

Project Brief

Design Criteria and Target Specifications

Unwanted Entry (UE), and Restriction Zones

The Gentleman's Guild of Engineering Excellence

JOHN DARLING, GHADI AL KHORI, GORDON MCGINN,

SEAN MCGONIGAL, AND DEVIN MYERS.

Client: Shabodi Corp, Toronto, ON

GNG 1103 Client Project Deliverable D

Due Date: October 13, 2024

Conceptual Design

1. Introduction	2
2. Recall: Problem Statement	2
3. Introduction Cont.	2
4. Design Criteria	2
5. Subsystems IN/OUT	3
6. Subsystem Boundaries	4
7. Subsystems	5
8. Overall Systems	8
9. Overall system choice	9
10. Conclusion	9

1. Introduction

This document details the overall concept and underlying subconcepts of the system to be created, based upon data collected during the “Design Criteria and Target Specifications” project brief document. Listed in this document are three concepts for a theoretically fully functioning solution for our problem statement.

2. Recall: Problem Statement

Private network users need a way to establish restriction zones within a cloud compatible security system that can identify, halt, and directly alert relevant parties of unwanted entry events.

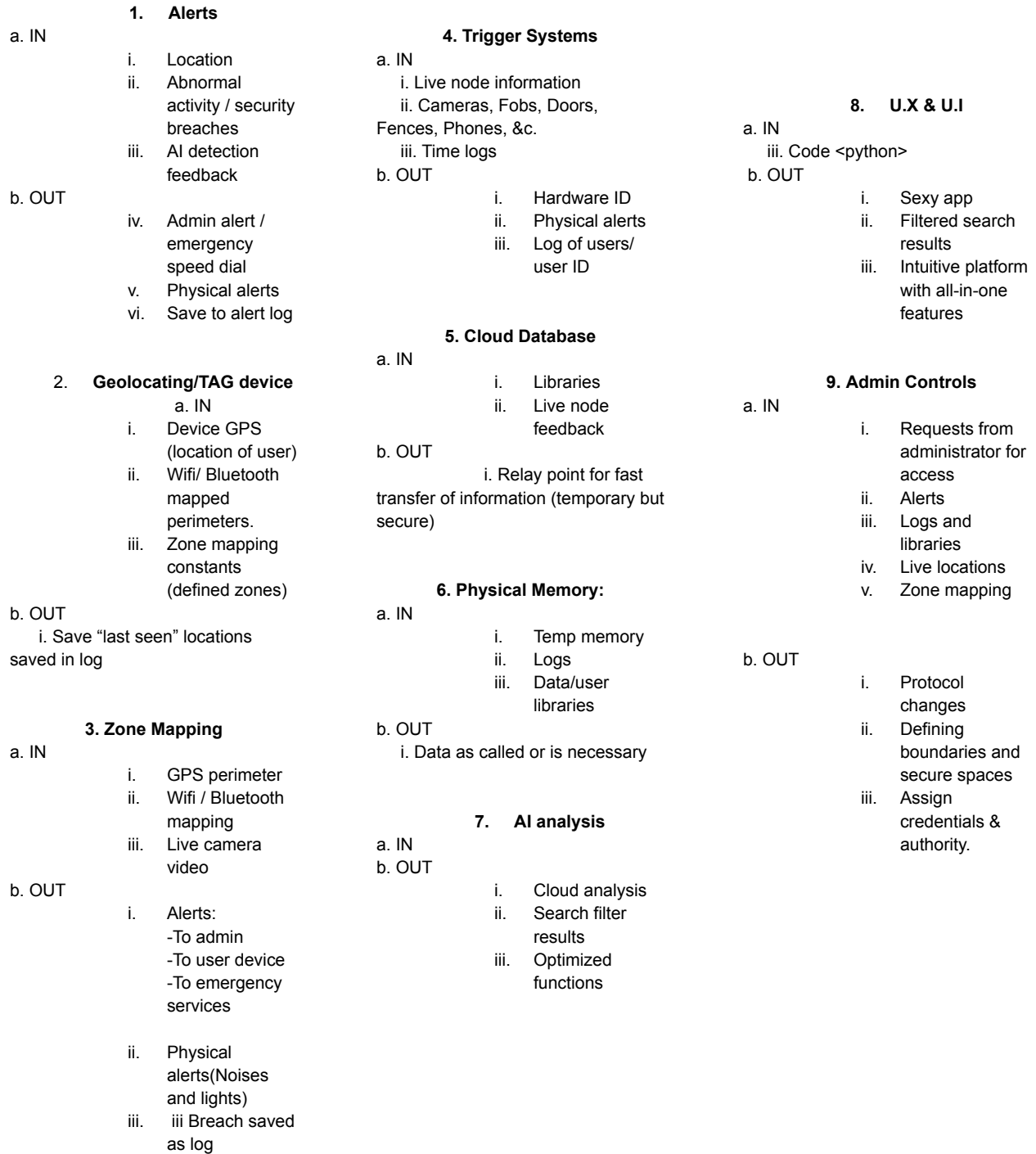
3. Introduction Cont.

