

Prototype and Testing

The Gentleman's Guild of Engineering Excellence

Ghadi Al Khorl, John Darling, Gordon McGinn, Sean McGonigal, and Devin Myers

Shabodi Client Project

October 27, 2024

Table of contents

1. Summary of Project Direction	3
Security in Two Parts	3
2. Detailed Design	4
Technical Flowchart	4
Detailed Summary for Flow of Data	5
3. Economics and Component related costs	6
Component Selection	6
4. Project Task Plan (Design Day Nov 28)	8
Real Time	8
Tasks (Ordered based on Priority w/ Dates & Engineer)	8
Soft Time	9
Tasks (Ordered based on Priority w/ Dates & Engineer)	9
5. Test Plan	10
Real Time	10
Soft Time	11

1. Summary of Project Direction

Security in Two Parts

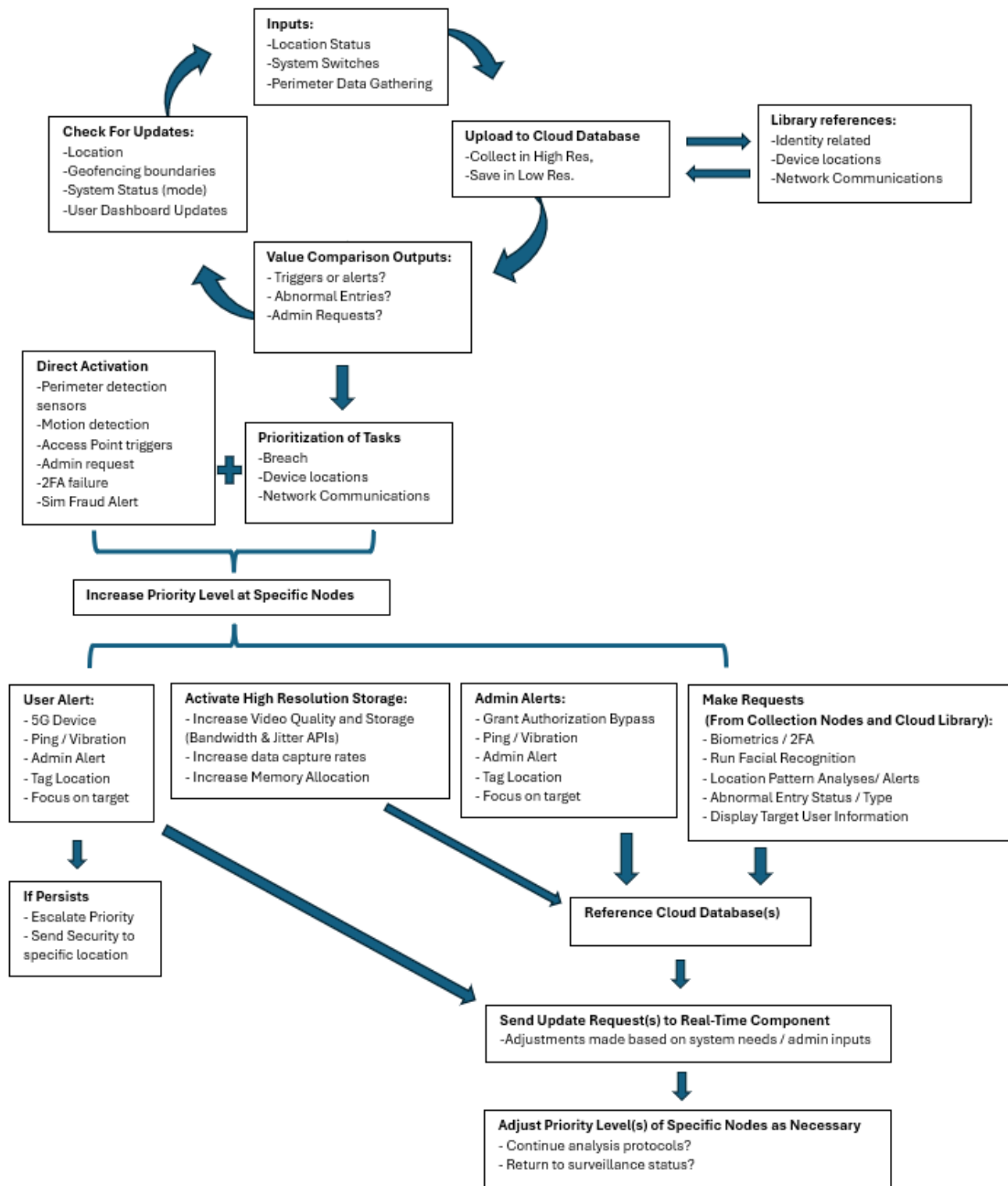
To solve the problem of a NetAware restriction zone security system, it has become evident that careful consideration is to take place at each stage of a secure entry system. There are two primary stages to our system design: real-time surveillance / breach detection, and soft-time breach recognition / investigation.

