Proof of Concept

1. Arkitektur

Enhet: ESP8266 utrustad med en avståndsmätare som mäter signalstyrkan (RSSI) och skickar data över Wi-Fi.

Molntjänst: ThingSpeak används för datainsamling och visualisering. Thingsspeak fungerar som en molnbaserad
tjänst som tar emot och lagrar data från IoT-enheten och erbjuder realtidsvisualisering av insamlad data.

Kommunikationsprotokoll: Datan som skickas från ESP8266 till ThingSpeak är via HTTPS för att säkerställa krypterad dataöverföring.

2. Kommunikationsflöde

Datainsamling: Systemet använder en HC-SR04 ultraljudssensor för att mäta avstånd till närliggande objekt. Avståndet beräknas i centimeter och skickas kontinuerligt till ThingSpeak.

Dataöverföring: Efter att avståndsdata har samlats in skickas det till ThingSpeak över HTTPS för att skydda datan under överföringen.

Databehandling och lagring: Datan lagras och organiseras i ThingSpeak för att underlätta analys och historisk översikt.

Datavisualisering: ThingSpeak används för att visualisera och analysera insamlad avståndsdata i realtid.

3.1 Säkerhetsåtgärder

Implementerat: Datan överförs från ESP8266 till ThingSpeak via HTTPS, vilket är ett sätt att kryptera datan och skydda den från avlyssning.

Framtida förbättringar: Just nu använder vi client.setInsecure() som en tillfällig lösning, vilket innebär att certifikatverifiering inte är aktiverad. En framtida version i produktion bör inkludera certifikatverifiering för att validera ThingSpeaks servercertifikat.

Implementerat: WiFi-uppgifter och API-nycklar sparas i en separat secrets.h-fil. Denna uppdelning ökar säkerheten genom att skydda känsliga uppgifter från att exponeras direkt i huvudkoden.

Framtida förbättringar: Se över möjligheten att kryptera denna fil eller lagra API-nycklar på ett säkert sätt om projektet skalas upp till fler enheter.

3.2 Cyber Resilience Act (CRA) – Efterlevnad

3.2.1 Säkerhet-by-design:

Säkerhet-by-design innebär att säkerhetsåtgärder är integrerade i systemet från början och inte läggs till i efterhand.

Implementerat:

HTTPS-kryptering: Dataöverföring är säkrad via HTTPS för att skydda datan under överföring mellan ESP8266 och ThingSpeak.

API-nycklar och WiFi-uppgifter lagras i secrets.h, vilket minskar risken för att känslig information exponeras i huvudkoden.

Framtida förbättringar:

Certifikatverifiering: I produktion bör certifikatverifiering aktiveras genom att ta bort client.setInsecure() från koden och istället validera ThingSpeaks servercertifikat. Detta förbättrar säkerheten och förhindrar man-in-the-middle-attacker.

3.2.2 Uppdaterbarhet

CRA kräver att IoT-enheter ska ha stöd för säkerhetsuppdateringar för att hantera nya hot och sårbarheter.

Framtida förbättringar:

OTA-(Over-the-Air)uppdateringar: ESP8266 har stöd för OTA, vilket möjliggör fjärruppdateringar av firmware.

En framtida version bör aktivera fjärruppdateringar för att möjliggöra säkerhetsuppdateringar på distans.

Automatiserad versionhantering: Implementera versionskontroll och en rutin för att säkerställa att alla enheter uppdateras till den senaste firmware-versionen vid varje uppdatering.

3.2.3 Sårbarhetshantering

Beskrivning: CRA kräver att systemet ska ha mekanismer för att upptäcka och hantera sårbarheter.

Implementerat:

Serial Monitor-loggning: Alla anslutningar och dataöverföringar loggas i Serial Monitor. Detta möjliggör identifiering och analys av problem, samt

felsökning av anslutnings- och överföringsfel.

Framtida förbättringar:

Central logghantering: I framtiden kan en central loggserver implementeras för att samla loggar från flera enheter, vilket underlättar övervakning och hantering av säkerhetsvarningar.

Automatiserad sårbarhetsrapportering: Genom att införa automatiserad felrapportering till en övervakningsplattform kan säkerhetsincidenter upptäckas och hanteras i realtid.