Each system is broken down into its respective subsystems, with defining characteristics and boundaries. Boundaries between the subsystems were identified as being semi-critical to client needs (Shabodi being the initial client, rather than end user). The ability to use API's and subroutines in a modular fashion will allow for: more efficient testing of prototypes against critical metrics, more efficient future updates, and problem isolation.

4. Design Criteria

ID	Design Spec	Relation (=,<,>)	Value	Units
1	Location Tracking	<	1-5 (depends on zone)	Meter(s)
2	Alerts	=	1	Second(s)
3	Detection of entry	<	1-5 (depends on zone)	Second(s)
4	Logs	=	User Defined	Months-years
5	Ease of use	<	0.25	Second(s)
6	Setup	<	2	Days

5. Subsystems IN/OUT



6. Subsystem Boundaries

Alerts

Does not identify security breaches. This subsystem acts once the trigger system identifies and sends the necessary data to the alert subsystem for programmed response.

Geolocating/TAG device

This system only tracks location based on private network parameters. Does not map out zones.

Zone Mapping

Gives the user the ability to map out zones based on data collected through cameras and other devices. Provides Alert, geolocating, and trigger subsystems with necessary data for their systems. Doesn't track or send out alerts itself.

Trigger Systems

Uses Zone mapping, geolocation and alert data to take real time data in conjunction with keyfobs, doors, phones, etc, to trigger the alert and trigger subsystems into action.

Cloud Database

Stores important data logs based on importance of events & severity of events. Does not perform any actions other than storage.

Physical Memory

Long term storage for critical data and libraries. Does not perform any real-time processing.

AI analysis

Processes data and provides threat/breach detection. Data sent to necessary subsystems for actionable procedures. Does not store data.

