2025

Biometrisch Toegangssysteem

Onderzoek naar de ontwikkeling van een veilig en schaalbaar biometrisch toegangscontrolesysteem

BIOMETRISCH TOEGANGSSYSTEEM
PIOTR TADRALA | INFORDB

O-PP-CMK

I. MANAGEMENT & SAMENVATTING

//TODO: Compleet samenvatting

II. VERSIEBEHEER & DISTRIBUTIE

VERSIEBEHEER

Versie	*Omschrijving*	*Auteur*
0.1	Eerste opzet van het document	Piotr Tadrala
0.2		
0.3		

DISTRIBUTIEBEHEER

Versie	*Ontvangers*
0.1	
0.2	
0.3	

III. WOORDENLIJST

Begrip	*Omschrijving*
Biometrische Verificatie	Authenticatiemethode op basis van unieke lichaamskenmerken, zoals gezichtsherkenning of vingerafdruk
Spoofing	Een techniek waarbij en systeem misleidt wordt met nep gegevens.
Liveness-detectie	Technologie die controleert of een biometrisch kenmerk afkomstig is van een levende persoon.
Deepfake	Door AI gegenereerde beelden of video's
MFA	Een beveiligingsmethode waarbij meerdere verificatiestappen worden gebruikt.
SDK	Software Development Kit
EDK	Embedded Development Kit
RFID	Radio Frequency Identification
BLE	Low Energy Bluetooth

INHOUDSOPGAVE

1.0INLEIDING

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 het enkele white-label applicaties ontwikkeld die door verschillende organisaties worden gebruikt.

Het bedrijf ziet er 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 er 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.

2.0 CONTEXT

2.1 INLEIDING

Biometrische verificatie wordt steeds vaker ingezet voor toegangssystemen, omdat het betrouwbaarder en gebruiksvriendelijker is dan traditionele methoden zoals fysieke sleutels. Toch geven veel systemen een valse hoop van veiligheid door beperkte maatregelen tegen spoofing.

2.2 HUIDIGE SITUATIE

Momenteel maken veel toegangscontrolesystemen gebruik van biometrische verificatie, zoals gezichtsherkenning en vingerafdrukscanners. Hoewel deze technieken goede beveiliging bieden, hebben ze enkele beperkingen:

- **Kwetsbaarheid voor spoofing**: Biometrische systemen kunnen worden misleid door foto's, video's of deepfake-technologie.
- **Gebrek aan liveness-detectie**: Veel systemen controleren niet of de biometrische input afkomstig is van een levende persoon.
- **Afhankelijkheid van één verificatiemethode**: De meeste systemen gebruiken slechts één verificatiemethode, waardoor ze minder robuust zijn tegen aanvallen.
- **Beperkte implementatie van anti-spoofingtechnieken**: Door kosten, infrastructuurbeperkingen of een gebrek aan regelgeving worden deze technieken niet altijd toegepast.

2.3 PROBLEEMSTELLING

Huidige biometrische toegangssystemen zijn niet voldoende bestaand tegen misleidpogingen, zoals deepfakes en spoofing. Daarnast zijn er veel systemen afhankelijk van één enkele verificatiemethode waardoor de veiligheid beperkt blijft.

2.4 DOELSTELLING

Het doel van dit document is te onderzoeken hoe een toegangssysteem kan worden ontwikkeld dat zowel gebruiksvriendelijk is, bestand is tegen spoofing-attacks en eenvoudig kan worden geïntegreerd in bestaande systemen.

3.0 ONDERZOEKSAANPAK

3.1 INLEIDING

In dit hoofdstuk laat ik zien waar dit document zich op richt. De hoofdvraag en de bijbehorende deelvragen worden in kaart gebracht, en wordt gekeken hoe deze vragen beantwoord kunnen worden.

3.2 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?

3.3 DEELVRAGEN

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

3.4 ONDERZOEKSMETHODEN

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

3.5 VERWACHTE ONDERZOEKSUITKOMSTEN

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

3.6 SCOPE

Dit document richt zich op het onderzoeken van de eerder genoemde onderzoeksvragen die beantwoord moeten worden om een prototype te kunnen ontwikkelen. Het beschrijft niet hoe het prototype kan worden omgezet tot een commercieel product.

3.7 CONCLUSIE

Dit hoofdstuk heeft de hoofd- en deelvragen in kaart gebracht en de onderzoeksmethoden bepaald. Het onderzoek richt zich op het ontwikkelen van een veilig en gebruiksvriendelijk biometrisch toegangscontrolesysteem dat bestand is tegen misleiding en eenvoudig te integreren is.