The primary focus of the real-time detection system is to collect raw data from multiple sources. This can be regarded as the perimeter monitoring system. This component is a loop circuit, providing a cloud database with updates to location values, sensor statuses, and users linked to the local network, comparing them against stored normal values to mark potential breaches. To optimize network bandwidth, this stage focuses on collecting bulk quantities of low resolution data (especially in terms of video surveillance).

Any values that indicate a possible breach or unwanted entry directly stimulate the linear and recognition focused soft-time protocols (soft-time = increased latency). Tripped sensors/ trigger events shift the priority status at specific input nodes, initiating higher resolution data collection at all relevant sensors near and involved in the breach. This component is also responsible for updating the priority status of subsystems, as well as elucidating, documenting, and reporting to all parties of interest relevant information as an event runs its course.

2. Detailed Design

A. Technical Flowchart



B. Detailed Summary for Flow of Data

Real-time data gathering begins as a series of inputs from various sources. Packet collection is unloaded at the cloud library for temporary storage (period of storage TBD) in its appropriate file (User related, Admin Related, Breach Related &c). Defined normal values are stored in respective libraries and are immediately compared against to determine alert/ priority status. Regular surveillance monitoring requires no change in alert status. System then verifies that no updates are required (no video requests, manual admin changes, &c), and continues low resolution data gathering. If alert detected in value comparison, then prioritization protocols ensue, initializing soft-time data analyses. Certain trigger switches at the input source, if above disruption threshold will also directly trigger soft-time protocol.

In the event of an unwanted entry event or alert, via direct activation by means of trigger switch or by value comparisons, nodes at target locations immediately gain an increased priority status, initiating several functions. Target user device receives an alert notification, high resolution data collection at surrounding area is initialized, administrator receives alert of breach, and secondary security protocols are requested. In all cases, the cloud acts as a means to document, and save records of events. In secondary analysis, cloud also acts as relay updates for immediate integration to real-time systems. When event values return to identical to surveillance thresholds, priority status of environment local to respective breach alerts decrease, or are manually decreased by admin, surveillance protocol recommences. If the event(s) continue past a predefined period, priority is escalated automatically, and further security measures are undergone.

3. Economics and Component related costs

A. Component Selection

Category	Actual Expenses	Difference
Motion Sensor	\$3	$\$25 - \$3 = \$22$
Phone	\$0	$\$22 - \$0 = \$22$
Internal/External API's	\$0	$\$22 - \$0 = \$22$
Camera	\$0	$\$22 - \$0 = \$22$
User-Registration Portal	\$0	$\$22 - \$0 = \$22$
Server/Cloud Storage	\$0	$\$22 - \$0 = \$22$
Geolocation (BLE) Beacons	\$6	$\$22 - \$6 = \$16$
5G Sim Cards	\$0	$\$22 - \$0 = \$16$
Phone Integration	\$0	$\$22 - \$0 = \$16$
Phone Verification	\$1	$\$16 - \$1 = \$15$
Backend Database	\$0	$\$15 - \$0 = \$15$

B. Justification

Motion Sensor (\$3):

Justification: Motion sensors are essential for security in zones where users' physical presence needs to be detected. These can help track movements, identifying unauthorized entries in real-time, and offer a first line of defense when monitoring restricted areas. The low cost makes them very affordable within the budget.

