**Documentul de specificare a cerin**

**Software Requirements Specification**

**(SRS) Document**

**Sistem de Securitate pentru Intrare cu Turnicheți și Amprentă**

|  |
| --- |
| **Istoricul versiunilor** |

| Versiune | Autor(i) principali | Descriere versiune | Dată |
| --- | --- | --- | --- |
|  |  |  |  |

|  |
| --- |
| **Revizuiri și aprobări** |

Istoric aprobări

| Aprobă | Versiune | Semnătură | Dată |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

Istoric revizuiri

| Revizor | Versiune | Semnătură | Dată |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **Cuprins** |

[1. Introducere 3](#_Toc159317952)

[1.1 Scopul 3](#_Toc159317953)

[1.2 Convenții ale documentului 3](#_Toc159317954)

[1.3 Audiență țintă 3](#_Toc159317955)

[1.4 Sfera de aplicare 3](#_Toc159317956)

[1.5 Referințe 3](#_Toc159317957)

[**2 Descriere generală 3**](#_Toc159317958)

[**2.1 Perspectiva produsului 3**](#_Toc159317959)

[**2.2 Caracteristici ale produsului 3**](#_Toc159317960)

[**2.3 Clase și caracteristici ale utilizatorilor 3**](#_Toc159317961)

[**2.4 Mediul de operare 4**](#_Toc159317962)

[**2.5 Constrângeri de proiectare și de implementare 4**](#_Toc159317963)

[**2.6 Presupuneri și dependențe 4**](#_Toc159317964)

[**3 Cerințele sistemului 4**](#_Toc159317965)

[**3.1 Funcționalitatea 1 4**](#_Toc159317966)

[**3.1.1 Descriere și Prioritate 4**](#_Toc159317967)

[**3.1.2 Secvențe Stimul/Răspuns 4**](#_Toc159317968)

[**3.1.3 Cerințe Funcționale 5**](#_Toc159317969)

[**3.2 Cerința funcțională 2 5**](#_Toc159317970)

[3.3 .... 5](#_Toc159317971)

[4 Cerințe pentru interfețe externe 5](#_Toc159317972)

[4.1 Interfețe ale Utilizatorului 5](#_Toc159317973)

[4.2 Interfețe Hardware 5](#_Toc159317974)

[4.3 Interfețe de Comunicare 5](#_Toc159317975)

[4.4 Interfețe Software 5](#_Toc159317976)

[5 Cerințe non-funcționale 6](#_Toc159317977)

[5.1 Cerințe de performanță 6](#_Toc159317978)

[5.2 Cerințe de siguranță 6](#_Toc159317979)

[5.3 Cerințe de securitate 6](#_Toc159317980)

[5.4 Atribute de calitate ale software-ului 6](#_Toc159317981)

[6 Alte cerințe 6](#_Toc159317982)

[7 Anexe 6](#_Toc159317983)

[7.1 Anexa A: Glosar 6](#_Toc159317984)

[7.2 Anexa B: Modele de Analiză 6](#_Toc159317985)

[7.3 Anexa C: Listă de Probleme 7](#_Toc159317986)

# Introducere

## Scopul

Scopul acestui proiect este de a dezvolta un sistem de securitate pentru controlul accesului într-o locație, folosind turnicheți și verificarea amprentei. Obiectivele principale ale proiectului includ crearea unei interfețe intuitive pentru utilizatori, implementarea unui sistem de recunoaștere a amprentelor fiabil și integrarea acestuia cu un sistem de gestionare a bazelor de date pentru stocarea informațiilor despre utilizatori și accesul lor.

## Convenții ale documentului

Acest document urmează convențiile tipografice standard, folosind fonturi clare și structură logică pentru a asigura o înțelegere adecvată. Abrevierile sunt folosite în mod corespunzător, iar titlurile și secțiunile sunt evidențiate pentru o navigare ușoară.

## Audiență țintă

Documentul SRS este destinat următoarelor părți interesate ale proiectului:

Dezvoltatorilor: Pentru a înțelege cerințele funcționale și non-funcționale ale sistemului.

Managerilor de Proiect: Pentru a evalua și gestiona progresul proiectului în conformitate cu cerințele stabilite.

Testerilor: Pentru a efectua teste de validare și verificare conform cerințelor specificate.

## Sfera de aplicare

Obiectivele software-ului se aliniază cu obiectivele generale ale afacerii de a asigura securitatea și controlul accesului în locații cheie. Beneficiile proiectului pentru afacere includ:

* Îmbunătățirea securității: Prin implementarea unui sistem robust de control al accesului.
* Eficiență sporită: Prin automatizarea procesului de autentificare și gestionare a accesului utilizatorilor.
* Reducerea riscului de fraudă: Prin utilizarea verificării amprentei pentru autentificare, care este mai dificil de compromis în comparație cu metodele tradiționale de autentificare bazate pe parole sau cartele.

## Referințe

Documentația Arduino: arduino.cc/documentation

Documentația Django: docs.djangoproject.com

Literatură relevantă despre securitatea sistemelor informatice.