Door middel van literatuuronderzoek, data-analyse en prototyping worden bestaande systemen, verificatiemethoden, anti-spoofingtechnieken en geschikte software- en hardwareoplossingen onderzocht. De uitkomsten vormen de basis voor een functioneel prototype.

4.0 ZIJN ER AL VERGELIJKBARE SYSTEMEN OP DE MARKT?

4.1 INLEIDING

Bij het ontwikkelen van een biometrisch toegangscontrolesysteem leek het mij verstandig om eerst te onderzoeken welke systemen al op de markt beschikbaar zijn. Dit helpt bij het identificeren van good & practices, en het vaststellen van de huidige marktstandaarden. In dit hoofdstuk vergelijk ik bestaande oplossingen.

4.2 BESTAANDE OPLOSSINGEN

PAXTON

Paxton's is een flexibel toegangscontrolesysteem dat integratie met biometrische lezers mogelijk maakt. Het systeem ondersteunt API-integraties, waardoor het kan samenwerken met andere systemen.

- Paxton, (Onbekend) Hoe maak ik een veilig toegangscontrole systeem nog veiliger?

ANVIZ

Anviz biedt oplossingen met liveness-detectie die zowel biometrische verificatie als traditionele methoden, zoals smartcards, ondersteunen. Het grootste verkoopargument van Anviz is de eenvoudige integratie dankzij hun EDK en SDK, gecombineerd met diverse toegangsbeheerfuncties, zoals gebruikersbeheer en apparaatbeheer.

- Anviz, (Onbekend) Slimme oplossing voor toegangscontrole

BOSCH SECURITY

Biometrische oplossingen van Bosch Security bieden zowel hoge verificatie naukeurigheid, als anti-spoofing technieken zoals Presentation Attack Detection (PAD) uitgevoerd door iBeta.

- Bosch, (Onbekend) Biometrische toegangscontrole

4.3 GOOD & BAD PRACTICES

PAXTON

	Omschrijving
Good	MFA.
Good	API Integraties mogelijkheden.
Bad	Geen informatie met betrekking tot anti-spoofing.
Bad	MFA werkt alleen met de traditionele technieken zoals cards of pin.

ANVIZ

	Omschrijving
Good	Eenvoudige API integraties dankzij hun EDK & SDK.
Good	Liveness-detectie.
Good	Toegangsbeheer portal.
Bad	Geen MFA mogelijkheden.
Bad	Liveness-detectie is puur op gezichtskenmerken gebaseerd.

BOSCH SECURITY

	Omschrijving
Good	Hoge verificatie nauwkeurigheid.
Good	Anti-spoofing
Good	API Integraties mogelijkheden
Bad	Geen MFA
Bad	Anti-spoofing is puur op gezichtskenmerken gebaseerd.

4.4 HUIDIGE MARKTSTANDAARDEN

Huidige oplossingen nemen stappen om zich te beschermen tegen spoofing, maar dit blijft in de meeste gevallen beperkt tot liveness-detectie op basis van gezichtskenmerken. Multi-Factor Authenticatie is nog geen standaardpraktijk. Hoewel sommige systemen MFA ondersteunen, is deze vaak beperkt tot traditionele methoden zoals een smartcard in combinatie met een PIN-code. API integratie mogelijkheden lijken in de meeste gevallen wel aanwezig te zijn, maar worden soms beperkt tot de lokale omgeving.

4.5 CONCLUSIE

Bestaande systemen bieden goede API-integraties, maar anti-spoofing blijft vaak beperkt tot liveness-detectie op gezichtskenmerken. MFA is nog geen standaard en wordt meestal beperkt tot traditionele technieken smartcards en PIN-codes. Hoewel er stappen worden gezet richting betere beveiliging, ontbreekt er in meeste gevallen MFA en geavanceerde anti-spoofing.

5.0 WELKE VERIFICATIEMETHODES ZIJN ER BESCHIKBAAR?

5.1 INLEIDING

In dit hoofdstuk onderzoek ik de beschikbare (biometrische) verificatiemethodes die toegepast kunnen worden binnen het toegangscontrolesysteem. Het doel is om inzicht te krijgen in de verschillende methodes. Hiermee is het doel om uiteindelijk to de conclusive te komen welke verificatiemethodes het meest geschikt zijn voor dit project.

