

Biometrisch Toegangssysteem

Onderzoek naar de ontwikkeling van een veilig en schaalbaar biometrisch toegangssysteem

BIOMETRISCH TOEGANGSSYSTEEM
PIOTR TADRALA | INFORDB

I. MANAGEMENT & SAMENVATTING

//TODO: Compleet samenvatting

II. VERSIEBEHEER & DISTRIBUTIE

VERSIEBEHEER

<i>Versie</i>	<i>Omschrijving</i>	<i>Auteur</i>
0.1	Eerste opzet van het document	Piotr Tadralla
0.2		
0.3		

DISTRIBUTIEBEHEER

<i>Versie</i>	<i>Ontvangers</i>
0.1	
0.2	
0.3	

III. WOORDENLIJST

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

INHOUDSOPGAVE

I. Management & Samenvatting	1
II. Versiebeheer & Distributie	2
Versiebeheer	2
Distributiebeheer	2
III. Woordenlijst.....	3
1.0 Inleiding	6
2.0 Context.....	7
2.1 Inleiding	7
2.2 Huidige situatie.....	7
2.3 Probleemstelling.....	7
2.4 Doelstelling	8
3.0 Onderzoeksaanpak.....	9
3.1 Inleiding	9
3.2 Hoofdvraag	9
3.3 Deelvragen.....	9
3.4 Onderzoeksmethoden	9
3.5 Verwachte onderzoeksuitkomsten	9
3.6 Scope	10
4.0 Zijn er al vergelijkbare systemen op de markt?	11
4.1 Inleiding	11
4.2 Bestaande oplossingen	11
4.3 Good & Bad practices.....	13
4.4 Huidige Marktstandaarden.....	13
4.5 Conclusie	14
5.0 Welke verificatiemethodes zijn er beschikbaar?	15
5.1 Inleiding	15
5.2 Beoordelingcriteria	15
5.3 Biometrische verificatiemethodes	15
5.4 Traditionele verificatiemethodes	15
5.5 Vergelijkingsmatrix	16
5.6 Conclusie	17
6.0 Welke anti-spoofing maatregelen kunnen er worden genomen?	18
7.0 Welke Architectuur en Welk Platform Zijn Geschikt voor een Schaalbaar en Uitbreidbaar Toegangssysteem?	19
7.1 Inleiding	19
7.2 Requirements.....	19
7.2.1 Functionele eisen.....	19

7.2.3 Technische eisen	19
7.3 Platform	19
7.3.1 Potentiele opties	19
7.3.2 Vergelijking.....	20
7.3.3 Beoordelingscriteria	20
7.3.4 Vergelijkingsmatrix.....	21
7.3.5 Conclusie.....	21
x.0 Bronnen.....	23

1.0 INLEIDING

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, gebruikersvriendelijk en veilig moet zijn.

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.
- **Privacyrisico's en angst voor datalek:** Biometrische gegevens zijn zeer gevoelig. Wanneer deze gegevens worden gelekt of gestolen, zijn ze niet eenvoudig te wijzigen zoals wachtwoorden.
- **Foutmarges en onnauwkeurigheid:** Biometrische systemen zijn niet altijd 100% nauwkeurig. Slechte lichtomstandigheden, verouderde algoritmes of wijzigingen in het uiterlijk van de gebruiker kan leiden tot onnauwkeurigheid van het systeem.
- **Hoge kosten:** De implementatie van geavanceerde biometrische systemen, zoals die met liveness-detectie of geavanceerde sensoren, kan hoge initiële kosten en onderhoudskosten met zich meebrengen.
- **Afhankelijkheid van technologie bij storingen:** Storingen in het systeem, zoals netwerkproblemen of hardwarefouten, kunnen de toegang blokkeren of het systeem onbetrouwbaar maken. Er dient dus altijd een back-upmethode aanwezig te zijn.

2.3 PROBLEEMSTELLING

Hoewel biometrische toegangssystemen een hoger beveiligingsniveau bieden dan traditionele methoden, zijn ze kwetsbaar voor misleidingspogingen zoals deepfakes en spoofing. Daarnaast vertrouwen veel systemen op slechts één enkele verificatiemethode, wat de veiligheid beperkt en de kans op ongeautoriseerde toegang vergroot. Bovendien brengen deze systemen privacyrisico's, foutmarges en hoge implementatiekosten met zich mee.

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 Architectuur en Welk Platform Zijn Geschikt voor een Schaalbaar en Uitbreidbaar Toegangssysteem?
D5	Welke componenten zijn er nodig en wat zijn de kosten 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.

