Software Development Plan

for

Multimodal Biometrics

Version 2.4

Brian Tan

Davina Doran

Fulya Kocaman

Konnor Gutierrez

California State Fullerton

CPSC 362 SOFTWARE ENGINEERING

11/4/2020

Table of Contents

Revision History

Name	Date	Reason for Changes	Version
Fulya Kocaman	10/12/20	Created	1.0

Brian Tan	10/14/20	Added Testing & Deployment and Maintenance	1.1
Davina Doran	10/14/20	Added Cost Estimate, Schedules and Milestones	1.2
Konnor Gutierrez	10/14/20	Added Risk Analysis & Technical Readiness	1.3
Fulya Kocaman	10/14/20	Added Design, Development & Implementations	1.4
Fulya Kocaman	10/17/20	Reformatted and added Class, Sequence and Activity Diagrams	2.0
Davina Doran	10/26/20	Updated Cost, and relocated Software Development Schedule	2.1
Konnor Gutierrez	10/30/20	Added Risk Assessment Charts	2.2
Brian Tan	10/31/20	Added Test Plan Flow and Activity Diagrams	2.3
Fulya Kocaman	11/1/20	Finalized formatting in a Word Doc	2.4

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. The detailed Software Development Plan of the **Multimodal Biometrics Recognition System** is provided in this document.

1.1 Purpose

The purpose of this Software Development Plan (SDP) document is to provide a detailed software management and tools necessary to develop and deliver a quality software product with a system that uses multimodal biometrics recognition system that can be customized based on the usage requirements, its parameters and goals.

The SDP shall be implemented and maintained throughout the software development life cycle. This plan contains these six steps include planning, analysis, design, development & implementation, testing & deployment and maintenance.

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 SDP shall focus on the following perspectives of the using a Multimodal Biometrics product:

- This project's goal is to use a multimodal biometrics recognition system which uses unique identifiers (**retina**, **fingerprint**, **voice**, **face**, **palm**) 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/
[5] Software Engineering: A Practitioner's: 9th Roger Pressman, Bruce Maxim
[6] https://www.bayometric.com/unimodal-vs-multimodal/
[7] Biometric Recognition- Challenges and Opportunities (2010) National Research Council (US) Whither Biometrics Committee; Pato JN, Millett LI, editors.
[8] https://resources.infosecinstitute.com/a-project-management-guide-to-deploying-biometrics-part-3-the-modality-aspect/#article
[9] Fundamentals of Biometric System Design by S. N. Yanushkevich

1.5 Overview

The remaining sections of this document provide a detailed description of the software development plan of the product.

- Section 2 contains a general description of the project.
- Section 3 provides project organization.
- Section 4 and 5 are for Planning and Analysis.
- Section 6 is for detailed description of Design and Architecture of the system.
- Section 7 is for Development and Implementation including class, sequence and activity diagrams.
- Section 8 focuses on the Cost.
- Section 9 is for Risk Management.
- Section 10 contains Schedule and Milestones.
- Sections 11 and 12 focus on Testing & Deployment and Maintenance.

2. Overall Description

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.

This project describes the planning associated with the Multimodal Biometrics Software System. This plan outlines the organizational roles and contains the six steps of Software Development Plan including planning, analysis, design (Architectural Design and Software Lifecycle), development & implementation, testing & deployment and maintenance

3. Project Organization

The chart in Figure 3 shows the sample structure of the software development team that our project should consist of.

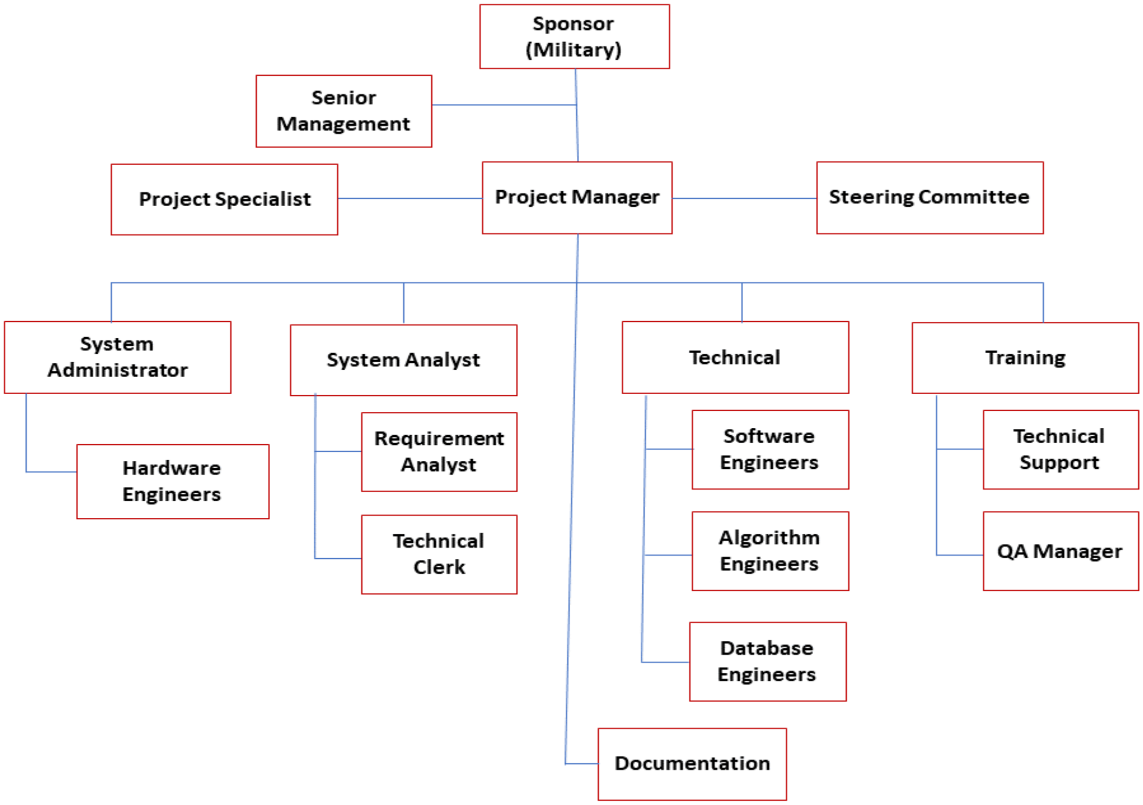


Figure 3: Software organization flow

3.1 Subcontractors

Since we want to focus on the system and software algorithm, we could need subcontractors for hardware for cameras, biometrics readers, sensors, hard disk to store data and servers.

4. Planning

The overall goal is to have systems securely up and running within 10 months. To do this the project has been compartmentalized into cohesive sections as follows: Requirements, Research, Design, Development, Testing (Phase I), Testing (Phase II), and Deployment. Each section has its specific project milestone that will be reached at competition of said phase. The modularity of our system allows for minimal interdependency between these processes until testing prototype multi modular systems.

5. Analysis

- Our system shall be robust, flexible, and extendable by using object-oriented analysis and design.
- Our multimodal biometrics system should be designed to handle the constant changes and improvements of the fast-growing industry.
- The design shall also be secure, fast using efficient and accurate algorithms.
- Accuracy is an important factor of a biometric system. Our biometric system shall accurately determine a person's identity within minimum margin of error.
- It shall handle different data types and formats according to different application requirements. It shall also interact seamlessly with other system architectures, hardware devices, and software application systems.
- If any of the identifiers fail to work for known or unknown reasons, the system should still provide security by employing the other identifier.
- Below are the Biometric identifiers as explained in [9] used in this project:
    - **Facial** recognition attempts to identify a subject based on facial characteristics (eye socket position, space between cheekbones, etc.).
    - **Fingerprint** recognition systems rely on the biometric device's ability to distinguish the impressions of ridges and valleys made by an individual's finger.
    - **Palm** recognition is based on the palms of the human hands that contain pattern of ridges and valleys (like the fingerprints) and additional distinctive features such as principal lines and wrinkles. When using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles may be combined to build a highly accurate biometric system.
    - **Retinal** scanning/recognition involves an electronic scan of the retina, the innermost layer of the wall of the eyeball.
    - **Voice** recognition techniques digitize a profile of a person's speech into a template voiceprint and stores it as a table of binary numbers. During authentication, the spoken passphrase is compared to the previously stored template.

6. Program Design Approach

6.1 Architectural Design

- Multimodal Biometrics Design shall be modular (compartmentalization of data and function) which makes it more flexible when adding and/or removing a user, hardware, database. This modular platform should collect the data, create a database, communicate with the hardware and then compare user data with the database using algorithms and the decision.

- Refactoring that simplifies the design without changing functionality should be used if possible.

