**Model pretnji HOSS Portabilni Sistem**

**Analizirani modul**

HOSS je rešenje po sistemu ključ u ruke. Uključuje niz uređaja (senzora, gateway-a) i web-mobilne aplikacije podržanih logikom zasnovanom na Cloud-u.

Dobija uvid u realnom vremenu i preuzima potpunu kontrolu nad procesom označavanja boca u pivarskoj industriji.

Korisnik prati napredovanje procesa, detektuje prekide i generiše upozorenja, nadgleda najvažnije parametre životne sredine i pomaže operaterima mašina da konfigurišu liniju za etiketiranje kako bi optimizovali količinu korićenog lepka.

Sistem se sastoji od kako fizičkih tako i digitalnih resursa uključujući:

1. Senzore koji prikupljaju podatke
2. Gateway uređaj
3. Azure Cloud servis za obradu i skladištenje podataka
4. Web API i mobilnu aplikaciju

Sistem garantuje tri vrste sigurnosti a to su

1. Sigurnost opreme- CE sertifikat koji osigurava uskladjenost sa EU smernicama I zaštitama podataka
2. Microsoft Azure ograničenja I ograničenja za pristup samo za kupca I zaposlene
3. Sigurnost podataka-softver za enkripciju garantuje sigurnost transfera podataka, takođe anonimizacija ličnih podataka obezbeđuje usklađenost sa GDPR pravilima

Microsoft Azure IoT obezbeđuje sigurnost opreme, konekcije kao I cloud-a.

**Tokovi podataka analiziranog sistema**

1. Glavni uređaj HOSS šalje podatke u IoT Hub u odgovarajućem JSON formatu preko MQTT protokola
2. Uređaj higrometra šalje podatke u IoT Hub u odgovarajućem JSON formatu preko HTTPS protokola
3. Azure funkcija obrađuje i kalibriše podatke sa IoT Hub-a preko AMQP protokola
4. Telemetrijski podaci se čuvaju na Azure SQL bazi podataka preko TCP protokola
5. Web API povezuje se sa SQL bazom podataka za dobijanje podataka preko TCP protokola
6. Web App povezuje se sa SQL bazom podataka za dobijanje podataka preko TCP
7. Android aplikacija operatera preuzima podatke iz Web API-ja preko HTTPS protokola

A black grid with white text

Description automatically generated

*Slika1(Dijagram toka podataka sistema)*

Android operatorska aplikacija

U fabrici se pored svih drugih komponenti instalira I uređaj za prikaz sa instaliranom Android aplikacijom operatera. Ova aplikacija je napravljena kako bi se olakšala kontrola procesa kao i izveštavanje o početku šarže ili njenom zaustavljanju.

Vrlo važna karakteristika je alarmiranje operatera mašine, tako da je putem displeja moguće obavestiti operatora o različitim vrstama nepravilnosti.

-Prvo postoji ekran za prijavu u aplikaciju. Odaberite željeni jezik, unesite

korisničko ime i lozinku i pritisnite login. Nakon uspešne prijave postoji dugme za pokretanje I zaustavljanje šarže, takodje imamo i mogućnost pregleda celog sistema-da li ili ne trenutno postoji aktivna serija takođe prikazuju se osnovne informacije o njoj kada je pokrenuta, kada je završila ako je završila, marku, lepak I njegov interni broj. Ovo daje korisniku uvid u trenutno stanje celog sistema.

Uvid u trenutno stanje sistema pomoću “Smart Labeling Control” koji mu omogućuje da prepozna neslaganje sa fabričkim stanjem u pogledu početka i kraja serije.

U zavisnosti od trenutnog stanja sistema u svakom trenutku je omogućeno samo jedno dugme-ako je serija aktivna dugme za pokretanje je onemogućeno i piše „Pokreće se“ a dugme za zaustavljanje je omogućeno. U obrnutoj situaciji aktivno dugme je „Start“.

Takođe postoje informacije koje je potrebno popuniti da bi se pokrenula nova serija. Potrebno je izabrati brend piva i upisati broj interne serije u fabrici svaki put pre pokretanja.

Svaka aktivna serije ima agregat sa karticom koja sadrži osnovne podatke- o trenutnoj temperaturi lepka i potrošnji struje. Alarmi se automatski proveravaju svakih 10 minuta.

Postoji nekoliko različitih tipova alarma.

-Detektuje početak ili kraj serije

-Detektuje prekomernu potrošnju lepka

-Detektuje previsoku temperaturu lepka

-Detektuje hiperkondenzaciju lepka

Takođe moguća je kalibracija vage putem aplikacije koja prikazuje najnovija merenja.

**Identifikacija resursa**

-Telemetrijski podaci kao što su vlažnost, temperatura ili parametri za etiketiranje gde bezbednosna svojstva mogu biti poverljivost i integritet.

-API ključevi i svi autentifikacijski tokovi gde bezbednosno svojstvo može biti poverljivost.

-Android APK mobilna aplikacija gde bezbednosna svojstva mogu biti integritet i dostupnost.

**Pretnje visokog nivoa**

1. **OWASP M3**: Insecure Communication - Izmena podataka u toku prenosa

Svaki HTTPS komunikacijski protokol se može presresti između mobilne aplikacije i web API-ja naročito u slučajevima kada SSL/TLS sertifikati nisu pravilno validirani gde bi bio ugrožen integritet Sistema.