4.0 ZIJN ER AL VERGELIJBARE 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.

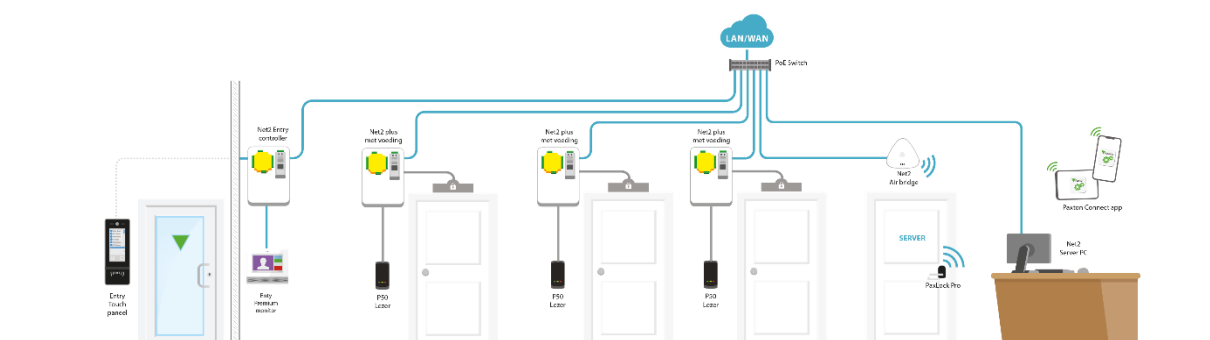
4.2 BESTAANDE OPLOSSINGEN

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.

Systemen van Paxton, zijn ontworpen met een modulaire opbouw. Voor elke deur die u wilt beveiligen, is één deurcontroller nodig. Deze architectuur maakt het mogelijk om klein te beginnen en het systeem vervolgens eenvoudig uit te breiden.

Paxton biedt draadloze deurbeslagen, zoals PaxLock, die rechtstreeks op de deur kunnen worden gemonteerd zonder noodzaak voor bekabeling. Deze beslagen communiceren volledig draadloos.



- 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.

Toegangscontrolesystemen van Anviz worden eenvoudig aan de muur bevestigd en aangesloten op een 12V DC-voeding en netwerk via Ethernet of Wi-Fi. De configuratie verloopt via de CrossChex-software, waarin gebruikers worden geregistreerd met biometrische gegevens of RFID-kaarten, en toegangsrechten worden ingesteld. Ook is mobiele toegang via een app mogelijk. De installatie is snel en gebruiksvriendelijk.



- Anviz, (Onbekend) [Slimme oplossing voor toegangscontrole](#)

BOSCH SECURITY

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

Bosch Security-toegangscontrolesystemen bieden een eenvoudige installatie met zowel bekabelde als draadloze opties. De apparaten worden aangesloten op een centrale controller en geïntegreerd met bestaande infrastructuur via Ethernet of RS485. Configuratie verloopt via Bosch's beheerssoftware, waarin gebruikers biometrische gegevens of RFID-kaarten registreren en toegangsrechten beheren. De systemen ondersteunen ook contactloze toegang en kunnen eenvoudig worden beheerd via een webinterface of mobiele app.



- Bosch, (Onbekend) [Biometrische toegangscontrole](#)

4.3 GOOD & BAD PRACTICES

PAXTON

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

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. Installatieprocessen verschillen per leverancier, maar de meeste systemen bieden eenvoudige, modulaire installatieopties met beheer via software of mobiele applicaties

4.5 CONCLUSIE

Bestaande toegangscontrolesystemen bieden flexibele API-integraties en modulaire installatieopties. Anti-spoofing is aanwezig, maar vaak beperkt tot basale liveness-detectie op gezichtskenmerken. MFA wordt ondersteund, maar voornamelijk via traditionele methoden zoals smartcards en PIN-codes. Hoewel deze oplossingen een goede basis bieden, ontbreekt het vaak aan geavanceerde anti-spoofingtechnieken en moderne MFA-opties die de algehele veiligheid verder kunnen versterken.

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 tot de conclusie 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 betrouwbaar is de methode?
- **Gebruikersgemak:** Hoe gebruikersvriendelijk en seamless is de verificatie?
- **Snelheid:** Hoe snel kan de gebruiker 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-sigitaal 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.
 - **Pincode:** De gebruiker voert een vooraf ingestelde pincode in via een keypad of touchscreen.
 - **Push-notificatie:** De gebruiker ontvangt een pushmelding op zijn smartphone en moet de toegang handmatig goedkeuren of weigeren.
- 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.