Figure 6.1 represents sources of information for Biometric fusion that we shall use in this project:

- **Multisensors**: Multiple sensors shall be used to capture the data. For example, a facial recognition system might employ multiple cameras to capture different angles on a face.
- **Multiple algorithms:** The same capture data are processed using different algorithms.
- **Multiple instances:** Multiple instances of the same modality shall be used. For example, multiple fingerprints may be matched instead of just one, as may the retinal scan of both eyes. Depending on how the capture was done, such systems may or may not require additional hardware and sensor devices.
- **Multisamples:** Multiple samples of the same trait shall be acquired. For example, multiple angles of a face or multiple images of different portions of the same fingerprint are captured.
- **Multimodal:** Data from different modalities shall be combined, such as face, fingerprint and palm, retina and voice. Such systems require both hardware (sensors) and software (algorithms) to capture and process each modality being used [7].

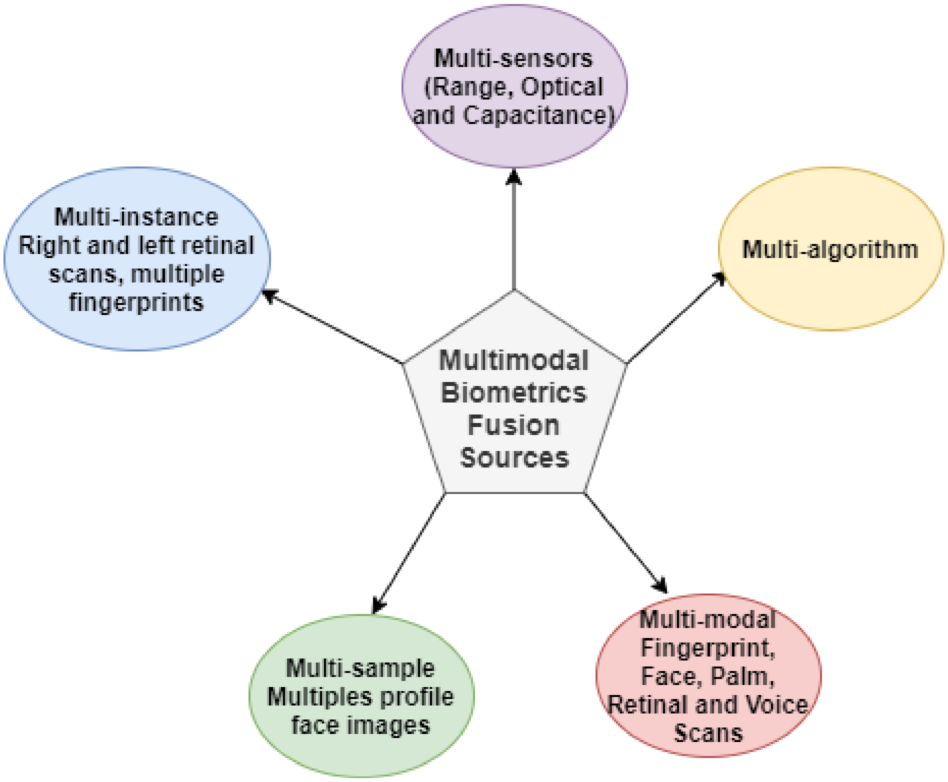

Multi-sensors (Range, Optical and Capacitance)
Multi-instance Right and left retinal scans, multiple fingerprints
Multi-algorithm
Multimodal Biometrics Fusion Sources
Multi-sample Multiples profile face images
Multi-modal Fingerprint, Face, Palm, Retinal and Voice Scans

Figure 6.1: Sources of information for Biometric Fusion

6.2 System Architecture

There will be different types and kinds of Biometric information/data which will be shared with the different modalities in a Multimodal based Biometric system. Multimodal systems fusion architecture as mentioned in [6] combines several biometric systems and thus requires the acquisition and processing of several data (Figure 6.2).

- In sensor level fusion, we shall fuse the biometric traits coming from different sensors such as fingerprint scanner, retinal scanner, video camera etc. to form a merged biometric trait and process.
- In feature level fusion, signals coming from different biometric channels shall be first processed after which the feature vectors are extracted separately from each biometric trait. The feature vectors are then combined to form a composite feature vector using a specific fusion algorithm and then used for further classification. In feature level fusion, some reduction techniques should need to be used in order to select only the useful features.
- In this matching score level fusion level, the feature vectors shall be processed separately rather than combining them. Then an individual matching score is found and based on the accuracy of each biometric channel, we then fuse the matching level to find a composite matching score which will be used for classification. We could use various techniques such as logistic regression, highest rank, Bayes rule, mean fusion etc. to combine match scores.
  - In addition to this, another important aspect of this fusion is the normalization of scores acquired from different modalities because each subsystem can have intervals of variation of the different scores, for example for a system the scores vary between 0 and 1 and for another the scores vary between 0 and 100. Hence, we shall need to normalize the scores before to combine them. We can use techniques such as Min-max, z-score, piecewise linear etc. to achieve normalization of the match scores. We could examine the effect of different score normalization techniques on the performance of a multimodal biometric system and compare normalization techniques on the basis of robustness and efficiency.
- In decision level fusion, each biometric trait is first pre-classified separately. The individual biometric trait is first captured and then features are extracted from the captured trait. The traits are classified as either accept or reject based on these extracted features. The final classification is obtained by combining the outputs of different modalities

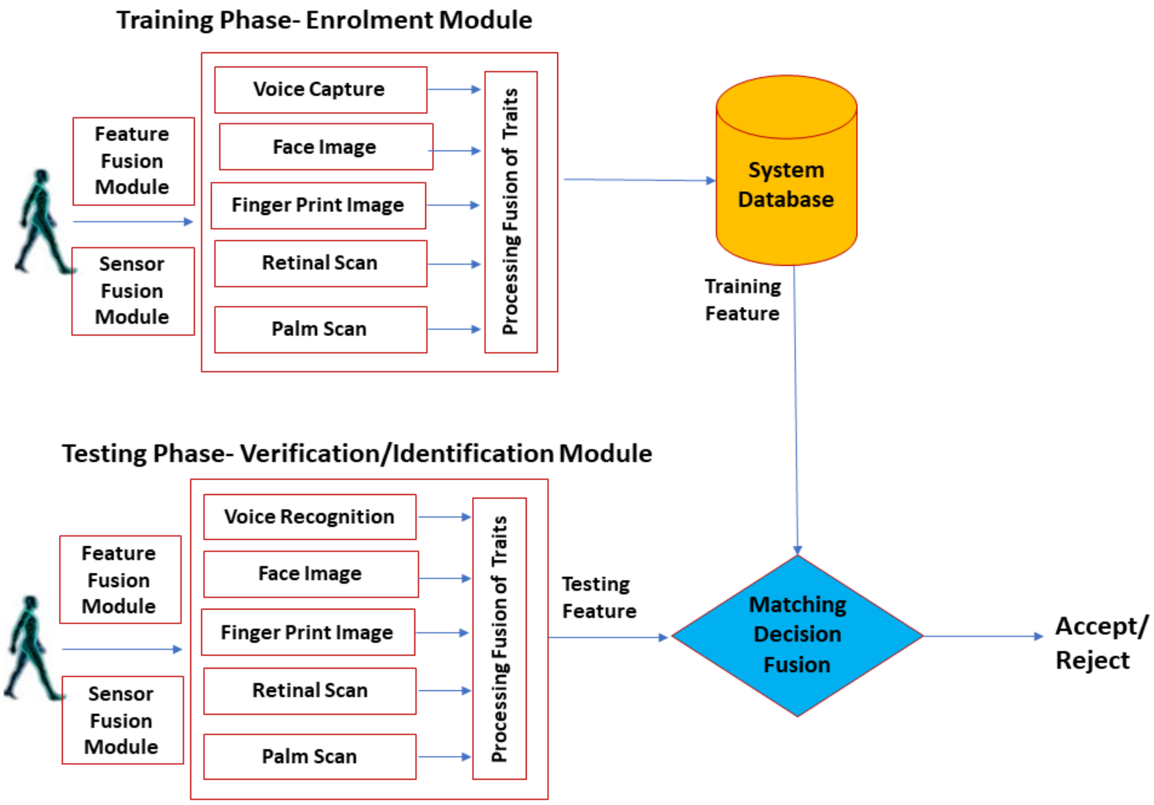


Figure 6.2: Enrollment and Authentication Phases of the system- Fusion Levels

6.3 Software Lifecycle

Multimodal Biometrics Design: Object Oriented Design shall be used in this Multimodal Biometrics project so that the components of a system encapsulate data and the operations that must be applied to manipulate the data. The coordination and communication between the components are established via the message passing.

6.4 Design Reviews

There shall be weekly design reviews to ensure product quality and to reduce the potential risk of avoiding the problems of not meeting the schedules and requirements.

These software design reviews shall start with a preliminary design review, then a critical design review and then a program design review.

7. Development and Implementation

7.1 Top-Down Development

- The Multimodal Biometrics system shall be designed from the top-down based on the requirements defined in our previous Software Requirements Specification report.