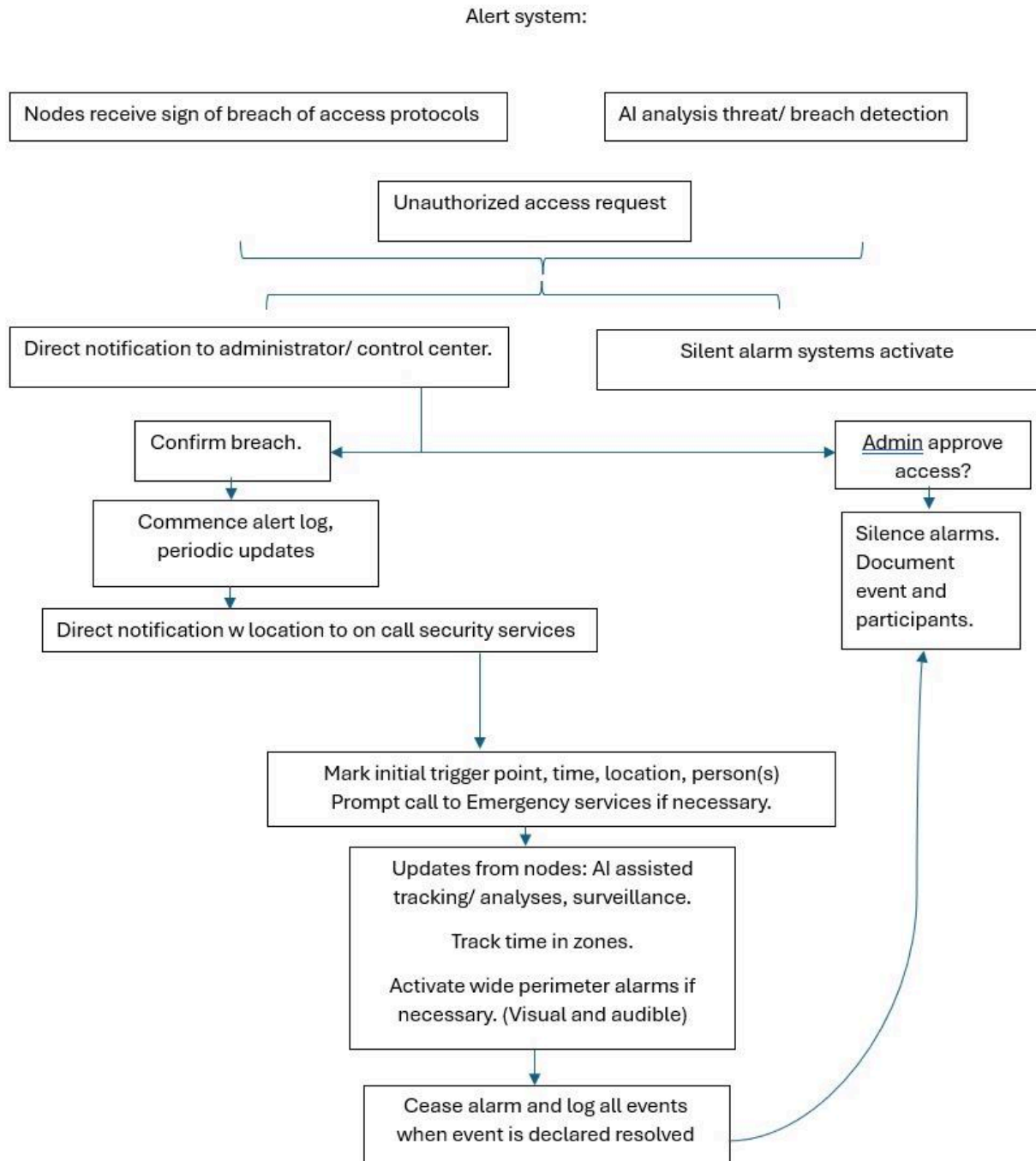
U.X & U.I

Displays data to users, as well as provides a platform for set up and use. Does not store information or process zone detection. A combination of subsystems can alert a single UI (ex: phone app) to inform it is in a restricted zone.

