

Machine Learning Pipeline Automation

Amar Kisoensingh

11 juni 2021

Voorwoord

Samenvatting

Summary

Lijst van figuren

1.1	Organogram van NGTI op 29-03-2021 [ngti-organogram].	10
1.2	Screenshot van de Swiss Climate Challenge app [ngti-swisscom-climate-challenge].	11
1.3	Screenshot van de My Swisscom App [ngti-my-swisscom-app]	11
4.1	Machine learning in de context van andere domeinen	20
4.2	Lifecycle van een model volgens Hapke en Nelson [building-machine-learning-pipelines-oreilly].	22
4.3	Gamma hyperparameter van een support vector classification (SVC) algoritme met waarde 0.1	24
4.4	Gamma hyperparameter van een support vector classification (SVC) algoritme met waarde 100	24
4.5	Model uitgerold met behulp van een API.	26
4.6	Vorm van expliciete feedback gebruikt door YouTube.	26
4.7	Machine learning pipeline met een algoritme exploratie tussenstap.	28
4.8	Machine learning pipeline waarbij stappen geautomatiseerd kunnen worden voor het gemak van developers.	29
5.1	Voorbeeld van een infrastructure as code (IaC) plan [terraform-plan-example].	31
5.2	Proces van een infrastructure as code (IaC) om aan de gewenste situatie te voldoen.	32
5.3	Sequence diagram van het experiment met orkestratietool Pulumi	35
5.4	Node.js server voor het experiment met orkestratietool Pulumi	36
5.5	De stack voor het experiment	36
5.6	POST endpoint van de Pulumi experiment	37
6.1	Voorbeeld van een C4 model [c4-model].	39
6.2	Context niveau diagram van het architecturaal ontwerp.	40
6.3	Container niveau diagram van het architecturaal ontwerp.	41
6.4	Single page application (SPA) component niveau diagram van het architecturaal ontwerp.	41
6.5	Node.js server component niveau diagram van het architecturaal ontwerp.	42
6.6	Sequence diagram van het aanmaken van een pipeline.	43
6.7	Sequence diagram van het starten van een pipeline.	44
7.1	Requirements opgesteld voor de proof of concept.	46
7.2	Sprint 1.	47

Lijst van tabellen

3.1	Onderzoeks methode deelvraag 1	17
3.2	Onderzoeks methode deelvraag 2	17
3.3	Onderzoeks methode deelvraag 3	17
3.4	Onderzoeks methode hoofdvraag	18
5.1	Knock-out criteria voor orkestratietools dat cloud computing platformen beheerd.	32
5.2	Knock-out criteria tegen orkestratietools dat cloud computing platformen beheerd.	33
1	Scope deelvraag 1	53
2	Scope deelvraag 2	54
3	Scope deelvraag 3	54
4	Scope hoofdvraag	55

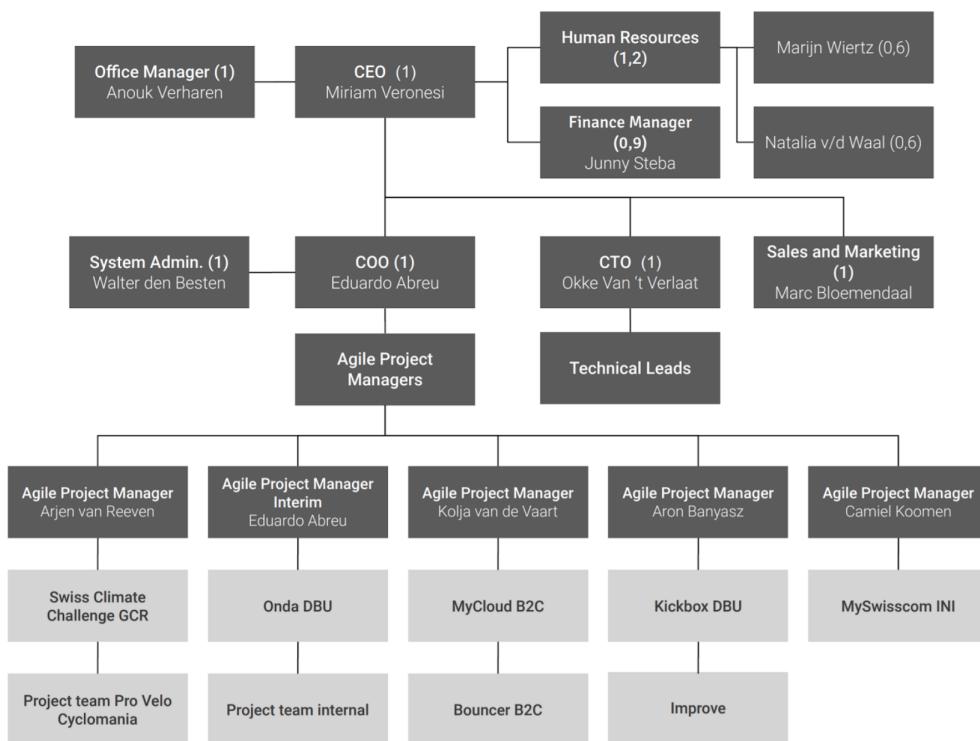
Inhoudsopgave

1 Inleiding	9
1.1 Projecten van NGTI	10
1.2 Tools die worden gebruikt	11
1.3 Aanleiding opdracht	12
1.4 Leeswijzer	12
2 Probleemanalyse	13
2.1 Obstakels voor NGTI	14
2.2 Vooronderzoek naar bestaande oplossingen	15
2.3 Doelstelling	15
2.4 Hoofd- en deelvragen	15
3 Onderzoeksmethoden en scope	16
4 Stappen in een machine learning pipeline	19
4.1 Wat is machine learning?	20
4.2 De stappen in een machine learning pipeline	21
4.3 Conclusie	27
4.4 Advies	27
5 Orkestratietools om platformen te beheren	30
5.1 Wat is infrastructure as code?	31
5.2 Orkestratietools vergeleken met elkaar	32
5.3 Experiment met de orkestratietool Pulumi	33
5.4 Conclusie	37
6 Architecturale ontwerp van de oplossing	38
6.1 Het C4 model	39
6.2 Architecturaal ontwerp	40
6.3 Sequence diagrammen	43
7 Proof of concept	45
7.1 User requirements verzamelen	46
7.2 Mock up van de proof of concept	47
7.3 De proof of concept	47
7.4 Kwaliteit van de code	47
7.5 Conclusie	47
7.6 Advies	47
8 Discussie	48
8.1	49
9 Reflectie	50
Bibliografie	51

1 Inleiding

NGTI is een software ontwikkelbedrijf dat gevestigd is in Rotterdam. Opgericht in 2012 maakt NGTI applicaties (apps) voor mobiel en/of webgebruik. Naast het ontwikkelen werkt NGTI aan het hele traject om een app heen, namelijk de probleemstelling, mockups, wireframes en prototyping. Daarnaast levert NGTI ook support en lost bugs op nadat een app live is gegaan [[ngti-services](#)]. Ook maakt NGTI white label apps en frameworks [[ngti-solutions](#)].