1. **OWASP M9**: Insecure Data Storage - Oslanjanje na nesigurne biblioteke trećih strana

Ako aplikacija koristi biblioteke trećih strana (third-party) za pristup internetu ili lokalno skladištenje podataka, te biblioteke bi mogle biti zastarele ili imaju već poznate ranjivosti gde bi time ugrozili integritet i poverljivost sistema.

1. **OWASP M10**: Reverse Engineering - Eksploatacija ranjivosti u Android aplikaciji

Prikupljanje poverljivih informacija kao što su API ključevi ili razumevanje logike aplikacije. Potencijalni napadač bi mogao da koristi alate za dekomponovanje kako bi povratio izvorni kod iz APK. Alati poput JADX ili APKTool omogućavaju potencijalno pregledanje strukture koda I tako otkrije hardkodovane ključeve razne URL-ove API-ja, lozinke..

**1. OWASP M3: Nesigurna komunikacija**

**1.1 Napadi na komunikaciju**

1.1.1 Man-in-the-Middle (MITM) napadi

1.1.1.1 Eksploatacija nevalidiranih SSL sertifikata

1.1.1.1.1 Implementacija dvosmerne autentifikacije

1.1.1.1.1.1 Validacija CA sertifikata

-Upotreba poverenih sertifikacionih autoriteta za validaciju

1.1.1.1.1.2 Provera vremenskog važenja sertifikata

-Automatsko odbijanje sertifikata sa isteklim datumima.

1.1.1.1.2 Automatizacija validacije sertifikata

1.1.1.1.2.1 Uključivanje biblioteka za pinovanje sertifikata (npr TrustKit)

1.1.1.1.2.2 Automatsko generisanje obaveštenja za istekao sertifikat

-Implementacija monitoring alata za sertifikate

1.1.1.2 Ometanje TLS/SSL protokola

1.1.1.2.1 Implementacija TLS 1.3

1.1.1.2.1.1 Ograničenje cipher suite na sigurne algoritme (npr AES-GCM)

1.1.1.2.1.2 Onemogućavanje fallback na nesigurne protokole

-Konfiguracija za odbijanje SSL 2.0, 3.0 i TLS 1.0

**2. OWASP M9: Nesigurna pohrana podataka**

**2.1 Pristup osetljivim podacima**

2.1.1 Skladištenje poverljivih informacija u tekstualnom formatu

2.1.1.1 Izbegavanje pohrane podataka u otvorenom formatu

2.1.1.1.1 Korišćenje šifrovanih baza podataka (SQLite sa enkripcijom)

2.1.1.1.1.1 Implementacija SQLCipher za SQLite baze

-Automatsko šifrovanje celokupne baze podataka

2.1.1.1.1.2 Upotreba korisničkih lozinki za pristup šifrovanim bazama

-Lozinka korisnika se koristi za generisanje ključeva.

2.1.1.1.2 Primena AES šifrovanja sa 256-bitnim ključem

2.1.1.1.2.1 Korišćenje PBKDF2 za generisanje enkripcijskih ključeva

-Upotreba salta i iteracija za zaštitu lozinki

**2.2 Ranjivosti u privremenom skladištenju**

2.2.1 Pohrana sesija u nesigurnom formatu (SharedPreferences)

2.2.1.1 Implementacija sigurnih sesija koristeći kriptografiju

2.2.1.1.1 Šifrovanje sesija pre pohrane

-AES-GCM sa IV za zaštitu podataka

2.2.1.1.2 Validacija sesija sa digitalnim potpisom

-HMAC validacija kako bi se otkrila manipulacija podacima.

**3. OWASP M10: Nedovoljna kriptografija**

**3.1 Korišćenje slabih algoritama**

3.1.1 Zastareli šifrovni protokoli (npr MD5, SHA-1)

3.1.1.1 Zamena nesigurnih protokola modernim (npr SHA-256, AES)

3.1.1.1.1 Automatizacija provere sigurnosti algoritama tokom razvoja

-Upotreba alata kao što su CryptoAnalyzer ili AppScan.

3.1.1.1.2 Testiranje performansi enkripcije na različitim uređajima

-Merenje uticaja modernih algoritama na slabijim uređajima

**3.2 Nedovoljna zaštita enkripcijskih ključeva**

3.2.1 Hardkodovanje ključeva u kodu

3.2.1.1 Implementacija Keystore-a za sigurno skladištenje ključeva

3.2.1.1.1 Upotreba Android Keystore API-ja

-Omogućavanje šifrovanja ključeva vezanih za uređaj

3.2.1.1.2 Automatsko zaključavanje ključeva nakon neaktivnosti

-Aktivacija mehanizma vremenskog ograničenja pristupa

**3.3 Loša implementacija enkripcije**

3.3.1 Enkripcija bez provere integriteta

3.3.1.1 Implementacija kombinacije HMAC i AES enkripcije

3.3.1.1.1 Verifikacija podataka nakon dekripcije

-Provera da li je HMAC vrednost podataka validna

3.3.1.1.2 Automatsko odbacivanje podataka sa nevalidnim potpisom

-Blokiranje bilo kakve dalje obrade podataka