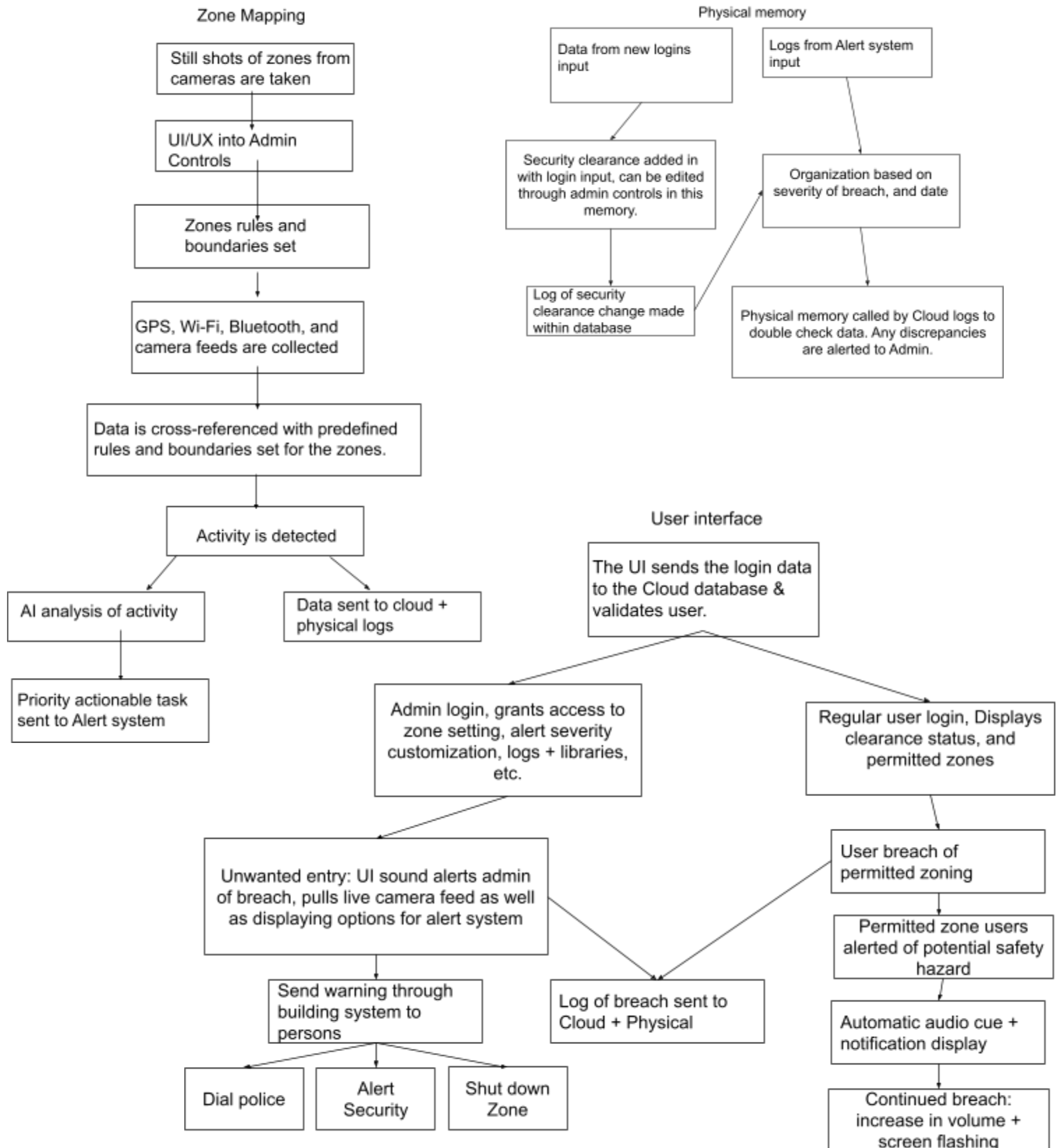
Admin Controls

Used for system management, acts as the central hub for access into zone mapping customization, alert severity control, etc. Does not perform those subsystems, simply acts as secure access into the.