Het bedrijf heeft, zoals de meeste bedrijven, een organogram (Figuur 1.1). In de praktijk is dit echter niet terug te vinden en wordt de structuur gezien als "plat". Collega's kunnen elkaar laagdrempelig benaderen waardoor niemand een onbekende is en verschillende disciplines makkelijk met elkaar samen kunnen werken.



Figuur 1.1: Organogram van NGTI op 29-03-2021 [[ngti-organogram](#)].

NGTI is een dochterbedrijf van Swisscom [[swisscom-other-division](#)]. Sinds maart 2021 is het bekend gemaakt dat Swisscom van plan is om een afdeling, Swisscom DevOps Center, te fuseren met NGTI. Omdat de fusie onzekerheid met zich meebrengt voor de structuur en manier hoe NGTI werkt, zal de situatie vóór de fusie aangehouden worden gedurende het afstuderen.

1.1 Projecten van NGTI

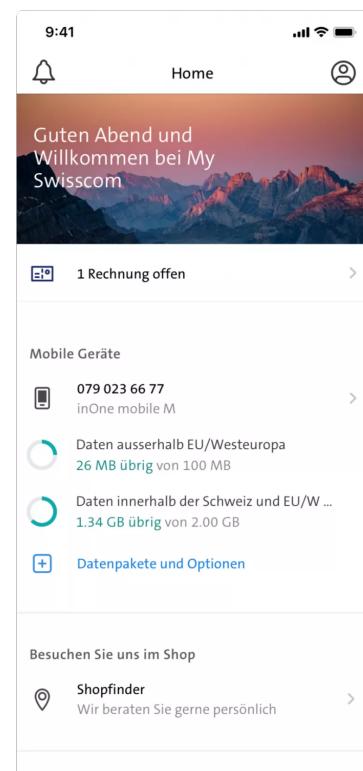
NGTI heeft een vrij breed portfolio met apps voor verschillende doeleinden. Een van deze apps is de Climate Challenge App [[ngti-swisscom-climate-challenge](#)]. Met deze app kunnen gebruikers hun CO₂-voetafdruk en impact in kaart brengen. Er wordt bijgehouden hoeveel kilometer de gebruiker reist en met welk vervoersmiddel. De app is onderdeel van twee bestaande

nieuwsapps, Blick en Bluewin [[swisscom-climate-challenge-integration](#)]. Het doel is om de gebruiker aan te sporen om groener te reizen. Een screenshot van de app is te zien in Figuur 1.2.

Een andere oplossing is de My Swisscom App [[ngti-my-swisscom-app](#)]. Dit is een native app voor Android en iOS waarbij Swisscom-klanten hun contract kunnen bestellen, wijzigen of beëindigen. In de app kunnen klanten ook de dataverbruik zien en instellingen voor abonnementen wijzigen. Een screenshot van de app is te zien in Figuur 1.3.



Figuur 1.2: Screenshot van de Swiss Climate Challenge app [[ngti-swisscom-climate-challenge](#)].



Figuur 1.3: Screenshot van de My Swisscom App [[ngti-my-swisscom-app](#)]

1.2 Tools die worden gebruikt

Om productief te zijn, gebruikt NGTI een aantal tools en programma's om producten te maken en te communiceren met zowel collega's als klanten. De meest gebruikte en belangrijkste zijn Slack, Google Workspace, Zoom en Microsoft Teams.

1.2.1 Slack

Interne communicatie gaat via Slack. Het programma faciliteert collega's om elkaar met een lage instap te benaderen en berichten die voor het hele bedrijf relevant zijn te versturen. Ook zijn er 'channels' beschikbaar over specifieke onderwerpen, zoals: `#dev`, `#ios` en `#test-automation`.

1.2.2 Google Workspace

Met Google Workspace kunnen bestanden en documenten gemaakt, opgeslagen en gedeeld worden. Dit is mogelijk via een browser waardoor werknemers geen software hoeven te installeren. NGTI gebruikt het ook om collaboratief en parallel te werken aan hetzelfde document.

1.2.3 Microsoft Teams en Zoom

Voorheen werd Zoom alleen gebruikt om te videobellen met collega's en geïnterviewden. In de tijd van de pandemie is Zoom echter een belangrijke speler geworden om effectief samen te werken. Meetings zoals introducties van nieuwe collega's of demo's van producten worden online gehouden.

1.3 Aanleiding opdracht

NGTI wilt de gebruikerservaring van haar apps verbeteren en een voorsprong hebben op haar concurrenten. Dit kan NGTI op een aantal manieren doen waarvan apps "slimmer" maken er een van is. Het slimmer maken houdt voor NGTI in dat de app bijvoorbeeld beter kan anticiperen wat de gebruiker wilt en nodig heeft op een gegeven moment. Dit kan onder andere door het toepassen van machine learning (ML). De opdracht kan verdeeld worden in twee onderdelen:

- Onderzoek naar hoe een pipeline opgezet kan worden op een cloud computing platform door middel van een framework
- Onderzoek naar het maken van een platform-agnostische oplossing

Daarnaast zal een proof-of-concept (PoC) gemaakt worden om aan te tonen of het haalbaar is in de praktijk. Een diepere duik in het probleem en het definiëren van de onderdelen is te vinden in hoofdstuk 2.

1.4 Leeswijzer

TODO: Schrijf leeswijzer voor elk hoofdstuk

2 Probleemanalyse

Zoals beschreven in paragraaf 1.3 wilt NGTI ML toepassen om haar apps slimmer te maken. Hier zijn een aantal redenen voor, onder andere om de gebruikerservaring te verbeteren en om een voorsprong te hebben op concurrenten.

Het 'slimmer' maken van applicaties kan op verschillende manieren, maar met machine-learning kan een platform gebouwd worden waarmee elke richting op gegaan kan worden. Om machine-learning te implementeren in haar applicaties loopt NGTI tegen een aantal obstakels aan, namelijk: expertise vereist in het ML domein, benodigde tijd om een pipeline op te zetten en vendor lock-in.