Phone (\$0):

Justification: Phones are being used as part of the system, but since users are expected to have their own devices, no additional cost is incurred. This is beneficial as it allows the system to leverage existing hardware and remain cost-effective.

Internal/External APIs (\$0):

Justification: APIs (Application Programming Interfaces) allow different parts of the system to communicate seamlessly, such as checking access credentials against the database. While there is currently no cost listed, it's important to allocate funds for potential future integrations that may require API usage or licensing.

Camera (\$0):

Justification: No cost has been allocated to cameras, we have our own camera. This is reasonable for face recognition throughout the security process.

User-Registration Portal (\$0):

Justification: A user-registration portal is critical for managing and verifying the users who will be allowed access. The system can remain within budget by using a free or low-cost solution for the portal, such as leveraging open-source software.

Server/Cloud Storage (\$0):

Justification: Data storage is necessary to store access logs, user credentials, and related information. Since no cost is shown, this could mean the project is planning to use free tiers of cloud storage or is still evaluating options. Eventually, some cost may arise if the system scales.

Geolocation (BLE) Beacons (\$6):

Justification: Bluetooth Low Energy (BLE) beacons are crucial for accurately determining user location within the facility. These ensure that the system knows which users are in which areas, preventing unauthorized access. The \$6 cost is reasonable considering the benefit of precise location data for security purposes.

5G SIM Cards (\$0):

Justification: SIM cards allow users' phones to connect to the system and access its features. Since there is no cost listed, it suggests that users provide their own SIM cards, or the system is designed to leverage existing infrastructure. This approach keeps expenses minimal.

Phone Integration (\$0):

Justification: Integration with users' phones is essential for seamless interaction with the system (e.g., scanning into zones or receiving alerts). If the integration is being handled by existing frameworks or free tools, the \$0 cost is justified as it avoids unnecessary expenditure.

Phone Verification (\$1):

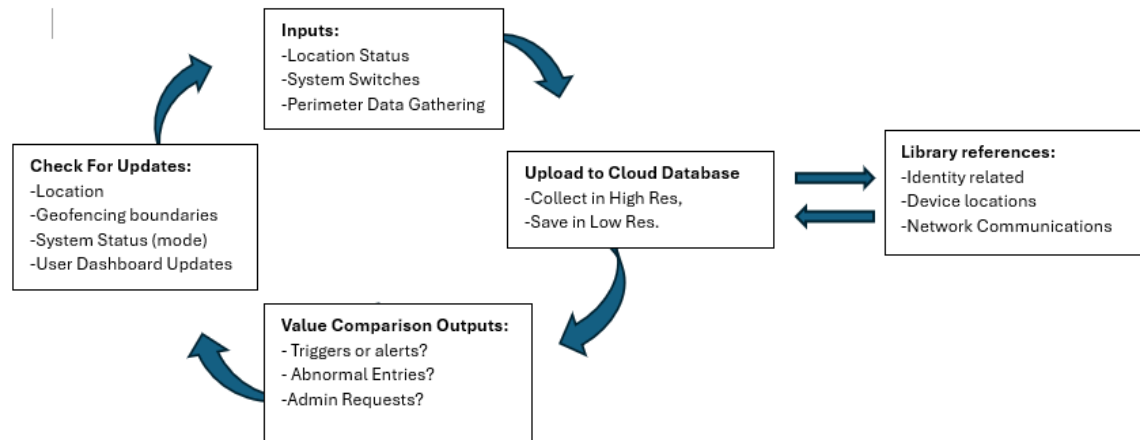
Justification: Phone verification ensures that users are authorized to use the system through a secure process, such as SMS verification. The low cost here is efficient and necessary, as it strengthens the overall security by ensuring the right users are associated with the right phones.