# Descriere generală

## Perspectiva produsului

Sistemul de securitate pentru intrare cu turnicheți și amprentă dezvoltat în cadrul acestui proiect își are originea în necesitatea de a asigura controlul accesului într-o locație specifică, într-un mod sigur și eficient. Produsul se integrează într-un mediu urban sau de afaceri și este proiectat pentru a furniza o soluție modernă și fiabilă pentru gestionarea accesului utilizatorilor.

## Clase și caracteristici ale utilizatorilor

Software-ul propus va îndeplini următoarele funcții și caracteristici:

Autentificare utilizatorilor prin verificarea amprentei.

Controlul accesului utilizatorilor folosind turnicheți automatizați.

Interfață web pentru administrarea utilizatorilor și a permisiunilor de acces.

Stocarea și gestionarea datelor utilizatorilor într-o bază de date securizată.

Auditarea și înregistrarea activităților de acces pentru scopuri de monitorizare și raportare.

## Mediul de operare

Utilizatorii sistemului sunt clasificați în următoarele categorii:

Administratori: Utilizatori cu privilegii deplinite, responsabili de administrarea și configurarea sistemului.

Utilizatori obișnuiți: Persoane care utilizează sistemul pentru accesul în locația specificată.

Utilizatorii pot fi clasificați și în funcție de nivelul de experiență tehnică și de necesitatea lor de acces frecvent sau sporadic în locație.

## Constrângeri de proiectare și de implementare

Software-ul este proiectat să opereze într-un mediu urban sau de afaceri și să fie compatibil cu următoarele componente:

Platforme hardware Arduino pentru controlul turnicheților și a senzorilor de amprentă.

Sisteme de operare compatibile, inclusiv Windows, Linux și MacOS.

Server web Django pentru gestionarea interfeței de utilizator și a bazelor de date.

Nu sunt prevăzute interfețe cu alte aplicații sau tehnologii specifice, iar operațiunile sistemului sunt concepute pentru a fi independente și fiabile în funcționare.

## Presupuneri și dependențe

Presupunerile și dependențele includ:

Disponibilitatea hardware-ului necesar pentru implementarea sistemului.

Accesul la tehnologii de recunoaștere a amprentelor compatibile cu platforma Arduino și Django.

Respectarea cerințelor și reglementărilor legale în vigoare pentru implementarea sistemului.

# Cerințele sistemului

## Funcționalitatea 1

### Descriere și Prioritate

Această funcționalitate permite utilizatorilor să se autentifice în sistemul de securitate folosind verificarea amprentei lor. Are prioritate ridicată deoarece reprezintă primul pas în procesul de control al accesului și este esențial pentru asigurarea securității.

### Secvențe Stimul/Răspuns

Stimul: Utilizatorul atinge senzorul de amprentă de pe dispozitivul de control al accesului.

Răspuns: Sistemul încearcă să identifice și să verifice amprenta utilizatorului.

Stimul: Amprenta utilizatorului este identificată cu succes.

Răspuns: Sistemul deschide turnicheții și permite accesul utilizatorului în locație.

Stimul: Amprenta utilizatorului nu este identificată sau nu este validă.

Răspuns: Sistemul afișează un mesaj de eroare și refuză accesul utilizatorului.

### Cerințe Funcționale

REQ-1: Sistemul trebuie să poată înregistra și să stocheze amprentele utilizatorilor într-o bază de date securizată.

REQ-2: Sistemul trebuie să aibă capacitatea de a detecta și de a verifica amprentele utilizatorilor în timp real.

REQ-3: Sistemul trebuie să permită configurarea și administrarea amprentelor utilizatorilor de către administratori.

REQ-4: În cazul unui număr predefinit de încercări eșuate de autentificare, sistemul trebuie să blocheze temporar accesul utilizatorului și să înregistreze această tentativă de acces neautorizată.

REQ-5: Sistemul trebuie să furnizeze o interfață de utilizator intuitivă pentru procesul de autentificare cu amprentă.

REQ-6: Sistemul trebuie să ofere oportunități de recuperare a accesului pentru utilizatorii cu amprente schimbate sau deteriorate.

# Cerințe pentru interfețe externe

## Interfețe cu utilizatorul

Interfața cu utilizatorul va include următoarele elemente:

* Ecran de autentificare: Utilizatorii vor putea introduce informațiile de autentificare sau să folosească verificarea amprentei pentru a accesa sistemul.
* Interfață de administrare: Pentru administratori, va exista o interfață web intuitivă pentru gestionarea utilizatorilor, permisiunilor și a altor setări ale sistemului.
* Mesaje de stare: Sistemul va afișa mesaje corespunzătoare în cazul succesului sau a eșecului autentificării, precum și pentru alte acțiuni importante.

## Interfețe hardware

Software-ul este destinat să ruleze pe platforme hardware Arduino pentru controlul turnicheților și a senzorilor de amprentă. Aceste dispozitive vor comunica cu software-ul prin intermediul unor interfețe adecvate, cum ar fi porturile seriale sau interfețe de comunicație dedicate.