2.1 Obstakels voor NGTI

NGTI loopt tegen de voorgenoemde obstakels aan omdat NGTI weinig ervaring heeft met ML. In samenwerking met een extern bedrijf worden modellen getraind die vervolgens gebruikt worden in apps van NGTI. Om zelf modellen te trainen heeft NGTI kennis over ML, ML pipelines en tijd nodig. Bovendien wilt NGTI niet bij één cloud computing platform haar infrastructuur opzetten maar gemakkelijk kunnen schakelen tussen platformen. De obstakels worden in de volgende koppen verduidelijkt.

2.1.1 Expertise Machine Learning

ML is ingewikkeld en diepgaand onderwerp. Om een model te trainen is kennis nodig van verschillende domeinen: data mining, software engineering en statistieken. Doordat er voorkennis nodig is om een model te trainen en een pipeline goed op te zetten, is het vaak te hoogdrempelig voor developers om een start te maken met ML. De expertise is daarnaast niet in een korte tijd te vergaren.

2.1.2 Opzetten pipeline

Bovenop de complexiteit van ML zelf bestaan er verschillende manieren om een model te trainen. Het opzetten van ML pipelines is daar een van. Een pipeline is een workflow dat bestaat uit een aantal stappen die doorgelopen worden om een model te trainen. In elke stap worden acties uitgevoerd, zoals het verwijderen van onbruikbare data of de prestatie van modellen vergelijken en een rapport met uitslagen genereren. Het opzetten van zo een pipeline én de actie(s) in de stappen definiëren kost tijd en vereist specifieke kennis. Daarnaast zijn de stappen en acties vaak hetzelfde voor verschillende pipelines. Het automatiseren en hergebruiken van stappen en acties tussen pipelines zou tot onder andere tijdwinst en het verminderen van herhaling van code kunnen leiden.

2.1.3 Vendor lock-in

Er bestaan een aantal diensten, zogenoemde Platform as a Service (PaaS), waarbij je een pipeline kan opzetten en acties kan definiëren. Een van de problemen met een PaaS is vendor lock-in. Dit betekent dat, als er eenmaal een pipeline is opgezet, de overdraagbaarheid van de pipeline naar een andere PaaS vrijwel onmogelijk is. Ook zijn de opties en mogelijkheden om uit te breiden in de toekomst gelimiteerd.

2.2 Vooronderzoek naar bestaande oplossingen

Het gebruik van ML pipelines is geen nieuwe techniek en is mogelijk bij PaaS en bedrijven die zich specialiseren in ML pipelines. Het gemak met zulke services is dat de gebruiker gelijk kan beginnen met het trainen van ML modellen en zich niet zorgen hoeft te maken over infrastructurele details. Echter is er sprake van vendor lock-in en kunnen services van deze bedrijven niet gebruikt worden.

Gedurende de vooronderzoek zijn "Infrastructure as Code" frameworks naar voren gekomen. Dit zijn frameworks waarmee, middels code, een infrastructure binnen een Platform as a Service (PaaS) opgezet kan worden. Dit kan gebruikt worden als onderdeel van de PoC en wordt in een van de deelvragen verder onderzocht.

2.3 Doelstelling

Om haar doel, de gebruikerservaring van apps verbeteren en een voorsprong hebben op concurrent, te bereiken is NGTI van plan ML pipelines te gebruiken om ML toe te passen. De gewenste oplossing is een systeem waarbij developers met weinig tot geen kennis een model kunnen trainen. Het systeem moet de infrastructurele taken voor zich nemen, zoals het opzetten van een pipeline en de stappen en acties automatiseren. Daarnaast moet een ML pipeline pijnloos doorlopen kunnen worden op verschillende platformen zodat het systeem platform-agnostisch is.

2.4 Hoofd- en deelvragen

Uitgaand van de drie obstakels kan de hoofdvraag als volgt worden geformuleerd:

*In welke mate kan een machine learning pipeline worden
geautomatiseerd onafhankelijk van het onderliggende cloud computing
platform?*

De hoofdvraag kan worden onderbouwd met vier deelvragen. Om te beginnen is het verstandig om te weten welke stappen er in een machine learning pipeline zit:

Waar bestaat een machine learning pipeline uit?

Daarnaast is een framework nodig dat, door middel van code, verschillende cloud computing platformen kan beheren:

*Hoe kan een framework verschillende cloud computing platformen beheren om een
machine learning pipeline op te zetten?*

Ten slotte wordt een PoC gemaakt om te laten zien of het probleem oplosbaar is. Hiervoor is een doordachte voorbereiden onmisbaar:

*Hoe ziet de architecturale blauwdruk van een applicatie, waarmee een
platform-onafhankelijk machine learning pipeline opgezet kan worden, eruit?*

3 Onderzoeksmethoden en scope

Om elke hoofd- en deelvraag te beantwoorden, wordt er bij elk gebruik gemaakt van een onderzoeks methode. Volgens Scribbr [research-methods] zijn er twee onderzoeks methoden: kwantitatief en kwalitatief. Bij een kwantitatief onderzoeks methode wordt data verzameld waarmee bijvoorbeeld grafieken of tabellen gemaakt kunnen worden. De focus bij een kwalitatief onderzoeks methode ligt bij het verzamelen van verschillende interpretaties en opvattingen. Hierop kan optioneel een eigen interpretaties op gemaakt worden. [quantitative-vs-qualitative].

Onder kwantitatief en kwalitatief vallen verschillende dataverzamelings methoden. Deze beschrijft simpelweg de manier hoe data wordt verzameld. Dit kan bijvoorbeeld met een enquête, literatuur onderzoek op websites en in boeken of een onderzoek over een lange periode [quantitative-vs-qualitative].

Elke hoofd- en deelvraag is gekoppeld aan een onderzoeks methoden. Vervolgens is beschreven welk(e) dataverzamelings methode(n) wordt gebruikt met een korte toelichting. Daarnaast wordt op een hoog niveau de scope bepaald.