- The design shall be modular with Object-Oriented Architecture which focuses on defining software objects and how they collaborate to fulfill the functional requirements of the software system.
- In this report Unified Modeling Language (UML) such as the use case, sequence, as well as class diagrams shall be used to specify, visualize, construct, and document the artifacts of software systems, business modeling, and other non-software systems.

7.2 Programming Standards and Conventions

- **C/C#** will be the designated programming language, and the BioAPI (Biometric Application Programming Interface) will be used for development.

7.3 Quality Assurance

- The recognition decision needs to be made in real-time, therefore computing efficiency is critical.
- Identification requests shall be processed as quickly and efficiently as possible (ideally in real-time), requiring considerable computational power.

- Communicates over existing network infrastructure.
  - Must be wired infrastructure.
    - Wireless infrastructure reduces stability, and is easily compromised in security.
- Biometric encryption techniques shall also be used. They use biometric characteristics as part of the encryption and decryption algorithm.
  - An extract from biometric data will be used as a key to encrypt an identifier needed for the service. With this system, there is no storage of the identifier or of the biometric data: only the result of the identifier encrypted with the biometrics is stored.

7.4 Class Diagram

The following lists the class characteristics to design multimodal biometrics software [5]

- Design shall have functional independence by having
  - **High cohesion** – Every subsystem in the overall Biometric system should only perform and execute specific tasks to which it has been assigned, in order to ensure that the Biometric system works as one harmonious unit.
  - **Low coupling** – Coupling shall be used and designed in such a way that each Subsystem in the overall Biometric system can operate separately from one another.

Figure 7.4 shows a class diagram for our multimodal biometrics system where we created using Object Oriented Design.

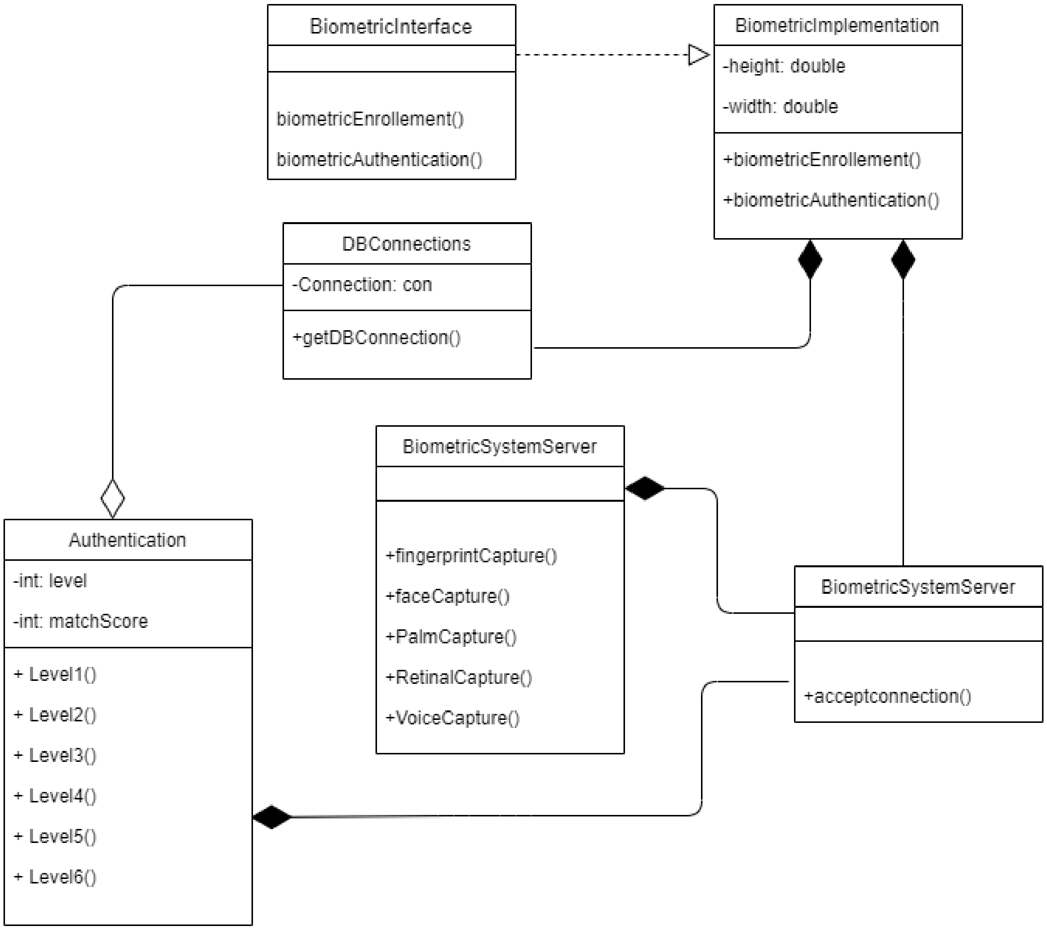


Figure 7.4: Class Diagram of multimodal biometrics system

Interface design: The ultimate goal of any Biometric system is to be the "Human to Machine Interface." As a result, the proper choice of the Sensor becomes of paramount importance to capture and collect the raw images as stated in [8].

- The interfaces shall reduce the complexity of connections between components and the external environment.
- Interfaces (both internal and external) shall be designed with care.
- User interface design shall be tuned to the needs of the end-user and stress ease of use.

The various subcomponents which shall be needed in this part of the process include the following:

1. The Computer Hardware: The speed of the actual modality hardware as well as the speed of the Central Processing Unit (CPU) are very important. Below are some important factors:
    - The generation of the of the CPU and its relative speed (measured in hertz)
    - The Arithmetic Logic Unit (also known as the ALU) which regulates the mathematical calculations

- The bus speed of the CPU, which is measured in the actual speed and the width
- The input/output rate (also known as the I/O rate) in which the Biometric information and data can be sent to other hardware devices which support the entire Biometric system.

2. The Parallel and Distributed Processing: In a large-scale Biometric system, just one processor shall not be enough. Therefore, the workload must be shared. To accomplish this, a concept known as Parallel and Distributed Processing are must be utilized:
    - Parallel Processing: In other words, one server processor can send the workload into different components to other server processors to execute a portion of the larger program that supports the Biometric software applications from within the system.
    - Distributed Processing: With this type of processing, the same task is broken up amongst a series of server processors. In this instance, a single mathematical instruction, multiple data architecture is utilized. This simply means that the server processors perform the same, repetitive tasks on different sets of Biometric information and data.

7.5 Sequence Diagram

The dynamic sequence diagrams describe the objects and their interactions in the system. The Figure 5 and 6 represent sequence diagrams for enrollment and authentication respectively.

- During the Enrollment process biometric samples are collected from a person and the device produces an enrollment template (Figure 7.5.1).

- During the Authentication process matching is processed by comparing a submitted biometric sample against one (verification) or many (identification) templates in the system's database (Figure 7.5.2).

