DISR - Department of Defense Information Technology Standards Registry
- NIST - National Institute of Standards and Technology