D1: Waar bestaat een machine learning pipeline uit?	
Methode(s)	Kwalitatief
Dataverzamelings methode(n)	Literatuuronderzoek, fundamenteel onderzoek, toegepast onderzoek
Scope	Bijlage 9

Tabel 3.1: Onderzoeks methode deelvraag 1

D2: Hoe kan een orkestratietool verschillende cloud computing platformen beheren om een machine learning pipeline op te zetten?	
Methode	Kwalitatief
Dataverzamelings methode(n)	Literatuuronderzoek, vergelijkend onderzoek
Scope	Tabel 9

Tabel 3.2: Onderzoeks methode deelvraag 2

D3: Hoe ziet de architecturale blauwdruk van een applicatie, waarmee een platform-onafhankelijk machine learning pipeline opgezet kan worden, eruit?	
Methode	Kwalitatief
Dataverzamelings methode(n)	Literatuuronderzoek
Scope	Tabel 9

Tabel 3.3: Onderzoeks methode deelvraag 3

H: In welke mate kan een machine learning pipeline worden geautomatiseerd onafhankelijk van de onderliggende cloud computing platform?	
Methode	Kwalitatief
Dataverzamelingsmethode(n)	Literatuuronderzoek
Scope	Tabel 9

Tabel 3.4: Onderzoeks methode hoofdvraag

4 Stappen in een machine learning pipeline

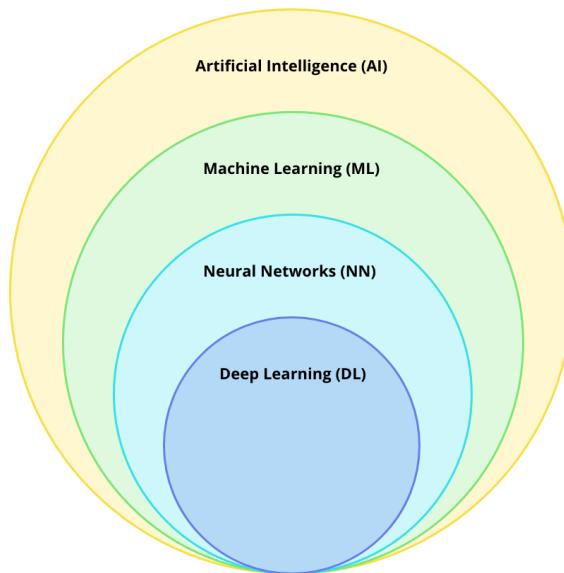
Een ML pipeline is zoals beknopt beschreven in deelparagraaf 2.1.2 een collectie van stappen dat wordt doorlopen om een model te trainen. Elke stap bevat een aantal acties dat wordt uitgevoerd, zoals onbruikbare data weghalen of de prestatie analyseren. De stappen en acties worden in paragraaf 4.2 uitgelegd met behulp van theorie en een experiment dat is uitgevoerd. Het volledige experiment is te vinden in [BIJLAGE LINK]. Een van de stappen in een pipeline is het trainen van het model. Om een idee te krijgen van ML en het trainen van modellen zal dit kort uitgelegd worden.

4.1 Wat is machine learning?

ML houdt in dat een computer een taak kan uitvoeren zonder daarvoor expliciet geprogrammeerd te zijn. Dit wordt gedaan door een ML model te laten leren van een gegeven dataset. Vervolgens kan er een voorspelling worden gemaakt [**introduction-to-machine-learning**].

De domeinen deep learning (DL), neural networks (NN) en artificial intelligence (AI) komen vaak voor als het over ML gaat. Zoals weergegeven in Figuur 4.1 is te zien dat ML een subset is van AI, NN een subset van ML en als laatste DL dat een subset is van NN [**ai-ml-nn-dl**].

Bij AI wordt niet alleen ML toegepast, maar ook concepten zoals beredeneren, plannen, vooruit-denken, onthouden en terug refereren. Een voorbeeld hiervan is dat een ML model kan voorspellen wat het volgende woord in een zin kan zijn, maar een AI kan beredeneren waarom de zin gebouwd is zoals het is en hoe het binnen de context van de alinea past [**ml-think-about-ml-brownlee**].



Figuur 4.1: Machine learning in de context van andere domeinen

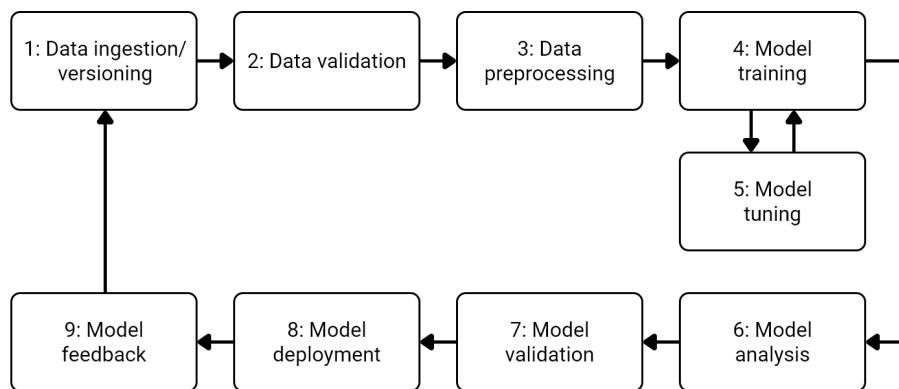
Een NN bestaat uit een collectie van nodes dat gemodelleerd is naar de hersenen. Een NN heeft minimaal 3 lagen: een inputlaag, een verborgen laag en een outputlaag. Elke laag bevat neuronen dat data als input kan krijgen en data als output aan de volgende laag meegeeft. DL is een NN dat meerdere verborgen lagen bevat [**ml-neural-network-nicholson**].

4.1.1 Een manier om een machine learning model te trainen

Het trainen van een ML model is een proces waarbij vooraf data wordt opgeschoond en achteraf de prestatie van het model wordt gevalideerd. Normaliter wordt dit gedaan door specifieke code te schrijven voor deze taken. Een valkuil is dat de code niet bij elke developer werkt en schaalt niet in alle gevallen naar een productieomgeving. Een manier om dit wel te behalen is om te werken met ML pipelines. Zoals kort uitgelegd in deelparagraaf 2.1.2 bestaat een ML pipeline uit stappen en acties. Er is echter geen consensus binnen het ML domein over wat de juiste stappen en acties in een pipeline zijn. Voor de scriptie is gekozen voor een pipeline van Hapke en Nelson uit het boek "Building Machine Learning Pipelines". Het boek is gemaakt en gepubliceerd door O'Reilly; een bekend en gecrediteerd bedrijf dat boeken maakt binnen het software engineering domein.

4.2 De stappen in een machine learning pipeline

Een ML pipeline begint met het opnemen van data en eindigt met het ontvangen van feedback om de prestatie van het model te verbeteren. De pipeline bevat een aantal stappen zoals data voorbereiden, het model trainen en het uitrollen van het model (Figuur 4.2).