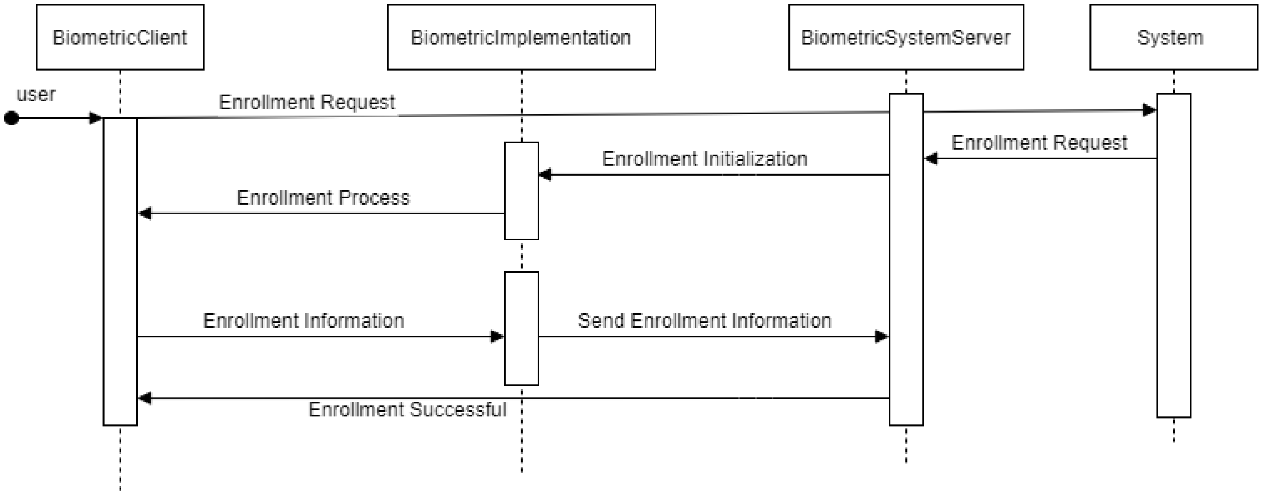


Figure 7.5.1: Sequence Diagram for Enrollment

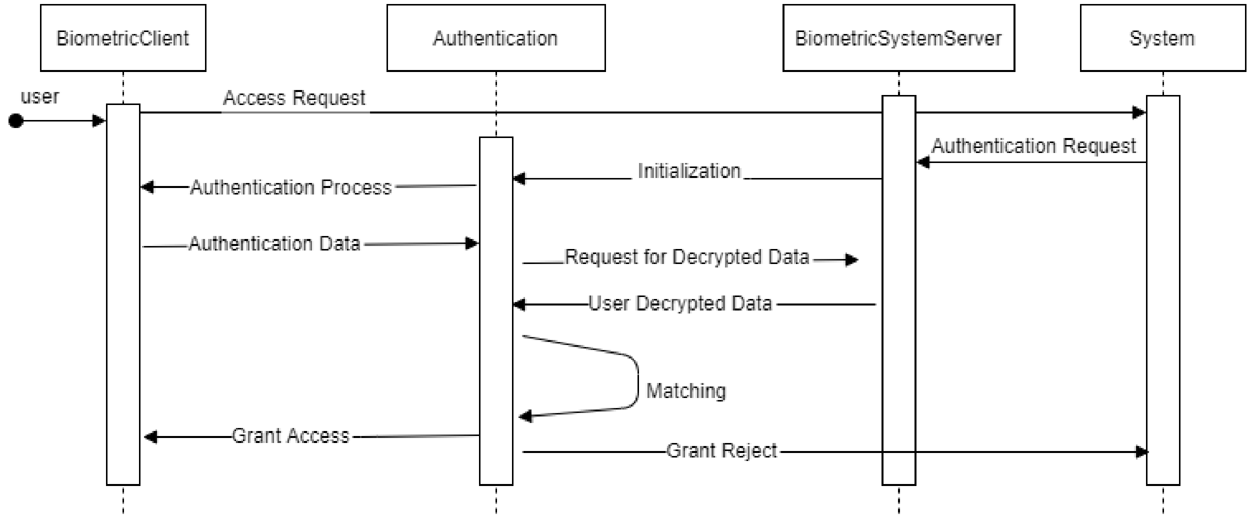


Figure 7.5.2: Sequence Diagram for Authentication

7.6 Activity Diagram

The activity diagram in Figure 7.6 incorporates all biometrics characteristics in this project; fingerprint, face, voice, palm and retinal scans. It consists of two parts. The first part of the model consists of the scenario on how 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.

- In the first part 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. After fusing together, the individual biometric identifiers, the fusion score will be achieved. Finally, it will try to match it with training data of the user.
    - This user case also covers 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.
- In the second part 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, palm and retinal scans will be used consecutively. The user needs to pass both biometric scans successfully to get access to the desired area.

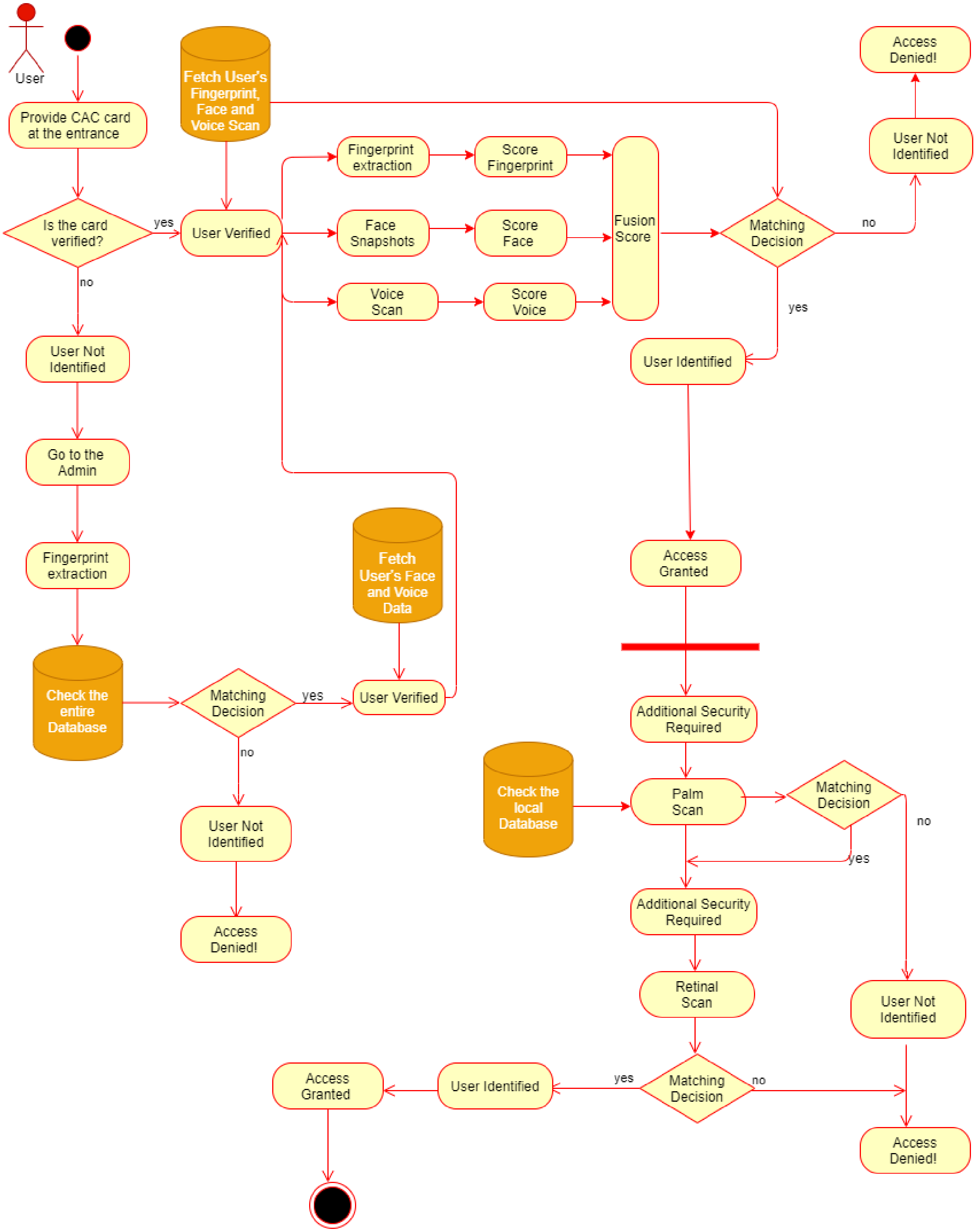


Figure 7.6: Activity Diagram with fusion method

8. Cost Estimate

8.1 Time Allocation

There are 10 months reserved for competition and deployment of the modular biometric security system. Due to the low coupling between each biometric system phases can begin during the progression of a previous phase. 20% of the time is to be allocated to research and requirements. 60% of the time is to be allocated to design and development. Finally, 15% will be allocated to testing and 5% to deployment. These ratios can vary depending on the progression on each phase.

8.2 People Power Requirements

In order to complete this project on time it has been determined that the software development team will consist include: the senior management team, project specialist, steering committee, project manager, system administrator, system analyst, hardware engineers, requirement analyst, technical clerk, software engineers, algorithm engineers, database engineers, technical support QA manager.

- Already filled roles: senior management team, project specialist, steering committee.
- To be hired: project manager, system administrator, system analyst, hardware engineers (team of 4-5 people), requirement analyst, technical clerk, software engineers (2 teams of 3-4 people, 6-8 people total), algorithm engineers (team of 3), database engineers (team of 3-4 people), technical support (5-10 people), QA manager.

8.3 Cost

- **Cost to develop/run the system:**
    - All estimates are based on current national averages, 40-hour work weeks, and a project length of 8-10 months. Roles listed as indefinitely insinuates that the job necessity will persist longer than the length of development (8-10 months), and will have an additional yearly estimate.
        - Project manager: 8-10 months, $50-60 hourly
            - life of project est. $64,000-$96,000
        - System administrator: indefinitely, $25-$35 hourly
            - life of project est. $32,000-$56,000
            - yearly est. $48,000-$67,200
        - System analyst: indefinitely, $25-$35 hourly
            - life of project est. $32,000-$56,000
            - yearly est. $48,000-$67,200
        - QA manager: 8-10 months, $50-$60 hourly
            - life of project est. $64,000-$96,000
        - Technical clerk: indefinitely, $10-$20 hourly
            - life of project est. $12,800-$32,000
            - yearly est. $19,200-$38,400
        - Software engineers: 8-10 people, 8-10 months, $30-$40 hourly
            - life of project est. $38,400- $64,000 per person = $230,400-$512,000

- Algorithm engineers: 3 people, 8-10 months, $55-$65 hourly
  - life of project est. $70,400-$104,000 per person = $211,200-$312,000
- Database engineers: 3-4 people, indefinitely, $25-$35 hourly
  - life of project est. $32,000-$56,000 per person = $96,000-$224,000
  - yearly est. $48,000-$67,200 = $144,000-$268,800
- Technical support: 5-10 people, indefinitely, $10-$20 hourly
  - life of project est. $12,800-$32,000 per person = $64,000-$320,000
  - yearly est. $19,200-$38,400 = $96,000-$382,000

- Estimated Total for the Software Development (8-10 months): $806,400-$1,704,000
- Estimated total per year (maintenance and support): $355,200-$823,600

- **Hardware costs:**
  - All hardware costs vary per system implemented. ($10,000 – 2M+, 1M Average)
- Input Device Costs(per unit)
  - Voice: $500
  - Palm: $100
  - Fingerprint: $1,300
  - Facial: $25,800
  - Retinal: $50,000
- Environmentally hardened scanners run at x2's the rate
- Processing/Storage Devices:
  - CPU: $200 - $400 per system
  - RAM: $30 - $50 per system
  - Database: $5000 – $10,000

- Backup Power (UPS): $2,000-$5,000 per system

8.4 Management Reserve

Based on the estimate that the cost to develop the system would cost $3M. A 5-15% MR would account for a total of $3.15-3.45M.