7. Subsystems

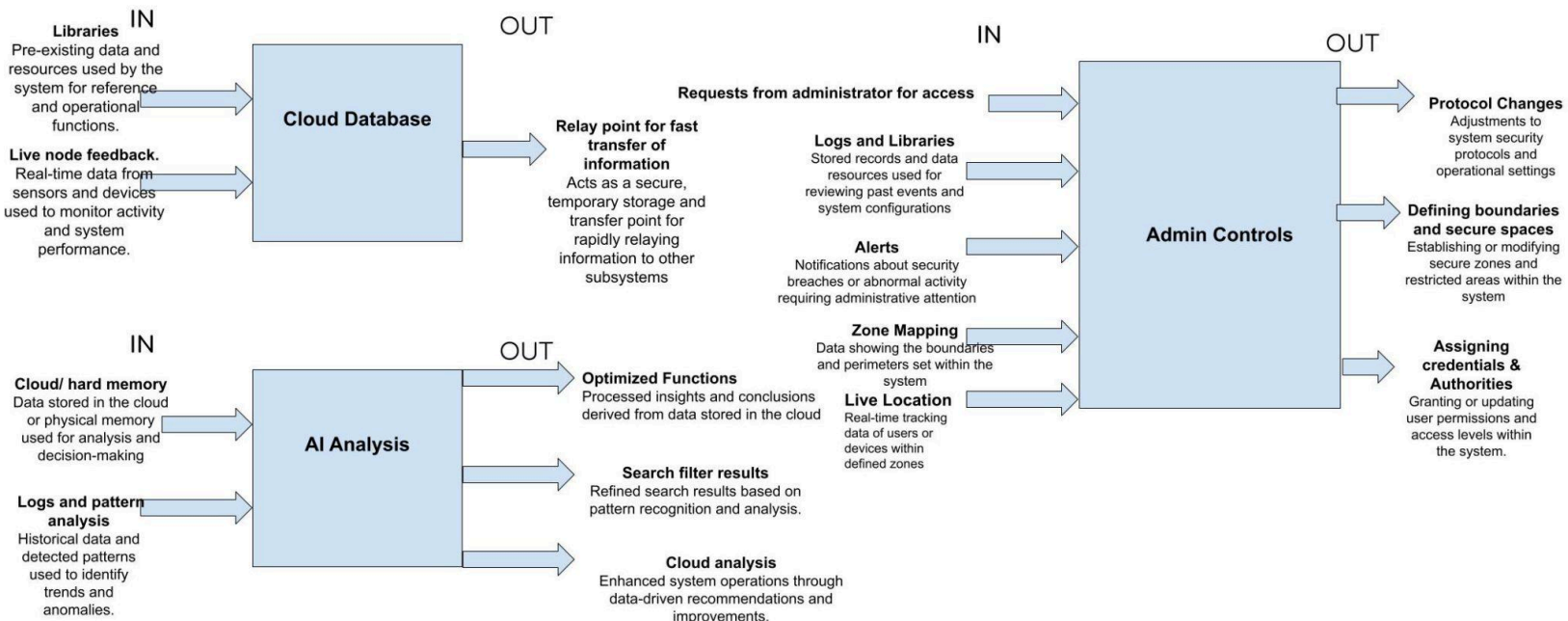
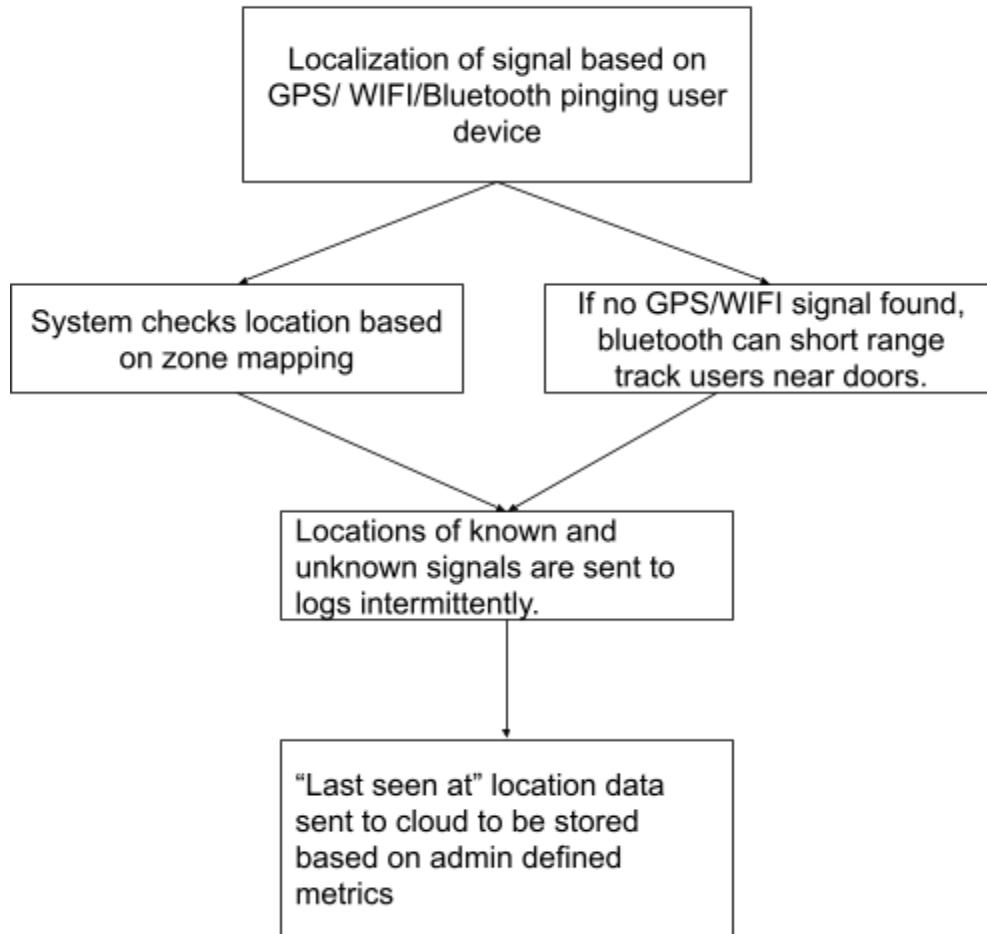