Figuur 4.2: Lifecycle van een model volgens Hapke en Nelson [building-machine-learning-pipelines-oreilly].

In totaal zijn er, zonder de feedbackloop stap, acht stappen die elke keer doorlopen moeten worden om een model te trainen. In de volgende subkoppen zullen de stappen worden doorlopen met een korte uitleg over wat er gebeurd in een stap.

4.2.1 Stap 1: Dataopname en versiebeheer (Data ingestion/versioning)

De eerste stap in de pipeline is het opnemen van data. Met deze data zal het model getraind, gevalideerd en getest worden. De dataset kan van een of meerdere bronnen komen, zoals lokaal, een online opslag locatie of van een database. Het dataset kan gekopieerd worden en op een plek worden opgeslagen waar alle datasets te vinden zijn. Zodra de data op een bereikbare plek is opgeslagen en ingeladen in, moet het verdeeld worden tussen een train-, validatie- en testdataset. Normaal gebeurt dit met een splitratio van 6:2:2. De train dataset is 60% en de validatie en testdatasets zijn

allebei 20% van de originele dataset [**building-machine-learning-pipelines-oreilly**].

Een use case van een pipeline is dat een nieuw model getraind kan worden door een geüpdatet dataset te gebruiken. Dit wordt gedaan door de voorgaande dataset te gebruiken, waarbij nieuwe data is toegevoegd. Door het gebruik van verschillende datasets is het verstandig om versiebeheer toe te passen. Zo is goed te zien welk dataset welke model produceert. Een versie geven aan een dataset gebeurt voordat de dataset wordt ingeladen [**building-machine-learning-pipelines-oreilly**]. Versiebeheer voor datasets kan bijvoorbeeld met DVC [**dvc**] of Pachyderm [**pachyderm**]. Beide zijn frameworks om bij te houden waar datasets zijn opgeslagen, welke versie het is en welk model het heeft geproduceerd.

4.2.2 Stap 2: Datavalidatie (Data validation)

Nu de dataset verdeeld is, een versie heeft en op een bereikbare plek is, kan de data gevalideerd worden. Deze stap is vooral belangrijk om te voorkomen dat een model wordt getraind dat niet nuttig is aangezien het trainen veel tijd in beslag kan nemen. Een bekende uitdrukking is "garbage in = garbage out". Dit betekent dat als de dataset niet goed is, het model ook niet goed zal presteren [**building-machine-learning-pipelines-oreilly**]. Tijdens de validatiestap wordt gecontroleerd op het volgende:

- Afwijkingen in de dataset
- Wijzigingen in de structuur
- Algemene statistieken in vergelijkingen met voorgaande datasets [**building-machine-learning-pipelines-oreilly**]

Bij het controleren van afwijkingen in de dataset wordt gekeken naar waarden die opmerkelijk zijn. Afwijkende waarden liggen te ver van het gemiddelde en kunnen een verkeerd beeld schetsen bij het trainen van het model. Deze uitschieters kunnen simpelweg uit de dataset gefilterd worden.

Het kan voorkomen dat bij een nieuwe dataset de type van waarden zijn gewijzigd. Een *int* kan bijvoorbeeld veranderd zijn in een *string* of *boolean*. Er is dan sprake van een wijziging in de structuur van de dataset. Dit is problematisch omdat er een vertaalstap gemaakt moet worden naar iets bruikbaars. Als dit niet mogelijk is moeten de waarden uitgefilterd worden wat de prestatie van het model negatief kan beïnvloeden.

De algemene statistieken is een hulpmiddel om te controleren op afwijkingen en wijzigingen. Vaak kan de controle in een oogopslag gedaan worden.

4.2.3 Stap 3: Data voorbereiden (Data preprocessing)

Het voorbereiden van de dataset is een stap dat de prestatie van het model verbetert en het proces van het trainen versneld. Deze stap kan verdeeld worden in twee substappen: het opschonen en het optimaliseren van de dataset.

Bij het opschonen worden bijvoorbeeld duplicaten of waarden die onbruikbaar zijn uit de dataset weggehaald. Onbruikbare waarden zijn waarden die simpelweg niet kloppen of verkeerd zijn ingevoerd. Hierbij kan bijvoorbeeld gedacht worden aan een medewerker die de interactietijd met een klant moet bijhouden, maar is vergeten om de eindtijd te noteren. Voor het algoritme zal het dan lijken alsof de medewerker een klant tot sluitingstijd heeft geholpen.

Datasets kunnen geoptimaliseerd worden om twee redenen: algoritmes werken sneller met waarden die dichter bij 0 liggen en algoritmes kunnen niet met elke waarde in de dataset omgaan. Om de efficiëntie van het algoritme te verbeteren kunnen een aantal technieken gebruikt worden:

- Schalen

Bij het schalen van data worden de waarden getransformeerd die liggen tussen een schaal, zoals tussen 0 en 100 of 0 en 1. Bij het schalen wordt het **bereik** getransformeerd [**scale-and-normalize-data**].

- Normaliseren

Als een dataset wordt gestandaardiseerd, worden de waarden getransformeerd in een standaard normale verdeling waarbij het gemiddelde 0 en de afwijking 1 is. Hierbij wordt de **vorm** van de dataset getransformeerd [**scale-and-normalize-data**]. Het normaliseren is belangrijk als het algoritme waarden vergelijkt met verschillende eenheden [**feature-scaling-standardization**]. In sommige gevallen is normalisering een vereiste bij een aantal algoritmes [**data-transformation-standardization-vs-normalization**].

- Categorische codering

Een groot aantal algoritmes kan alleen omgaan met numerieke waarden. Het kan voorkomen dat datasets categorische waarden bevatten. Dit zijn waarden die een label voorstellen, zoals *first*, *second* of *third*. Om deze waarden te gebruiken moeten ze worden gecodeerd als een numerieke waarde. De label kan bijvoorbeeld als de waarde 1, 2 of 3 gecodeerd worden. Deze techniek heet label encoding of integer encoding en kan gebruikt worden als de volgorde van de codering klopt. De bovenstaande labels zullen als volgt gecodeerd worden:

Categorical label	Encoded
<i>first</i>	1
<i>second</i>	2
<i>third</i>	3

Een andere techniek om waarden te coderen heet hot encoding. Deze techniek wordt gebruikt waarbij de labels geen relatie met elkaar hebben en maakt gebruik van meerdere waarden om een label te beschrijven:

Animal	C1	C2	C3
<i>cat</i>	1	0	0
<i>dog</i>	0	1	0
<i>mouse</i>	0	0	1

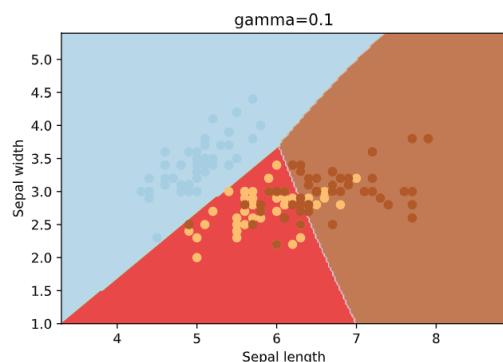
Dit is een goed moment om de getransformeerde dataset op te slaan als "tussen-dataset" zodat deze stap niet herhaald hoeft te worden. Het voorbereiden van grote datasets kan een grote hoeveelheid tijd in beslag nemen.