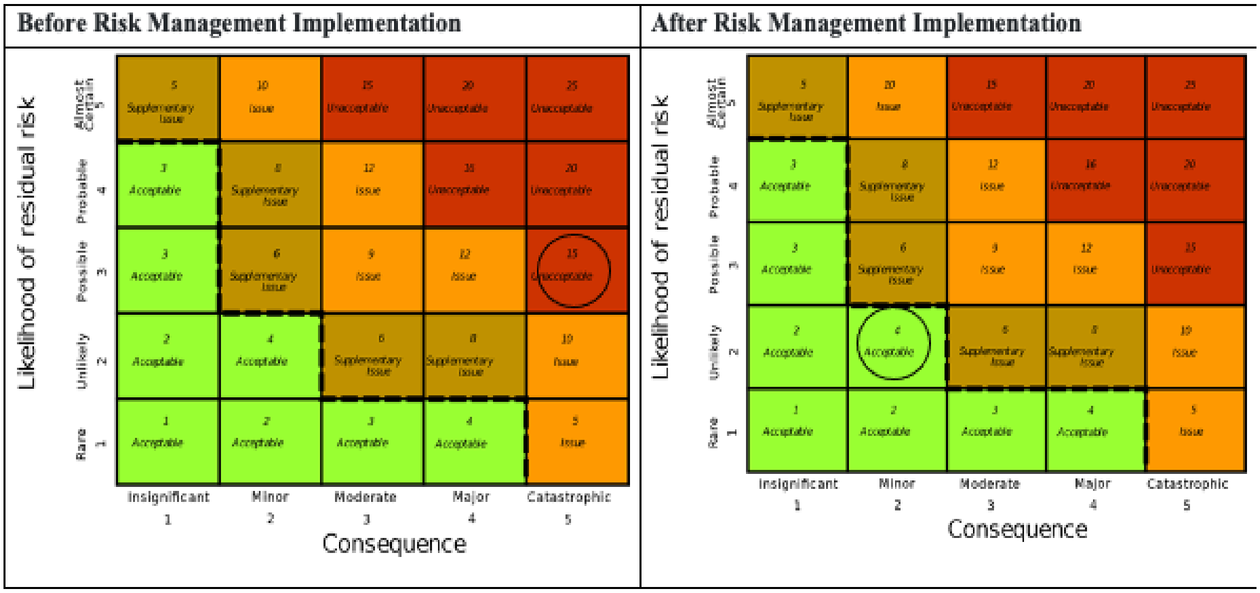
9. Risk Analysis

9.1 Identified Risks and Risk Management

1. Performance of System shown in Figure 9.1.1.a
   a. In the event of a total system failure:
      i. Allow for CAC authorization + personnel verification in total system failure event

ii. Protection against this event by having live backups taken, and the ability to roll back the system as needed.

iii. Rollback method is built into BIOS, not OS



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Figure 9.1.1.a: Total System Failure Risk Assessment

b. Individual scanner failure shown in Figure 9.1.1.b

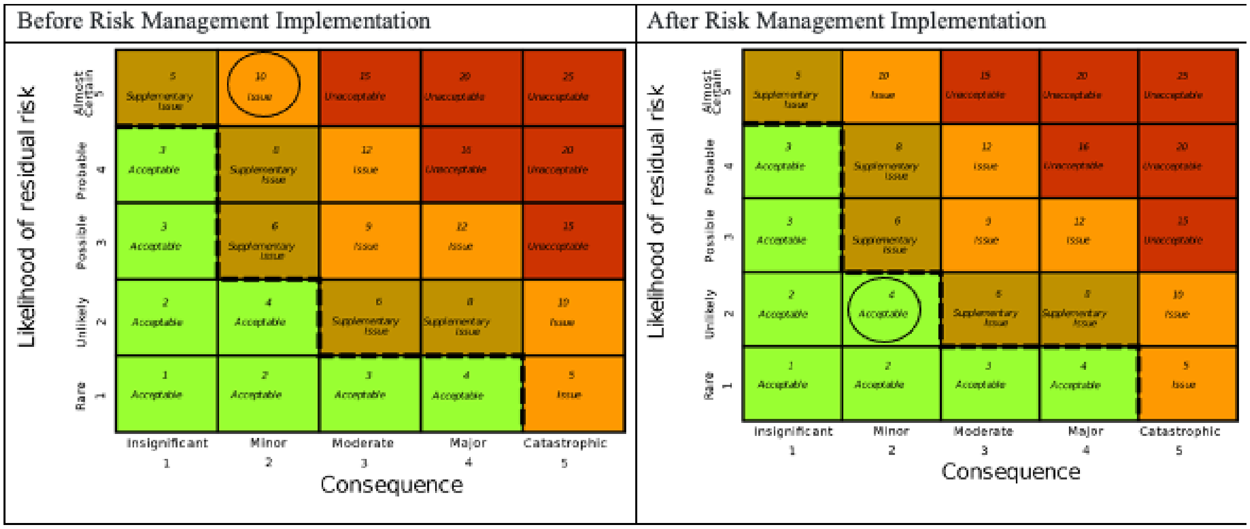
i. Implementation of having failover biometric authentication method.

1. example: iris scanner is offline, so allow voice recognition as a method of authentication.

ii. Include a built-in self-test (BIT) and error correction mode upon boot/reboot.

1. If device is offline, reboot procedure is sent from server.

iii. Allow for failover to CAC card authentication when applicable.



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

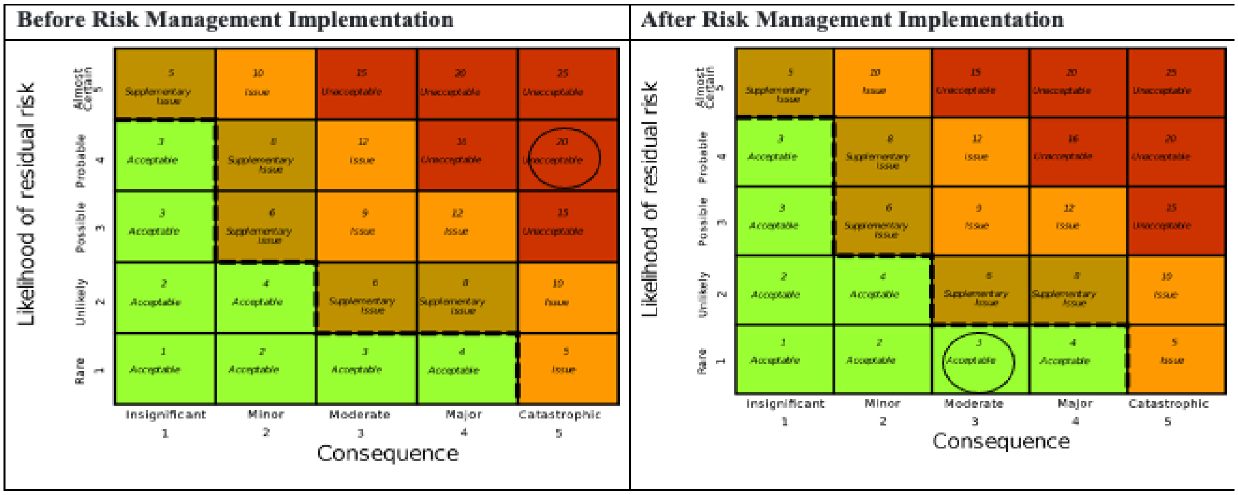
After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Figure 9.1.1.b: Individual Scanner Failure Risk Assessment

2. Type I Errors: False Reject Rate (FRR) and Type II Errors: False Accept Rate (FAR) shown in Figure 9.1.2
    a. Depending on the deployment of the scanner, allow for an adjustment in FRR and FAR.
        i. FAR lowers when only minimal biometric authentication methods are deployed.
        ii. FRR tolerance increases when requesting multiple methods of biometric authentication
        iii. Highest tolerance rate is when all biometrics + CAC cards are required for access. Lowest tolerance rate required when 1 method is required.