## Interfețe de comunicare

Software-ul va folosi protocoale de comunicație standard pentru a interacționa cu dispozitivele hardware și pentru a comunica cu alte componente software. Aceste protocoale includ comunicații seriale pentru interfața cu dispozitivele hardware și protocoale HTTP pentru interacțiunea cu interfeța web de administrare.

## Interfețe software

Software-ul va interacționa cu următoarele componente software:

Frontend: Interfața web pentru utilizatori și administratori va fi dezvoltată folosind HTML, CSS și JavaScript.

Backend: Sistemul de gestionare a bazelor de date și logica de business va fi implementată folosind framework-ul Django în limbajul de programare Python.

Sistemul de Baze de Date: Software-ul va utiliza o bază de date relațională pentru stocarea informațiilor despre utilizatori, acces și alte date relevante.

# Cerințe non-funcționale

## Cerințe de performanță

Timp de răspuns al sistemului: Sistemul trebuie să răspundă la cererile de autentificare într-un timp foarte scurt, de preferință sub 1 secundă. Aceasta este o cerință critică pentru a asigura o experiență utilizator fluidă și pentru a minimiza timpul de așteptare al utilizatorilor.

Capacitate de procesare: Sistemul trebuie să fie capabil să gestioneze un număr mare de cereri simultane de autentificare, fără a afecta în mod semnificativ performanța generală a sistemului. Acest lucru este esențial pentru a susține utilizarea în medii cu trafic intens.

Fiabilitate: Sistemul trebuie să fie stabil și să funcționeze fără erori sau căderi frecvente. Timpul mediu între eșecuri (MTBF) trebuie să fie ridicat, iar capacitatea de recuperare în caz de eșecuri trebuie să fie rapidă și eficientă.

## Cerințe de siguranță

Controlul accesului la date: Accesul la datele sensibile trebuie să fie restricționat numai la utilizatorii autorizați, cu permisiunile corespunzătoare. Acest lucru poate fi realizat prin autentificare și autorizare adecvată în cadrul sistemului.

Protecția datelor sensibile: Toate datele utilizatorilor, inclusiv amprentele digitale, trebuie să fie stocate și transferate într-un mod securizat, folosind tehnici de criptare puternice și protocoale de comunicație sigure.

Auditare și jurnalizare: Sistemul trebuie să înregistreze în mod adecvat toate activitățile de autentificare și de acces, pentru a permite o monitorizare eficientă și pentru a identifica orice tentative de acces neautorizat sau de utilizare abuzivă a sistemului.

## Cerințe de securitate

Conformitate cu GDPR și alte reglementări: Software-ul trebuie să respecte cerințele legale privind protecția datelor personale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR), pentru a asigura confidențialitatea și integritatea datelor utilizatorilor.

Măsuri de securitate a infrastructurii: Serverele și alte componente ale infrastructurii software-ului trebuie să fie protejate împotriva atacurilor cibernetice și să aibă implementate măsuri adecvate de securitate, cum ar fi firewall-uri, monitorizare a securității și actualizări regulate de securitate.

## Atribute de calitate ale software-ului

Fiabilitate: Software-ul trebuie să fie stabil și să funcționeze corect în toate situațiile, fără a avea erori sau căderi frecvente.

Ușurința în Întreținere: Codul software-ului trebuie să fie bine structurat și documentat pentru a facilita întreținerea și modificările ulterioare.

Portabilitate: Software-ul ar trebui să fie portabil între diferite platforme hardware și sisteme de operare, pentru a permite utilizarea sa într-o varietate de medii de lucru.

# Alte cerințe

Backup și Recuperare: Sistemul trebuie să ofere capacități robuste de backup și recuperare a datelor pentru a asigura că informațiile utilizatorilor sunt protejate împotriva pierderilor accidentale sau a coruperii datelor.

Consistență și Integritate: Datele stocate în baza de date trebuie să fie consistente și integre, iar sistemul trebuie să implementeze măsuri adecvate pentru a preveni corupția datelor și inconsistentele.

# Anexe

## Anexa A: Glosar

## Anexa B: Modele de Analiză

## Anexa C: Listă de Probleme

TBD-1: Este necesară o decizie cu privire la algoritmul specific de recunoaștere a amprentelor care să fie utilizat în cadrul sistemului.

TBD-2: Informații suplimentare sunt necesare cu privire la cerințele specifice de securitate și conformitate cu reglementările legale pentru protecția datelor.

TBD-3: Trebuie să se clarifice cerințele exacte de localizare și internaționalizare pentru a sprijini utilizatorii din diferite regiuni geografice.

TBD-4: Este necesară o decizie cu privire la structura și formatul datelor stocate în baza de date pentru a asigura consistența și eficiența sistemului.

TBD-5: Mai multe informații sunt necesare cu privire la cerințele de performanță exacte și la metricile care vor fi utilizate pentru a evalua performanța sistemului.