4.2.4 Stap 4 en 5: Model trainen en tunen (Model training and Model tuning)

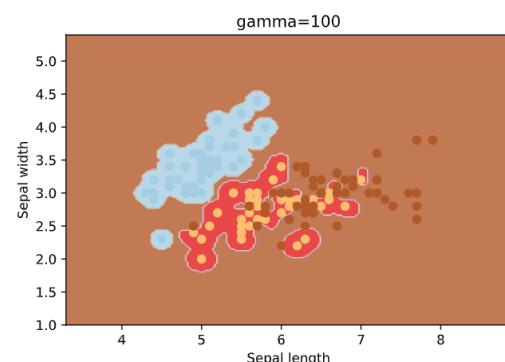
Na het valideren en voorbereiden van de dataset kan het model getraind worden. Het trainen gaat door middel van een ML algoritme. Een ML algoritme is vergelijkbaar met een conventioneel algoritme in software engineering zoals bijvoorbeeld binary search, merge sort en depth first search. Het algoritme slaat na het trainen met de dataset regels, nummers en algoritme specifieke datastructuren op in de vorm van een model. Het algoritme kan worden gezien als een specifiek programma waarmee, gegeven een input, voorspellingen mee gedaan kunnen worden [**ml-algorithm-model-difference**].

Elk algoritme heeft variabelen om er voor te zorgen dat het algoritme beter aansluit op de dataset. Deze variabelen heten *hyperparameters*. Het algoritme heeft standaard hyperparameters die niet altijd de optimale prestatie behalen. Op een heuristische wijze kunnen de optimale hyperparameters gevonden worden [**ml-model-hyper-parameter-brownlee**]. Dit proces heet *tunen*.

In Figuur 4.3 en Figuur 4.4 is te zien hoe de *gamma* hyperparameter van een support vector classification (SVC) algoritme invloed heeft op het model. Dit algoritme classificeert op basis van gegeven waarden. De waarden worden geplot en zal binnen een van de drie kleuren vallen. Het model met als hyperparameter waarde 100 zal vaker de classificatie met de bruine kleur als voorspelling geven dan als de waarde 0.1 zou zijn.



Figuur 4.3: Gamma hyperparameter van een support vector classification (SVC) algoritme met waarde 0.1



Figuur 4.4: Gamma hyperparameter van een support vector classification (SVC) algoritme met waarde 100

In het ML domein bestaan talloze algoritmes om voorspellingen te maken. In de [BIJLAGE LINK] is een mind-map te vinden van de algoritmes die gedurende de scriptie naar voren zijn gekomen. De algoritmes kunnen grotendeels gegroepeerd worden in vier stijlen: supervised, unsupervised, semi-supervised en reinforcement learning. In de [BIJLAGE LINK] is meer informatie over de stijlen te vinden.

4.2.5 Stap 6 en 7: Modelanalyse en -validatie (Model analysis and Model validation)

Na het trainen en tunen kan analyse en validatie plaatsvinden. Bij het analyseren wordt de prestatie van het model vergeleken met voorgaande modellen. Om dit te doen kunnen, net

als in deelparagraaf 4.2.2, statistieken gegenereerd worden van het model. De soort statistiek hangt af van wat voor soort algoritme is gebruikt. Een classificatie-algoritme heeft bijvoorbeeld andere statistieken dan een regressie-algoritme. Op basis van de uitkomst kunnen de dataset of hyperparameters aangepast worden om de accuraatheid te verhogen.

Met de validatie van een model moet er gekeken worden met een genuanceerd perspectief. Validatie gaat namelijk over hoe eerlijk een model is als er gekeken wordt naar een bepaalde groep. Een groep kan gedefinieerd worden als geslacht, etniciteit, locatie of leeftijd. Het kan namelijk voorkomen dat de dataset voornamelijk bestaat uit bijvoorbeeld vrouwen. Dit *kan* ervoor zorgen dat het model minder accurate voorspellingen maakt voor mannen [**introduction-to-machine-learning**]. Een voorbeeld waar het gebruik van ML grote negatieve gevolgen had was de toeslagenaffaire in 2020. De Nederlandse overheid maakte gebruik van een systeem dat aangaf of een burger mogelijk bijstandsfraude had gepleegd. Het systeem maakte gebruik van ML om fraude aan te geven. Jaren na het gebruik bleek dat er sprake was van etnische profilering. De dataset bestond voornamelijk uit immigranten uit Islamitische landen. Het systeem heeft hierdoor een *bias* [**ml-fairness-dutch-syri**].

4.2.6 Stap 8: Model uitrollen (Model deployment)

Na het analyseren en valideren kan het model uitgerold worden. Het uitrollen kan op twee manieren: inbakken in een app of serveren met een application programming interface (API).

Met het inbakken in een app wordt bedoelt dat het model meegenomen wordt als de app gebouwd wordt. Voordelen van deze methode is dat het model offline bruikbaar is en de rekenkracht van het apparaat gebruikt kan worden om te voorspellen of classificeren. Een nadeel is dat het model niet makkelijk geüpdatet kan worden.

De andere optie is om het model te serveren door middel van een API. De app die het model wilt gebruiken zal een request moeten doen met input. De API geeft de input door aan het model. Het model geeft een predictie terug dat de API doorstuurt naar de applicatie. Het updaten van het model gaat gemakkelijker dan het model inbakken met een app. Een nadeel is de eis dat de app een internetverbinding moet hebben om het model te gebruiken [**introduction-to-machine-learning**].