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

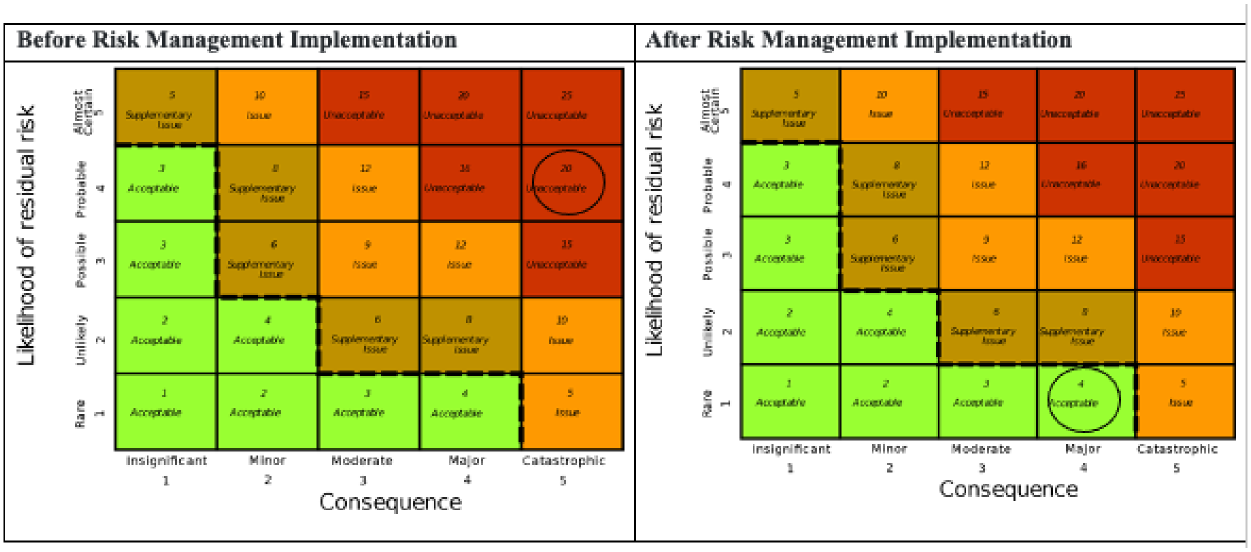
After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	20 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Figure 9.1.2: FRR/FAR Authentication Risk Assessment

3. Spoofing shown in Figure 9.1.3
    a. Constantly update the anti-spoof algorithm.
        i. Use of in-house algorithms will mitigate reverse engineering.
            1. Dedicated teams will create and re-make algorithms as needed.
                a. Re-makes will be done in the event of a major breakthrough in algorithm cracking methods.
            2. Applying algorithm will be deployed locally by trusted staff of the company, not client.



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

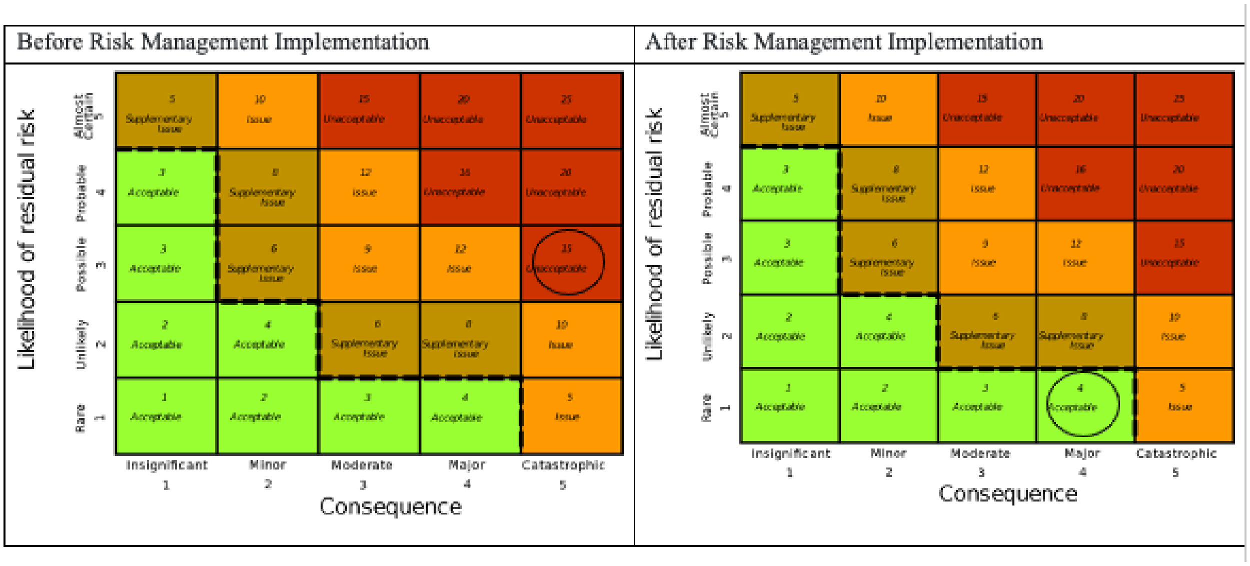
After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Figure 9.1.3: Spoofing Risk Assessment

4. Data Breaches shown in Figure 9.1.4
   a. Data will not be saved on the local scanner to mitigate intrusion.
   b. Biometric enrollment must not be taken from an existing database.
   c. Databases should not be connected to the internet.
      i. Database is on an alternate subnet that can only be used by the biometric system.
      ii. Subnet will be accessible only through valid MAC addresses.
   d. All communications using AES encryption.



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

After Risk Management Implementation

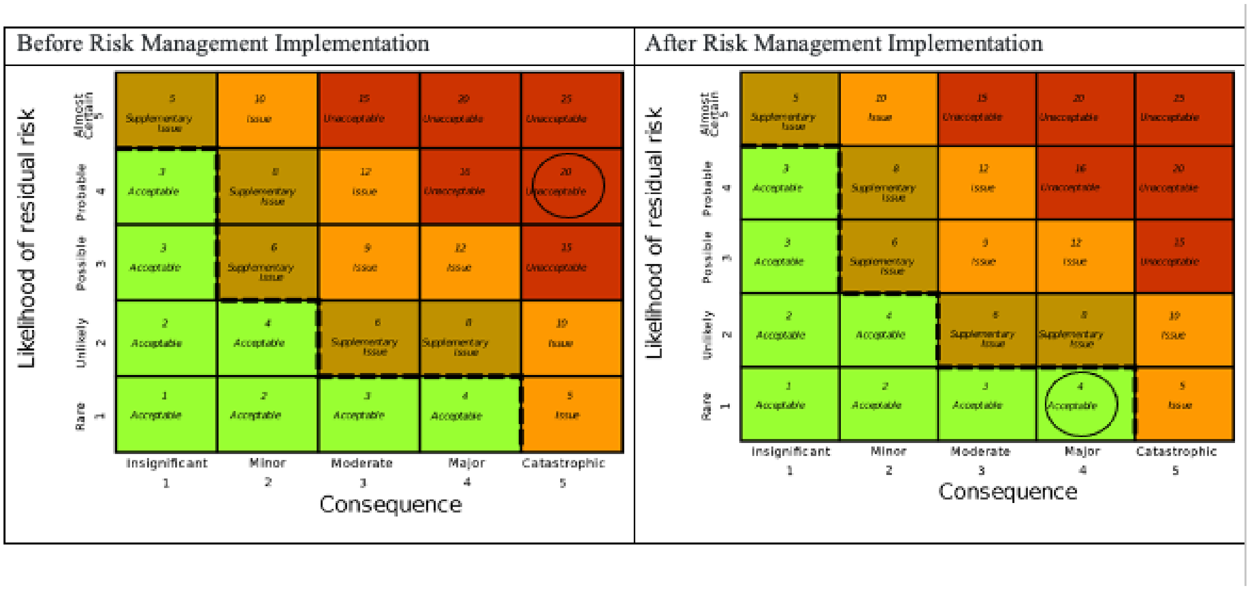
Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	4 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Figure 9.1.4: Data Breach Risk Assessment

5. Privacy shown in Figure 9.1.5
   a. Data is encrypted using AES encryption algorithm
   b. Data will not be directly tied to username. Will be using a unique ID generated at time of enrollment.

c. The ID is tied to the logging database that will track names. Need both databases to access.



Before Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	10 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

After Risk Management Implementation

Likelihood of residual risk	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain 5	5 Supplementary Issue	20 Issue	15 Unacceptable	20 Unacceptable	25 Unacceptable
Probable 4	3 Acceptable	8 Supplementary Issue	12 Issue	16 Unacceptable	20 Unacceptable
Possible 3	3 Acceptable	6 Supplementary Issue	9 Issue	12 Issue	15 Unacceptable
Unlikely 2	2 Acceptable	4 Acceptable	6 Supplementary Issue	8 Supplementary Issue	10 Issue
Rare 1	1 Acceptable	2 Acceptable	3 Acceptable	4 Acceptable	5 Issue

Consequence

Figure 9.1.5: Privacy Breach Risk Assessment

9.2 Technical Readiness Levels

Level 1 – Basic Principles Observed and Reported

- Research biometric sensors and their execution.
- Research modularity design
- Begin database specification
- Design algorithms for biometric scans.

