2025

Projectplan

Plan van aanpak voor het ontwikkelen van een Biometrisch Toegangssysteem

BIOMETRISCH TOEGANGSSYSTEEM

PIOTR TADRALA | INFORDB

O-PP-CMK

INHOUDSOPGAVE

1.0 INLEIDING

1.1 CONTEXT

InforDB BV is opgericht in 2005 en begon als specialist in softwareontwikkeling en database-consultancy, met een focus op de financiële sector. Het bedrijf ontwikkelde applicaties voor organisaties zoals ABN Amro, ABP en ING Bank. In 2012 werd InforDB Development opgericht om zich te richten op apps en webapplicaties. Inmiddels levert InforDB maatwerksoftware voor diverse branches en heeft diverse applicaties ontwikkeld die door verschillende organisaties worden gebruikt.

Het bedrijf ziet potentie in de ontwikkeling van een toegangssysteem dat zowel betrouwbaar als gebruikersvriendelijk is, met nadruk op de integratiemogelijkheden in de bestaande applicaties van InforDB.

Biometrische technologie biedt hiervoor een oplossing, maar wordt steeds makkelijker te omzeilen, bijvoorbeeld door AI. InforDB ziet potentie in de ontwikkeling van een systeem dat niet beperkt is tot een verificatiemethode, zoals een vingerafdruk- of gezichtsherkenning, maar een bredere set van (biometrische) verificatietechnieken toepast voor toegangscontrole. Eisen voor het uiteindelijke product zijn dat het plug-and-play, gebruiksvriendelijk en veilig moet zijn.

1.2 STAKEHOLDER

Ton Scheres, mede-eigenaar en directeur van InforDB, heeft het project voorgesteld en speelt de rol van stakeholder binnen het project. Ton zal het directe aanspreekpunt binnen het bedrijf zijn voor reviews en overleggingen.

1.3 PROJECTOMSCHRIJVING

Traditionele toegangssystemen, zoals sleutels en toegangspassen, zijn kwetsbaar voor verlies, diefstal en misbruik. Biometrische technologieën, zoals gezichts- en vingerafdrukherkenning, bieden een verbeterde beveiliging, maar zijn niet volledig betrouwbaar. Door de groei in AI en deepfake-technologie wordt het steeds eenvoudiger om biometrische verificatiesystemen te omzeilen. Dit vergroot de noodzaak voor een beter toegangssysteem dat meerdere verificatiemethoden en algoritmes combineert.

Dit project richt zich op de ontwikkeling van een geavanceerd toegangscontrolesysteem dat meerdere verificatiemethoden combineert om de veiligheid te verbeteren. Naast biometrische herkenning wordt een extra verificatiestap toegevoegd, zodat het systeem niet uitsluitend afhankelijk is van biometrische verificatie en beter bestand is tegen spoofing en deepfake-aanvallen. Het systeem wordt zo ontworpen dat het eenvoudig kan worden geïntegreerd in bestaande applicaties / systemen.

1.4 DOELSTELLING

Het doel van dit project is om een gebruiksvriendelijk en veilig toegangssysteem te onderzoeken en te ontwikkelen. Dit systeem moet bestand zijn tegen omzeilingspogingen met technieken zoals deepfakes. Het systeem moet ook schaalbaar zijn voor integraties met andere systemen en producten.

2.0 PROJECTOMSCHRIJVING

2.1 HOOFDVRAAG

Hoe kan een biometrisch toegangscontrolesysteem worden ontworpen en ontwikkeld dat zowel gebruiksvriendelijk als veilig is tegen misleidingspogingen, zoals deepfakes, en eenvoudig te integreren is met andere systemen?

2.2 REQUIREMENTS

2.2.1 FUNCTIONELE EISEN

- Het systeem moet biometrische verificatie ondersteunen.
- Het systeem moet niet afhankelijk zijn van een verificatiemethode.
- Het systeem moet een slot kunnen aansturen op basis van succesvolle verificatie.
- Het systeem moet logging en monitoring van verificatiepogingen ondersteunen.
- Het systeem moet een gebruikersbeheerfunctie hebben voor toegangscontrole.

2.2.2 NIET FUNCTIONELE EISEN

- Het systeem moet scalable zijn voor eventuele toekomstige integraties.
- Het systeem moet een snelle en efficiënte verificatie bieden.
- Het systeem moet gebruiksvriendelijk zijn voor zowel beheerders als gebruikers.
- Het systeem moet een hoge beschikbaarheid en betrouwbaarheid hebben.
- Het systeem moet "easy to install & maintain" zijn.
- Het systeem moet veilig zijn en aan de geldende normen voldoen.

2.2.3 TECHNISCHE EISEN

- De backend moet REST API ondersteunen.
- H et systeem moet compatibel zijn met bestaande sloten.
- Het systeem moet gebruik maken van encryptie voor databeveiliging.
- De hardware moet geschikt zijn voor gebruik in diverse omgevingen (binnen/buiten).
- Voor de software moet het best mogelijke platform worden gekozen (embedded systems, cloud, on-premise).

2.3 ONDERZOEK

2.3.1 ONDERZOEKSVRAGEN

Index	Deelvraag
D1	Zijn er al vergelijkbare systemen op de markt?
D2	Welke verificatiemethodes zijn er beschikbaar?
D3	Welke componenten zijn er nodig om het systeem te realiseren
D4	Welke maatregelen kunnen worden genomen om biometrische data te beschermen tegen vervalsing en diefstal?
D5	Welke software- en hardwarearchitectuur & platform is het meest geschikt voor een schaalbaar en uitbreidbaar toegangscontrolesysteem?