In Figuur 4.5 is te zien hoe een model geserveerd wordt via een API. Een endpoint genaamd "classify" is gedefinieerd waarop een *POST* request gedaan kan worden. De endpoint haalt de input uit de request en geeft het door aan het model. De model maakt vervolgens een predictie dat uiteindelijk naar de app teruggestuurd wordt.

4.2.7 Stap 9: Feedbackloop (Model feedback)

Om het model continue te verbeteren kan feedback verzameld worden. De feedback geeft een beeld van de effectiviteit van het model in een productieomgeving. Feedback kan verdeeld worden in twee soorten: impliciet en expliciet [**introduction-to-machine-learning**].

Het verzamelen van impliciete feedback wordt gedaan zonder dat de gebruiker zich daar bewust van is. Dit wordt gedaan door bij te houden of een voorspelling correct was volgens een gebruiker. Een voorbeeld van deze methode is het bijhouden of een gebruiker een video kijkt dat door het algoritme voorgesteld is. Als een gebruiker de voorgestelde video bekijkt, wordt dit gezien als

```

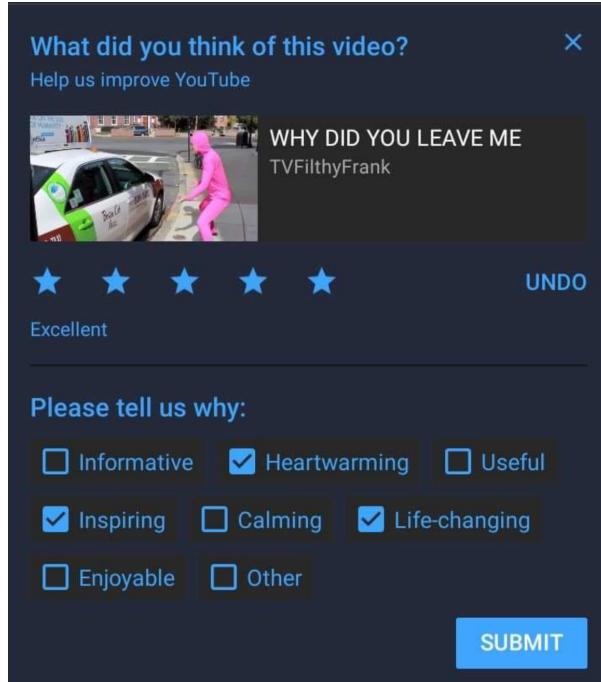
1 @app.route("/classify", methods=["POST"])
2 def classify():
3     # Get input from request
4     json = request.get_json()
5     data = json["data"]
6
7     # Get prediction from model
8     classification = model.predict([data])
9
10    # Return prediction to app
11    return jsonify({ "family": classification[0] })

```

Figuur 4.5: Model uitgerold met behulp van een API.

een succesvolle voorspellen. Mocht de gebruiker niet een voorgestelde video bekijken, wordt dit gezien als onsuccesvol.

In tegenstelling tot impliciet wordt bij expliciete feedback gevraagd aan de gebruiker of een voorspelling gepast is. Een voorbeeld van deze vorm in de praktijk is hoe YouTube expliciete feedback vraagt (Figuur 4.6). Naast het aangeven of de voorspelling gepast was, kan de gebruiker ook aangeven waarom de video gepast was.



Figuur 4.6: Vorm van expliciete feedback gebruikt door YouTube.

Het verzamelen van feedback is niet noodzakelijk maar helpt met het verbeteren van het model. Deze output van deze stap gaat samen met een nieuwe dataset naar de eerste stap in de lifecycle

(Figuur 4.2). Met de nieuwe dataset en de feedback kan een nieuw model getraind worden dat beter presteert dan de voorganger.

4.3 Conclusie

In dit hoofdstuk is er onderzoek gedaan naar het antwoord op de deelvraag: **D1: Waar bestaat een machine learning pipeline uit?** Het onderzoek is uitgevoerd met behulp van zowel digitale bronnen, een boek en een experiment.

Een ML pipeline bestaat uit verschillende stappen die op hun beurt bestaan uit acties. De stappen zijn gericht op het waarborgen van de kwaliteit van de dataset en model, het voorbereiden van de dataset en het trainen van het model. Daarnaast kan het model uitgerold worden in een productieomgeving en kan er feedback verzameld worden over de prestatie van het model volgens gebruikers.

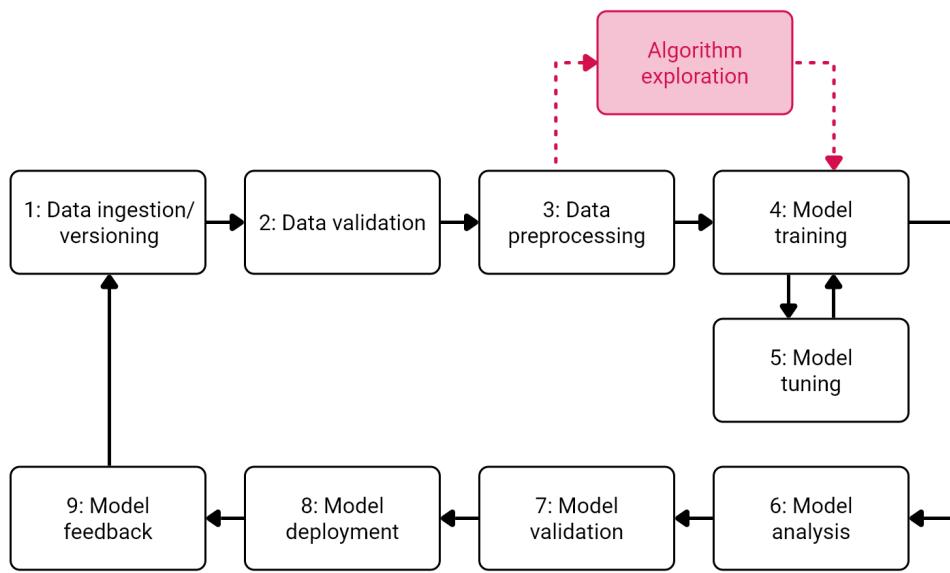
De acties in de stappen moeten bij het eerste gebruik van de pipeline gedefinieerd worden. De acties kunnen bijvoorbeeld het filteren van onbruikbare data, een model trainen of statistieken genereren zijn. Als dit vast staat, kan de pipeline hergebruikt worden om nieuwe modellen te trainen met nieuwe datasets. Op deze manier is een ML pipeline een gestructureerde en reproduceerbaar proces.

