**CPSC 362 Class Project:**

**Group 1**: Subject Material: Multimodal Biometrics

**Group 1 Members**: Brian Tan, Davina Doran, Fulya Kocaman, Konnor Gutierrez

**Homework 2:** Write a Requirements Document

**Part 1:** General Requirements

1. What are the objectives of the system?

* 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

1. What is to be accomplished?

* Increase security through the use of unique identifiers (iris, fingerprint, voice, face, hand geometry)
* Add additional security authorization in the event another fails
* Logging of events of who accesses
* Mitigate intrusion of unauthorized personnel.

1. How does this fit into the needs of the military?

* Secures valuable data/high clearance buildings and rooms
* Allows for biometric tracking of who has accessed these secure locations/devices
* Mitigates intrusion via stolen credentials.

1. How is the product going to be used?

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

1. Who are we asking about this?

* The client (military/private security)

Eric - This is a start but what about

This might help

<https://www.sampletemplates.com/business-templates/requirement-document.html>

# **Types of Requirements**

Cost Interface

Customer Performance

Derived Schedule

Environmental Time

Functional

# **Performance Requirements**

Quantity – How Many, How Much

Quality – How Well

Coverage – How Much Area, How Far

Timeliness – How Responsive, How Frequent

Readiness – Availability, MTBF

# **Sources of Requirements**

User Goals / Desires:

- A fast and smooth process of identity verification. (the whole process should be faster than the status quo of using a CAC (common access card). Higher speed of the process will also decrease the wait times of people in line.

Standards / Specifications:

- System must meet standards outlined in the Department of Defense Information Technology Standards Registry (DISR).

- System must have IP rating of 65 or higher; protection from entry by tools, wires, or brute force, dust tight, moisture protection. Outdoor systems must withstand elements of the region; high temperatures, snow, rain, wind, hail.

Laws and Regulations:

- System must be in compliance of mandates detailed in the National Institute of Standards and Technology 800-171 (NIST 800-171) Special Publication. The DOD requires all IT related systems to meet or exceed the minimum cyber-security standards described in the NIST 800-171 publication.

Systems Analysis – Derived Requirements:

- System must 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.

Solution Dependent

Technology:

- Scanners must meet or exceed industry standards of scanner/machine learning technology.

Interface Definition:

- The system will comprise of a combination of recognition technologies; iris, fingerprint, voice, face, hand geometry recognition software. As such, the system interface will 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 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.

Engineering Specialties:

- 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.

- Software engineers proficient in cyber-security and machine learning software development. Cloud computing engineers to maintain sensitive data.

-Hardware engineers capable of installing the system and deploying it.

Risk Management:

- Determining which technology to use at each access point, or a combination of technologies. If possible, develop 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, system must be intuitive to shut down.

- In the event of unauthorized tampering of the hardware, system must be intuitive to alert the administrators, and shut down, maintain door lockdown to protect from unauthorized access.