2.3.2 ONDERZOEKSAANPAK

Index	Onderzoeksmethode
D1	Literatuuronderzoek
D2	Literatuuronderzoek
D3	Literatuuronderzoek, Prototyping
D4	Literatuuronderzoek, Data-analyse, prototyping
D5	Literatuuronderzoek, Prototyping

2.3.3 VERWACHTE ONDERZOEKSUITKOMSTEN

Index	Verwachte uitkomst
D1	Eventuele bestaande systemen
D2	Potentiele verificatiemethodes
D3	Te realiseren hardware en software componenten
D4	Anti-spoofing methodes
D5	Meest geschikt software & hardware architectuur & platform

2.4 DELIVERABLES AND NON-DELIVERABLES

2.4.1 DELIVERABLES

- **Hardwareprototype:** Werkend biometrisch toegangssysteem met sensoren en besturing.
- **Backend/API:** Een backend voor de communicatie tussen de hardware en het systeem (indien nodig).
- **Onderzoeksrapport:** Analyse van bestaande systemen, beveiligingsrisico's en teschnische mogelijkheden .
- **Realisatierapport:** Documentatie van de ontwikkelde hardware, software en de gemaakte keuzes.
- **Testplan:** Testcases voor functionele en beveiligingstests.
- **Managementrapport:** Omschrijving van de CI/CD pipeline.

2.4.2 NON-DELIVERABLES

- **Volledig commercieel product:** Het project levert een prototype op.

2.5 BEPERKINGEN

Het systeem moet worden gerealiseerd binnen een relatief korte periode van ongeveer vier maanden, waardoor tijd een van de grootste beperkingen is. Daarnaast kunnen technische beperkingen een rol spelen, omdat de gekozen hardware binnen het beschikbare budget moet passen. Dit kan invloed hebben op de prestaties en effectiviteit van de geïmplementeerde verificatiemethodes.

3.0 PLANNING

3.1 SPRINTS

Het project wordt uitgevoerd volgens een agile aanpak, waarbij het werk wordt opgesplitst in sprints van vier weken. Elke week vindt er een meeting plaats met de stakeholder om de voortgang te bespreken. Daarnast zal er elke vier weken een sprint demo plaatsvinden.

SPRINT 1

- Opstelen van het plan van aanpak.
- Uitvoeren van de probleemanalyse.
- Initiële onderzoek naar de onderzoeksvragen.

SPRINT 2

- Testimplementaties van de biometrische verificatiesmethodes.
- Ontwikkelen van de software- en hardwarearchitectuur.
- Opzetten van de backend / API infrastructuur.

SPRINT 3

- Realisatie van een werkend prototype.
- Integratie tussen hardware en backend.
- Opstellen van het realisatierapport.

SPRINT 4

- Implementatie van de CI/CD Integratie.
- Opstellen van het Realisatierapport
- Opstellen van het Managementrapport.

4.0 MANAGEMENT

4.1 BUDGET & FINANCIËN

Gedurende het semester zullen er diverse hardware- en softwarecomponenten aangeschaft moeten worden, zoals sensoren, microcontrollers, licenties voor ontwikkeltools en eventuele cloudservices. Deze worden beheerd en gefinancierd door het bedrijf.

VERWACHTE KOSTENOVERZICHT

Categorie	Omschrijving	Gescahtte kosten
Hardware	Sensoren	€ 100 / 300
	Microcontrollers	€ 10 / 50
	Slot aansturing	€ 50 / 150
	Overige componenten (Kabels, PCB's etc)	€ 10 / 50
Software & Licenties	Cloudservice (AWS, Azure, Firebase)	€ 10 / 50 / maand
Overig	Onvoorziene Kosten	€ 10 / 100
Totaal	**Totale verwachten kosten**	**€ 180 / 650 + (€ 10 / 50 / maand)**

4.2 KWALITEIT

Tijdens de wekelijkse sprints vindt er een validatie plaats met de stakeholder, waarbij zowel de functionaliteiten als de prestaties van het systeem worden beoordeeld. Gedurende het project kan er iemand worden toegevoegd voor extra controle volgens het four-eyes-principe.

Tijdens de wekelijkse sprints wordt er op de volgende punten gelet:

- **Voortgang:** Zijn de geplande taken afgerond.
- **Implementaties:** werken de nieuwe implementaties zoals verwacht?
- **Kwaliteit en prestaites:** Functioneren geïmplementeerdefunctionaliteiten accuraat en efficiënt?
- **Feedback van de stakeholder:** Komt de project overeen met de verwachtigingen en eisen van de stakeholder?
- **Documentatie:** Zijn de rapportages en documentatie up to date?
- **Compatibiliteit:** Werkt de hardware goed met de backend?

4.3 TIJD EN MILESTONES

Het project zal ongeveer vier manden duren en wordt opgeplitsts in sprints van vier weken.

Sprint	Milestone
1	Goedgekeurd plan van aanpak, inclusief een duidelijke probleemanalyse en vastgelegde onderzoeksvragen.
2	Afgerond architectuurontwerp met een werkende testimplementatie van de biometrische verificatiemethoden en opgezette backend-/API-infrastructuur.
3	Een werkend prototype dat de integratie tussen hardware en backend demonstreert, ondersteund door een realisatierapport.
4	Volledig geïntegreerd systeem met geïmplementeerde CI/CD-pipeline en afgeronde rapportages (realisatie- en managementrapport).

4.4 ORGANIZATION

Aangezien de challenges in semester 7 volledig zelfstandig worden uitgevoerd, is de organisatie klein. De stakeholder van het project is mijn werkgever. Op school word ik ondersteund door twee coaches: één die mijn wekelijkse aanspreekpunt is en één die elke vier weken aanwezig is tijdens de sprint demo’s.