Conceptual Design

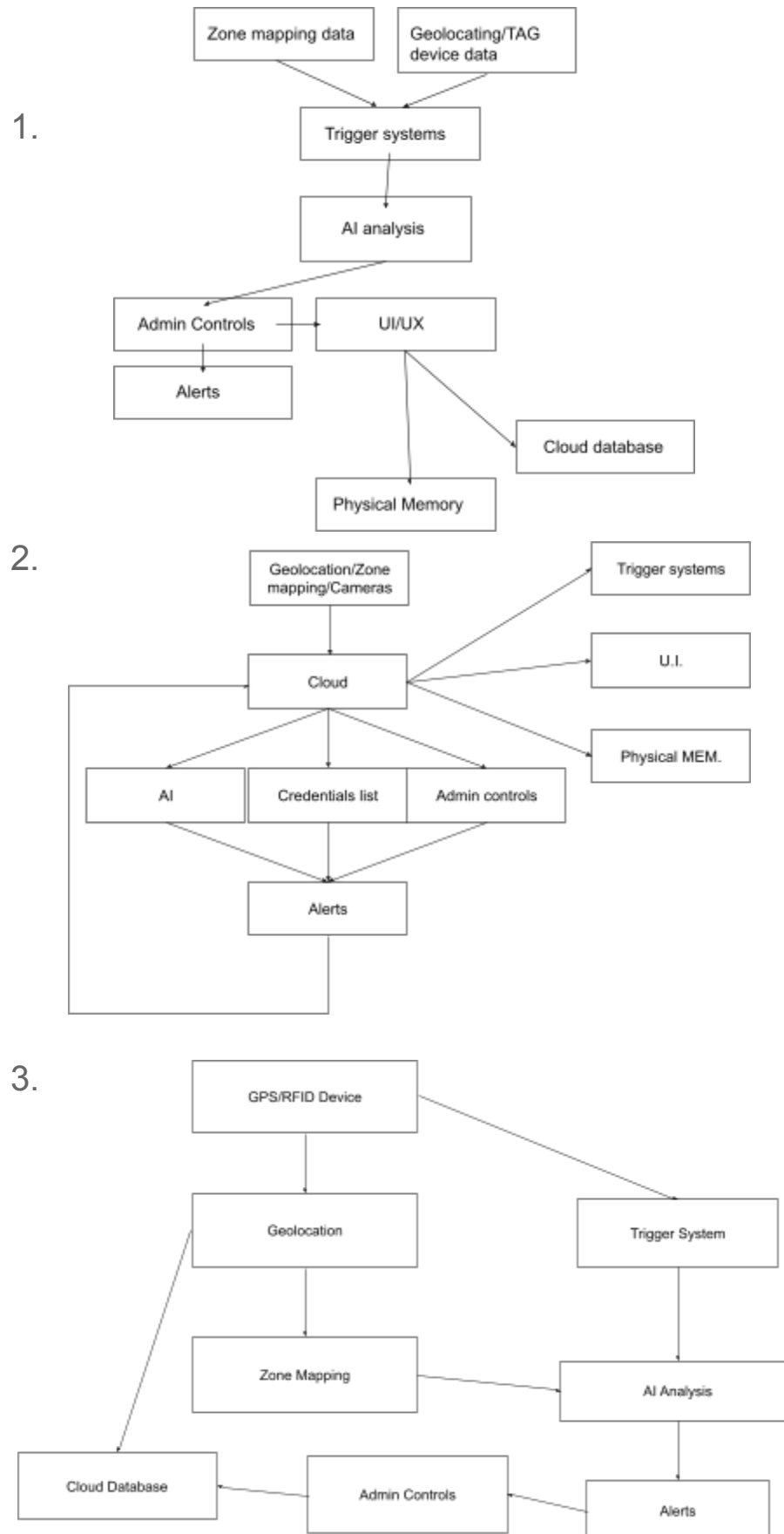


Conceptual Design

Geotracking/ TAG device



8. Overall Systems



9. Overall system choice

Design 1 was chosen for the overall system flow through all subsystems in the most efficient manner. This will allow for the theoretical fastest run time of the program, ensuring metrics will be met or exceeded as testing gets under way. Focusing on when zones are breached, security measures and alerting admin, this flow ensures that the problem statement maintains the main focus of the system. Leaving the update to physical memory and the cloud database until last ensures all data collected during an entry (wanted or unwanted) can be logged in a single step. This one step update of system logs will greatly cut down the amount of latency in the private network. It will cut down latency because a lot of small data packets being sent and updated consistently takes up more room for longer on the network, than one slightly larger data packet once in a while. This will also decrease system jitter, as with less data packets there is less of a chance of mistimed data being sent.

10. Conclusion

In conclusion, the design of the cloud compatible security system is driven by the need to establish restricted zones, provide alerts for unauthorized entry and focusing on zone breaches, security measures and alerting admin, this flow ensures that the problem statement maintains the main focus of the system. The system is structured around interconnected subsystems each playing a critical role in ensuring seamless functionality. The nature of these subsystems is key to efficient testing and problem isolation, allowing the system to meet client and end user requirements flexibly. Metrics such as location tracking, alert speed and ease of use are prioritized, ensuring high performance across all components.