Level 2 – Potential Application Validated

- Algorithms to be decided
- Communications method to and from DBs decided.
- Choose a handful of modularity options

Level 3 – Proof-of-Concept Demonstrated, Analytically and/or Experimentally

- Validate which modularity designs work in our scenarios
- Have a database design completed
- Have network communications completed.
- Validate data is being encrypted

Level 4 – Component and/or Breadboard Laboratory Validated

- Rough design of scanning system that has modularity built in.
- Have communications from DB and scanners validated.

Level 5 – Component and/or Breadboard Validated in Simulated or Real Space Environment

- Finalize hardware design of scanners
- Test hardware design of scanning systems in various environments. Tweak as needed
- Validate that sensors are able to withstand harsh environments and abuse.

Level 6 – System Adequacy Validated in Simulated Environment

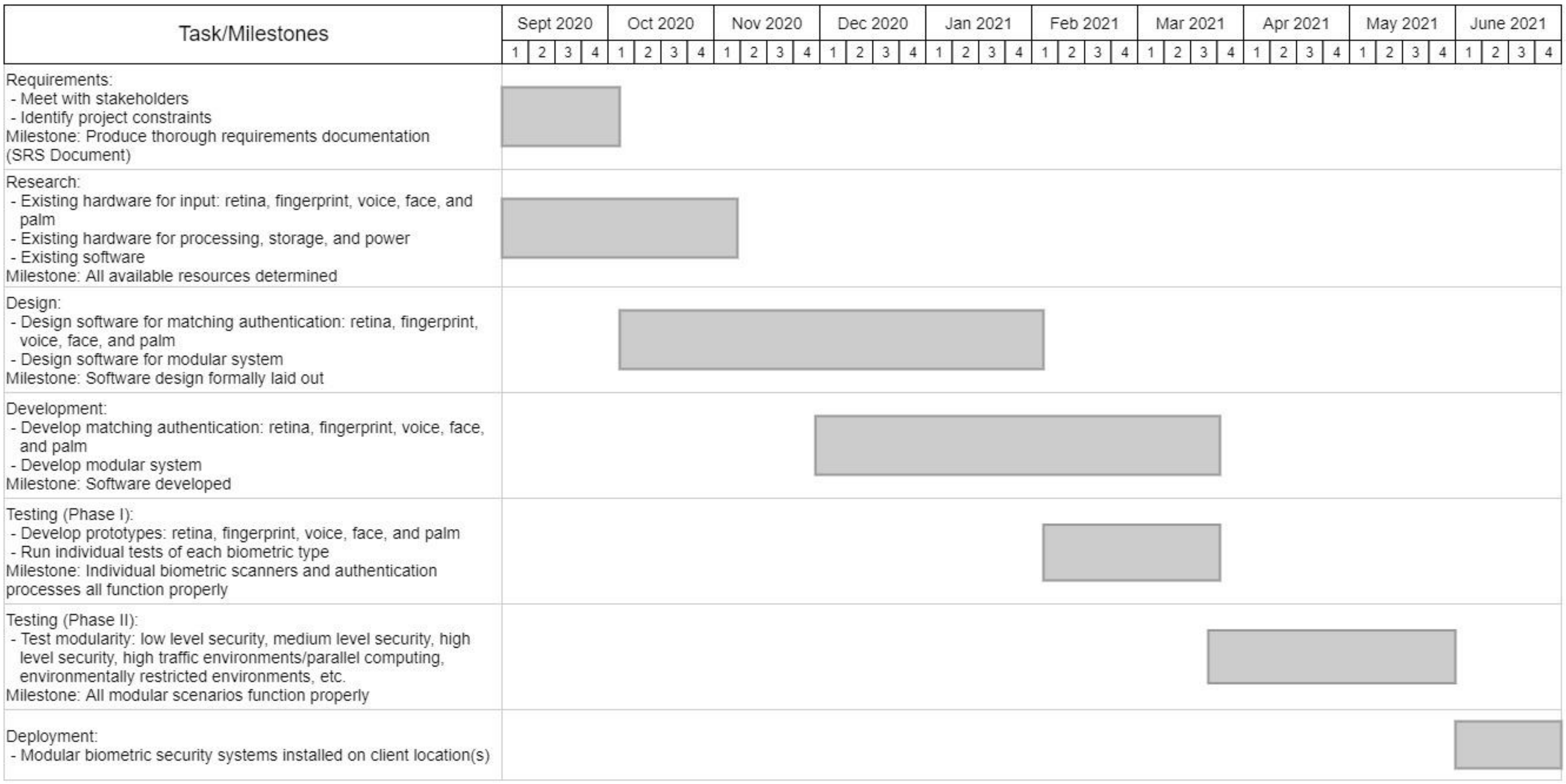
- Begin small scale deployment of systems in an uncontrolled environment.
- Validate performance of system.

Level 7 – System Adequacy Validated in Deployment

- Begin full scale deployment of the system.
- Support system as needed based upon customer.

10. Schedules and Milestones

The project has been compartmentalized into cohesive sections as follows: Requirements, Research, Design, Development, Testing (Phase I), Testing (Phase II), and Deployment. Each section has its specific project milestone as shown in Figure 10 that will be reached at competition of said phase. The modularity of our system allows for minimal interdependency between these processes until testing prototype multi modular systems. This schedule is designed to have systems securely up and running within 10 months.



Task/Milestones	Sept 2020				Oct 2020				Nov 2020				Dec 2020				Jan 2021				Feb 2021				Mar 2021				Apr 2021				May 2021				June 2021			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Requirements: - Meet with stakeholders - Identify project constraints Milestone: Produce thorough requirements documentation (SRS Document)	▨	▨	▨	▨																																				
Research: - Existing hardware for input: retina, fingerprint, voice, face, and palm - Existing hardware for processing, storage, and power - Existing software Milestone: All available resources determined	▨	▨	▨	▨	▨	▨	▨	▨	▨																															
Design: - Design software for matching authentication: retina, fingerprint, voice, face, and palm - Design software for modular system Milestone: Software design formally laid out					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨																				
Development: - Develop matching authentication: retina, fingerprint, voice, face, and palm - Develop modular system Milestone: Software developed													▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨													
Testing (Phase I): - Develop prototypes: retina, fingerprint, voice, face, and palm - Run individual tests of each biometric type Milestone: Individual biometric scanners and authentication processes all function properly																					▨	▨	▨	▨	▨	▨	▨													
Testing (Phase II): - Test modularity: low level security, medium level security, high level security, high traffic environments/parallel computing, environmentally restricted environments, etc. Milestone: All modular scenarios function properly																												▨	▨	▨	▨	▨	▨	▨	▨	▨				
Deployment: - Modular biometric security systems installed on client location(s)																																					▨	▨	▨	▨

Figure 10: Schedules and Milestones

11. Testing and Deployment

11.1 Test Plan

Each test procedure shall contain the following:

1. Test Identification Number (MM - ###): Each test shall have a unique ID number. The module acronym (MM), and number.
2. Code Modules/Procedures included in the test.
3. Test Objective.
4. Special Test Environment Requirements: Description of any hardware and software needed for the test.
5. Step-by-step Instructions: Include any setup procedures.
6. Test Inputs: Variable names, values, where applicable.
7. Expected Results: Include all pass/fail criteria.
8. Test Limitations/Constraints (if any): Additional comments where needed.