Backend Database (\$0):

Justification: A backend database is critical for storing user access data and authorization levels. The \$0 cost could indicate the use of free tiers from cloud providers like AWS, Google Cloud, or Firebase. While initially cost-free, future upgrades may require additional investment.

4. Project Task Plan (Design Day Nov 28)

Real Time



The Real time aspects of this project focus on all data that must be gathered and analyzed in real time (as it's happening). This will encompass the gathering of data, sending it to the cloud and making necessary triggers activate based on the data gathered.

Lead Engineers:

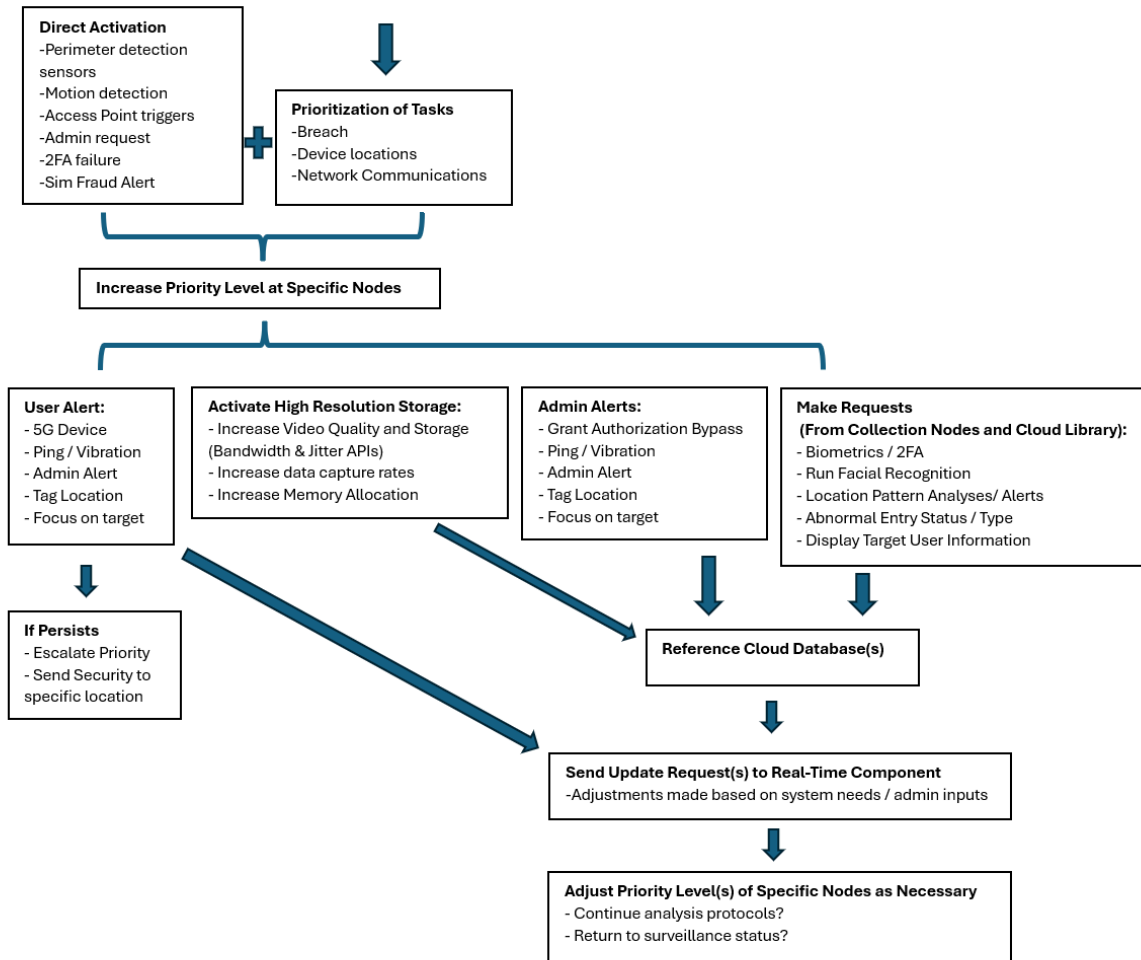
Devin

John

Tasks (Ordered based on Priority w/ Dates & Engineer)