Score	Betekenis	Kleur			
1	Slecht	Rood			
2	Gemiddeld	Geel			
3	Goed	Groen			

Methode	Veiligheid	Gebruiksgemak	Snelheid	Kosten	Totaal
<i>Gezichtsherkenning</i>	2	3	3	1	9
<i>Spraakherkenning</i>	1	2	1	2	6
<i>Vingerafdruk</i>	3	1	2	1	7
<i>RFID</i>	2	2	1	1	6
<i>BLE</i>	3	2	2	3	10
<i>GPS (Mobiele APP)</i>	3	2	2	3	10
<i>Pincode</i>	2	2	1	3	8
<i>Push-Notificatie</i>	3	2	2	3	10

5.6 CONCLUSIE

Voor de primaire verificatiemethode lijkt gezichtsherkenning de beste keuze. Het is snel, veilig en gebruiksvriendelijk. Een nadeel zijn de hogere kosten en het feit dat gezichtsherkenning relatief makkelijk te spoofen is, maar dit wordt in het volgende hoofdstuk verder onderzocht. Voor de secundaire verificatie kiezen we voor combinatie van een pincode of een push-notificatie, waarbij de gebruiker aan eentje moet voldoen. De pincode biedt extra zekerheid, omdat het de gebruiker op basis van kennis verifieert, naast de biometrische gegevens. Een push-notificatie verhoogt het gebruiksgemak, omdat de gebruiker zijn telefoon al kan voorbereiden voordat hij de deur komt. Zodra het gezicht gescand is, hoeft de gebruiker alleen nog de melding te bevestigen.

6.0 WELKE ANTI-SPOOFING MAATREGELEN KUNNEN ER WORDEN GENOMEN?

Facial-recognition => detection

Facial-recognition => thermal facial scan

Facial-recognition => proximity sensors

<https://bioconnect.com/blog/2024/01/30/anti-spoofing-facial-authentication-hardware-what-you-need-to-know#:~:text=Liveness%20Detection%3A%20Implement%20liveness%20detection,depth%20estimation%2C%20or%20infrared%20sensors.>

<https://paperswithcode.com/task/face-anti-spoofing>

7.0 WELKE ARCHITECTUUR EN WELK PLATFORM ZIJN GESCHIKT VOOR EEN SCHAAALBAAR EN UITBREIDBAAR TOEGANGSSYSTEEM?

7.1 INLEIDING

Het toegangssysteem moet gebruiksvriendelijk, schaalbaar en veilig zijn. Daarom is het cruciaal om goede keuzes te maken over de architectuur en het te gebruiken platform. InforDB wilt het systeem eenvoudig integreerbaar te maken met bestaande softwareoplossingen, waardoor goede integratiemogelijkheden cruciaal zijn.

7.2 REQUIREMENTS

7.2.1 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.

7.2.3 TECHNISCHE EISEN

- De backend moet REST API ondersteunen.
- Het 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).

7.3 PLATFORM

7.3.1 POTENTIELE OPTIES

Voor het platform zijn er meerdere opties. We kunnen kiezen voor een **embedded opzet**, waarbij het volledige systeem in één hardwarecomponent is geïntegreerd. Dit is de meest gebruiksvriendelijke optie, omdat de gebruiker enkel het kastje hoeft te monteren en te installeren—daarna is het systeem direct operationeel.

Een andere optie is een **on-premise opzet**, waarbij het kastje bij de voordeur gegevens verzamelt, zoals camerabeelden en pincodes. Deze data wordt vervolgens via het lokale netwerk verstuurd naar een centrale hub binnen het gebouw. De hub verwerkt de data en neemt de uiteindelijke beslissingen, zoals het openen van de deur.

Tot slot is er de **cloud-opzet**, waarbij het kastje eveneens de data verzamelt, maar deze direct naar de cloud stuurt voor verwerking. Beslissingen en logica worden hierbij extern afgehandeld, wat het beheer en schaalbaarheid eenvoudiger kan maken, maar afhankelijk is van een stabiele internetverbinding.

7.3.2 VERGELIJKING

Om te bepalen welke opzet het meest geschikt is voor ons systeem, moeten de voor- en nadelen van de verschillende architectuuropties worden vergeleken. Hieronder een overzicht van de genoemde opties.