5.2 BEOORDELINGCRITERIA

Om de meest geschikte verificatiemethode te bepalen, is het belangrijk om eerst de beoordelingscriteria vast te stellen. Vervolgens kunnen de onderzochte verificatiemethodes worden beoordeeld. Op basis van deze scores kan de meest geschikte methode worden gekozen. De belangrijkste factoren die hierbij een rol spelen, zijn:

- **Veiligheid:** Hoe veilig en betrouwbaaar is de methode?
- **Gebruikersgemak:** Hoe gebruikersvriendelijk en seamless is de verificatie?
- **Snelheid:** Hoe snel kan de gebruiken worden geverifieerd?
- **Kosten:** Wat zijn de kosten van implementatie

5.3 BIOMETRISCHE VERIFICATIEMETHODES

GEZICHTSHERKENNING

Gezichtskenmerken, zowel afzonderlijk als in combinatie, worden gebruikt voor biometrische verificatie. Dit houdt meestal in dat een face match-algoritme controleert of twee gezichten (het geregistreerde en het gepresenteerde) overeenkomen om de identiteit te verifiëren.

SPRAAKHERKENNING

Dankzij spraakherkenning is het mogelijk om gebruikers te onderscheiden en authenticeren op basis van hun unieke stemafdruk. Bij spraakherkenning evalueert het programma kenmerken zoals toonhoogte, intonatie, ritme en frequentie van de stem. Het systeem vergelijkt deze kenmerken met een eerder opgeslagen stemprofiel om de identiteit van de gebruiker te bevestigen

VINGERAFDRUK

Bij een authenticatie via de vingerafdruk, wordt de vingerafdruk gescand en gedigitaliseerd. Zo wordt een digitaal beeld van de kenmerken van de vingerafdruk gemaakt. Dit wordt opgeslagen in een beveiligde database. Iedereen heeft een uniek patroon van lijnen op de vingers, waardoor vingerafdrukken een effectieve manier zijn om iemand te identificeren.

- Shaip, (2024) Wat is spraakherkenning.
- Seon, (Onbekend) Biometric Verification
- Veiliginternetten, (Onbekend) Wat is biometrische authenticatie? En wanneer gebruik je het?

5.4 TRADITIONELE VERIFICATIEMETHODES

Naast de biometrische methoden kunnen we ook gebruik maken van traditionele methodes, die als secundaire verificatie stap van de MFA functioneren. Denk hierbij aan een verificatieflow waarbij gezichtsherkenning de primaire methode is, maar waarbij de gebruiker daarnaast aan een secundaire, niet perse biometrische, verificatie moet voldoen. Mogelijke opties hiervoor zijn:

- **RFID:** Een tag gekoppeld aan de gebruiker, die binnen een bepaalde afstand gedetecteerd moet worden tijdens de gezichtsverificatie.
- **BLE:** In plaats van een tag kan een mobiele telefoon worden gebruikt, waarvan de BLE-signaal binnen een bepaalde afstand gedetecteerd moet worden.
- **GPS (Mobiele App) :** Om verificatie op basis van de locatie van de gebruiker uit te voeren, kan een geautoriseerde mobiele applicatie die op de achtergrond automatisch een request naar het systeem sturen zodra de gebruiker zich binnen een bepaald bereik bevindt.

- Cie-group, (Onbekend) Access control contactless authentication methods

5.5 VERGELIJKINGSMATRIX

De onderstaande matrix geeft een visuele vergelijking van de verschillende verificatiemethoden op basis van vier belangrijke criteria: Veiligheid, Gebruiksgemak, Snelheid en Kosten. De kleuren in de tabel vertegenwoordigen de score per criteria.

De veiligheid score staat los van de eventuele anti-spoofing maatregelen die in de volgende hoofdstuk worden onderzocht.

Methode	Veiligheid	Gebruikersgemak	Snelheid	Kosten
Gezichtsherkenning				
Spraakherkenning				
Vingerafdruk				
RFID				
BLE				
GPS (Mobiele APP)				

5.6 CONCLUSIE

Gezichtsherkenning + (BLE/GPS)?

6.0 WELKE ANTI-SPOOFING MAATREGELEN KUNNEN ER WORDEN GENOMEN?

Facial-recognition => detection
Facial-recognition => thermal facial scan
Facial-recognition => proximity sensors
BLE / GPS => rolling hashes

X.0 BRONNEN

- Paxton, (Onbekend) Hoe maak ik een veilig toegangscontrole systeem nog veiliger?
- Anviz, (Onbekend) Slimme oplossing voor toegangscontrole
- Bosch, (Onbekend) Biometrische toegangscontrole
- Seon, (Onbekend) Biometric Verification
- Shaip, (2024) Wat is spraakherkenning.
- Veiliginternetten, (Onbekend) Wat is biometrische authenticatie? En wanneer gebruik je het?
- Cie-group, (Onbekend) Access control contactless authentication methods