- Gathering data from SIM location: Nov 2 - Devin, John, Ghadi, Gordon, Sean
- Sending data to the cloud: Nov 2 - Devin, John, Ghadi, Gordon, Sean
- Geofencing of area Nov 9 - Devin
- Boundary system: Nov 16 - Sean, Ghadi
- Alerting from boundary:
(ability to identify SIM in zones/trigger system when in a no-go zone)
- Detect person in an area: Nov 16 - Ghadi, John,
(reduced bandwidth)
- Recognize person in area: Nov 16 - Gordon, Devin
(increase in bandwidth of cameras)
- Send data to soft time: Nov - 23 Sean, John
- UI development/refinement: Oct 27- Nov 27, Devin, John, Ghadi, Gordon, Sean

Soft Time



The soft time aspects of this project focus on all data further investigated following collection. (Increased latency vs real time). It encompasses the updating of system needs, and relays communications between the admin and the network to the software.

Tasks (Ordered based on Priority w/ Dates & Engineer)

- Increase video quality along with memory allocation and priority level: Nov 9 - John, Ghadi
- Increase AI resource allocation: Nov 9 - John, Gordon
- Location feedback: Nov 9 - Ghadi, Sean
- User Alert (vibration): Nov - 23 Devin, Gordon
- Admin alerts: Nov - 23 John, Ghadi
- Live stream: Nov - 23 Sean, Gordon
- Admin controls (dashboard options): Nov - 23 Devin, Ghadi

5. Test Plan

A. Real Time

Test#	Reason	Metric Criteria	Level of Prototype	Kind of Prototype	Metrics	Test Desc.	Analysis method	Notes
1	Can we gather location data?	Ability to locate, track and store data.	Focused LoFi	Physical	co-ordinates	Run the code, track a sim. See if we can get its location data	1 min track, locations close + far. Need a computer and sim card	
2	Does the boundary system work?	Real time alert on phone of breach >1sec	Comprehensive HiFi	Physical	>1 sec alert +data sent to cloud	Run the code, track a sim as it enters a restricted zone.	1 sim card track, test entries from multiple zone angles.	
3	Does the camera increase quality when a non-registered detection is made?	Camera quality must increase once a person is detected so it can be recognized.	Comprehensive LoFi	Physical	>1 sec change in camera quality after detection	Run the code, a person as it enters a restricted zone, see how fast code changes to high bandwidth	1 person enters from multiple zone angles, without sim.	

B. Soft Time

Test#	Reason	Metric Criteria	Level of Prototype	Kind of Prototype	Metrics	Test Desc.	Analysis Method	Notes
1	Confirm system response to user alerts	System generates appropriate alerts	Comprehensive LoFi	physical	Response time (ms), >95% alert accuracy (% correctly identified?)	Test system's ability to notify users when an event is detected	Simulate alerts and see if the system correctly identifies area/alert type	Focusing on functionality, not necessarily response time
2	Does the camera recognize the person?	Camera can correctly identify a person	Focused LoFi	physical	>90% identification accuracy	Setup the camera and facial recognition AI, see if it can correctly recognize and identify people	Have a person's face in view from the camera	
3	Validate resource usage	Is the resource usage acceptable?	Comprehensive HiFi	physical	<15% usage of total bandwidth available	Setup the prototype and monitor bandwidth usage	Have geolocation, and cameras running at the same time. Monitor bandwidth usage while simulating an alert	