Embedded

<i>Voordelen</i>	Plug & Play
	Snelle verwerking, omdat alles lokaal gebeurt, is er geen vertraging door netwerkcommunicatie
	Onafhankelijk van het network
	Hogere privacy dankzij alle data die lokaal blijft opgeslagen
<i>Nadelen</i>	Beperkte rekenkracht
	Niet schaalbaar
	Beperkte functionaliteiten zonder netwerkverbinding
	Beperkte management opties

On-Premise

<i>Voordelen</i>	Hogere privacy dankzij alle data die lokaal blijft opgeslagen
	Schaalbaar
	Vereist geen internetverbinding
	Voldoende rekenkracht
<i>Nadelen</i>	Complexere installatie
	Beperkte functionaliteiten zonder netwerkverbinding
	Beperkte management opties

Cloud

<i>Voordelen</i>	Makkelijke installatie
	Geen fysieke onderhoudskosten
	Management mogelijkheden op afstand
	Schaalbaar
<i>Nadelen</i>	SaaS opzet wat waarschijnlijk maandelijkse abonnement zal vereisen
	Beperkte privacy
	Afhankelijkheid van internetverbinding

- Robert Chamberlin, (2024) [Key differences between on-premise and cloud based access control systems](#)
- Sailpoint, (2025) [Cloud based access control vs. on-premise](#)

7.3.3 BEOORDELINGSCRITERIA

Nu de voor- en nadelen van elk platform globaal in kaart zijn gebracht, kunnen we de belangrijkste criteria voor ons systeem bepalen. Door een vergelijkingsmatrix op te stellen en de platforms te beoordelen op deze criteria, kunnen we concluderen welk platform het meest geschikt is.

- **API Integraties:** Hoe makkelijk is het systeem integreerbaar andere systemen?
- **Scalability:** Hoe schaalbaar is het systeem voor eventuele toekomstige uitbreidingen?
- **Data Privacy:** Hoe goed wordt data beschermd tijdens opslag en overdracht?
- **Snelheid & Latency:** Hoe snel kan het systeem verificaties uitvoeren?
- **Betrouwbaarheid:** Hoe robuust is het systeem?
- **Management:** Hoe beheerbaar is het systeem?

7.3.4 VERGELIJKINGSMATRIX

Score	Betekenis	Kleur
1	Slecht	Rood
2	Gemiddeld	Geel
3	Goed	Groen

Criteria	Embedded	On-Premise	Cloud
<i>Api Integraties</i>	1	1	3
<i>Scalability</i>	1	2	3
<i>Data Privacy</i>	3	3	2
<i>Snelheid & Latency</i>	3	2	2
<i>Betrouwbaarheid</i>	3	3	2
<i>Management</i>	2	2	3
Totaal	13	13	17

7.3.5 CONCLUSIE

Uit het onderzoek naar de platforms is het te concluderen dat geen enkel platform volledig voldoet aan alle eisen. Elk platform heeft zijn eigen sterke en zwakke punten. Daarom zal de oplossing bestaan uit een **hybride opzet van on-premise en cloud**. In deze opzet draait de hardware lokaal en communiceert met een centrale hub, die vervolgens verbinding maakt met een cloud-backend voor extra functionaliteiten, zoals API-integraties en beheer op afstand.

7.4 COMMUNICATIEPROTOCOLLEN

7.4.1 ON-PREMISE COMMUNICATIE

Bij een on-premise opzet, dienen de individuele componenten met elkaar te kunnen communiceren. Hiervoor is het noodzakelijk om een geschikt communicatieprotocol te kiezen. De meest gebruikte protocollen waaruit gekozen kan worden zijn MQTT, COAP, HTTP en WebSockets

MQTT

MQTT is een publish/subscribe-protocol dat werkt op basis van berichten. Het gebruikt het TCP-protocol voor betrouwbare communicatie tussen de broker en de aangesloten clients (publishers en subscribers).

De MQTT-broker functioneert als de centrale server die verantwoordelijk is voor het ontvangen, filteren en doorsturen van berichten naar de juiste clients. De publishers verzenden berichten naar specifieke topics op de broker, terwijl de subscribers zich subscriben op deze topics om de berichten te ontvangen.

COAP

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](#)
- Robert Chamberlin, (2024) [Key differences between on-premise and cloud based access control systems](#)
- Sailpoint, (2025) [Cloud based access control vs. on-premise](#)
- Ian Craggs, (2022) [MQTT vs CoAP for IoT](#)
- Sob, (2017) [What are the differences between MQTT, HTTP, CoAP devices \(besides communication protocol\)?](#)