Figure 11.1 Test Plan Flow Diagram

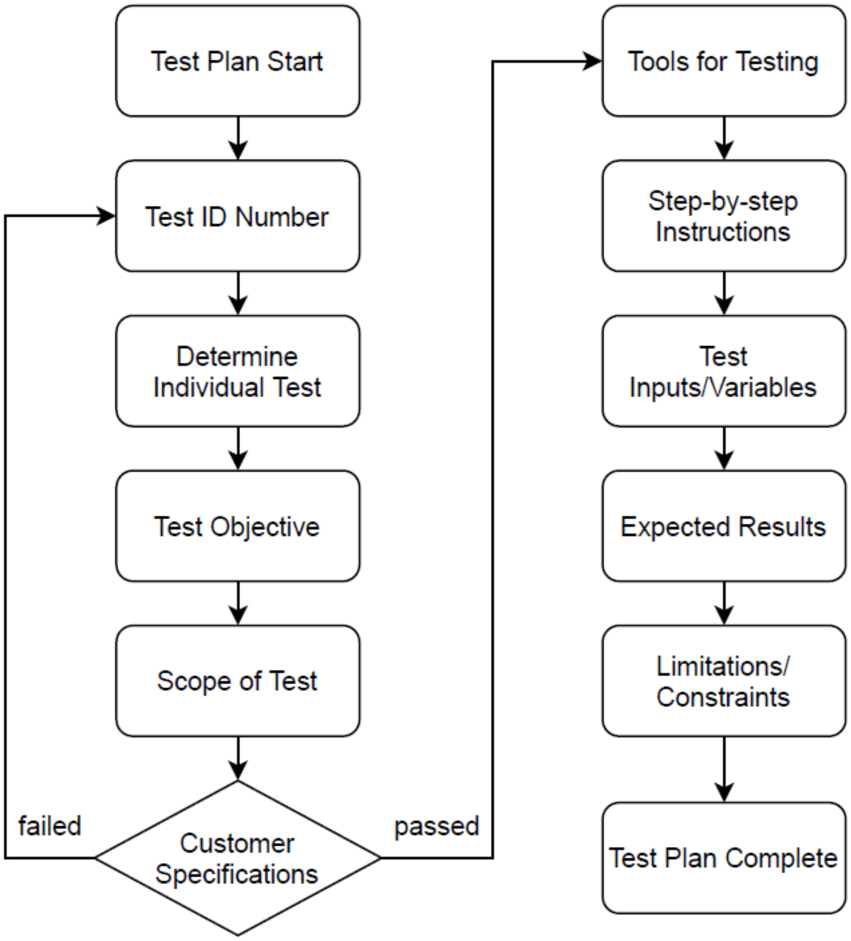


Figure 11.1: Test Plan Flow

Each time a test procedure is executed, the test engineer shall prepare a test report consisting of the following:

1. Test Procedure Number.
2. Revision Dates.

3. Reason for Test.
4. Test Date.
5. Name of Test Engineer.
6. Test Environment Used.
7. Actual Results.
8. Test Evaluation.

Figure 11.2 Test Activity Diagram

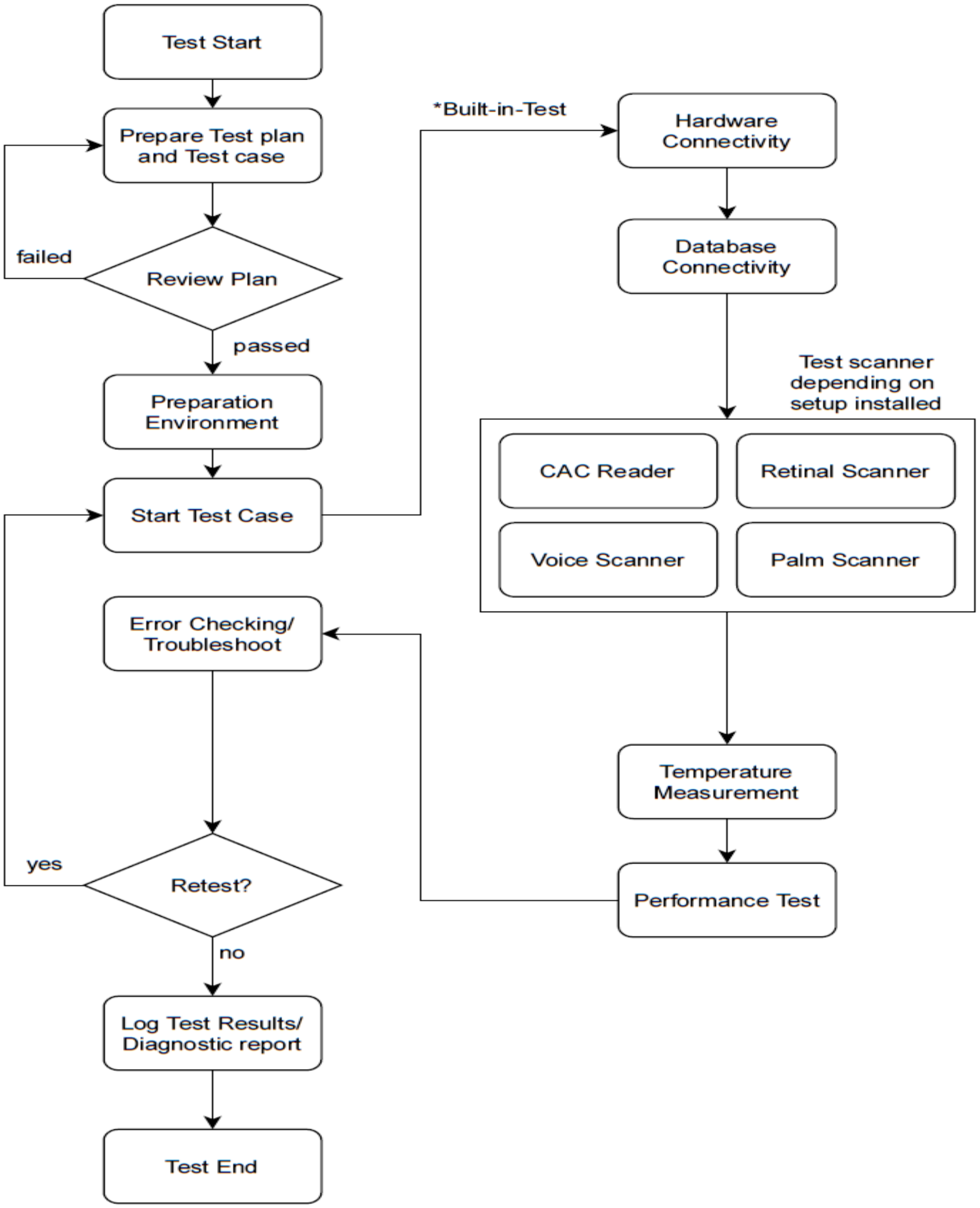


Figure 11.2: Test Activity Diagram

System Code and Test:

- Prior to installation, each system is debugged to the point of successful compilation to eliminate all syntax and coding errors.
- Each system is then tested for required functionality as detailed in the requirements document. Pass/fail criteria, measurable parameters, and tolerances will be specified and tested for the designated test cases.

Hardware Test:

- Protection and sealing of system hardware shall be tested in varying conditions; heat, cold, dust, rain. The hardware shall meet or exceed IP65 rating.

11.2 Deployment Plan

This section provides detailed information on the deployment of the system including installation schedule, resource requirements, technology infrastructure, support considerations, and training requirements.

Deployment schedule and resource requirements

Target Deployment and Sequence	Scheduled Release Dates	Resource Requirements
Bldg 76, Main Entrance, Fort Bragg, NC	**12/01/2020**	**1 software developer + 1 hardware tech**
Bldg 360, Room A, Fort Bragg, NC	**12/02/2020**	**1 software developer + 1 hardware tech**
Bldg 81, Room J, Joint Base Lewis-Mcchord, WA	**12/7/2020**	**1 software developer + 1 hardware tech**

Technology, infrastructure, and support considerations

Target	Technology/Infrastructure Requirements	Support Requirements
Bldg 76, Main Entrance, Fort Bragg, NC	**Outdoor system install. CAC and voice scanners only.**	**Contact site POC upon arrival for access**
Bldg 360, Room A, Fort Bragg, NC	**All-scanners install.**	**Access to site requires military police escort**
Bldg 81, Room J, Joint Base Lewis-Mcchord, WA	**CAC, retinal, hand scanners only.**	**Access to site requires military police escort**

Training Requirements:

Training will be limited to military personnel whose job is to maintain systems and software operations of the building. i.e. Cyber-security officer, cyber-security specialist, staff civilian IT technician. They will be trained to perform basic troubleshooting of software, accessing log files, and basic maintenance of the system.

Site	Scheduled Dates	Trainer	Materials
Stimson Hall, Fort Bragg, NC	**12/3/2020**	**Software developer**	**System manual**
Waller Hall, Joint Base Lewis-Mcchord, WA	**12/8/2020**	**Software developer**	**System manual**

12. Maintenance

12.1 Software Maintenance and Support Plan

- The firm (our team/company) is responsible to coordinate the continuous maintenance of the software components developed for this system. The firm shall furthermore strive to preserve system stability and reliability so that users can rely on them.

Component Releases

- Major component releases will be delivered periodically, tentatively once a year in the month of December to provide a good balance of stability and innovation.
- Minor component releases will be delivered more frequently as dictated by the user feedback.
- Revision releases will be made to fix specific defects found in the software.
- Emergency release will be made to fix immediate-priority defects found in the system; i.e. security issues.

Incidents, problems, and changes

- A change is the addition, modification, or removal of services or service components.
- An incident is an unplanned interruption to the system service or reduction in quality of the service.
- A problem is the cause of one or more incidents.
- Our team's maintenance team will be responsible for the investigation of any incident, problem, or change that occurs when a system fails to operate optimally.

User Support

- A helpdesk technician shall be the primary point-of-contact for the user to get support.
- Requests for support will be on a first-come-first-served basis, and the severity of the problem.

Incident Resolution

- Upon receiving an incident report, maintenance teams shall restore system functionality as quickly as possible to ensure service quality and security integrity.
- The incident report shall stay open until a satisfactory solution for the user has been found.

Glossary

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