4.4 Advies

Het in gebruik nemen van een ML pipeline werkwijze is initieel ingewikkeld, maar lonend op de lange termijn. Het opzetten van de pipeline en de acties definiëren kost tijd en kennis. Echter als dit eenmaal gedaan is, kan eenvoudig een verbeterd model worden getraind door een nieuwe dataset aan te leveren. Een verbeterd model is vrijwel gegarandeerd omdat de stappen in de ML pipeline de dataset en het model analyseren en valideren.

4.4.1 Een betere keuze maken tussen machine learning algoritmes

Zoals eerder aangegeven in paragraaf 4.1 bestaat er niet één ML pipeline dat correct is. Een ML pipeline is een werkwijze waarbij de stappen anders geïnterpreteerd kunnen worden. Hierdoor is er geen regelmaat tussen verschillende pipelines. Een pipeline kan stappen of acties weglaten of extra hebben. Overeenkomst tussen pipeline is ook niet haalbaar aangezien stappen gemaakt kunnen worden die specifiek zijn voor het algoritme of workflow van het bedrijf. De stappen in de pipeline van Hapke en Nelson (Figuur 4.2) is een valide basis, maar kan uitgebreid worden om de ervaring van developers te verbeteren. In stap 4 en 5 (deelparagraaf 4.2.4) wordt een model getraind waarbij het beste algoritme om het ML probleem op te lossen al bekend is. De verwachting is dat de keuze/onderzoek vóór het starten van de pipeline is gedaan. Tussen stap 3 en 4 kan echter een stap tussen zitten om te experimenteren met een combinatie van verschillende algoritmes en hyperparameters. In Figuur 4.7 is te zien hoe zo een stap zou passen in de lifecycle. De stap is met een stippeellijn aangegeven omdat de stap de eerste keer meegenomen kan worden als de pipeline wordt doorlopen. Na de eerste keer zijn de beste algoritme en hyperparameters al bekend en kan deze stap overgeslagen worden.

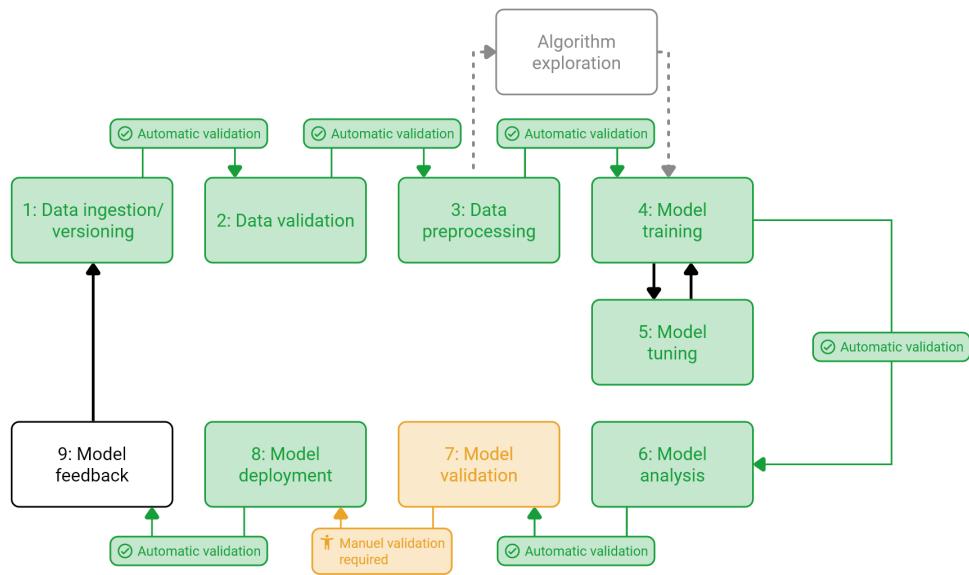


Figuur 4.7: Machine learning pipeline met een algoritme exploratie tussenstap.

In de "Algorithm exploration" stap kunnen verschillende algoritmes die hetzelfde doel bereiken en een variatie van hyperparameters voor elk algoritme getest worden tegen de dataset. Uit deze tests kan een prestatiescore gegenereerd worden om vervolgens te kiezen voor het algoritme dat het meest geschikt lijkt. Na de keuze kan de pipeline verder gaan met de volgende stappen.

4.4.2 Machine learning versimpelen

Een van de focuspunten is om te onderzoeken in hoeverre ML te vergemakkelijken is voor developers. Met de huidige pipeline is er vrij veel kennis vereist over ML om ermee te werken. Toch kan een groot deel van de stappen geautomatiseerd worden. Tussen elke stap kan een validatie plaatsvinden met een aantal randvoorwaarden waaraan voldaan moeten worden om door te gaan naar de volgende stap. In Figuur 4.8 is te zien hoe tussen elke stap een validatie plaats vindt. Om bijvoorbeeld van stap 6 (Model analysis) naar stap 7 (Model validation) te gaan, moet het model even goed of zelfs beter presteren dan de voorganger. Hoe veel beter het model moet kunnen presteren is aan een developer. Mocht het zo zijn dat het model niet voldoet, kan de pipeline stopgezet worden.



Figuur 4.8: Machine learning pipeline waarbij stappen geautomatiseerd kunnen worden voor het gemak van developers.

Niet alle aspecten van de pipeline kunnen versimpeld worden. Een van de stappen die niet kan is stap 7 (Model validation) in Figuur 4.8. Deze stap vereist input van een mens aangezien de bias van het model wordt beoordeeld. Wel kunnen rapporten over de bias gegenereerd worden zodat de workflow van developers gestroomlijnd wordt.

5 Orkestratietools om platformen te beheren

Om resources in een cloud platform te beheren kan gebruik gemaakt worden van een portal. In een portal kunnen databases, servers en netwerken aangemaakt worden om een infrastructuur te creëren. Omdat een portal uitgebreid en complex is, moet de developer een infrastructuur kunnen opzetten zonder het gebruik van een portal. Dit is mogelijk met infrastructure as code (IaC) orkestratietools. IaC zal als eerst worden uitgelegd. Vervolgens worden verschillende IaC orkestratietools met elkaar vergeleken. Als laatst wordt een experiment uitgevoerd om de haalbaarheid met een orkestratietool te valideren.

5.1 Wat is infrastructure as code?

IaC is een manier om een infrastructuur op te zetten binnen een cloud platform zonder gebruik te maken van een interface zoals een portal. De gewenste infrastructuur wordt beschreven waarna de orkestratietool de gewenste situatie een realiteit probeert te maken [[iac-amazon-web-services-in-action](#)].

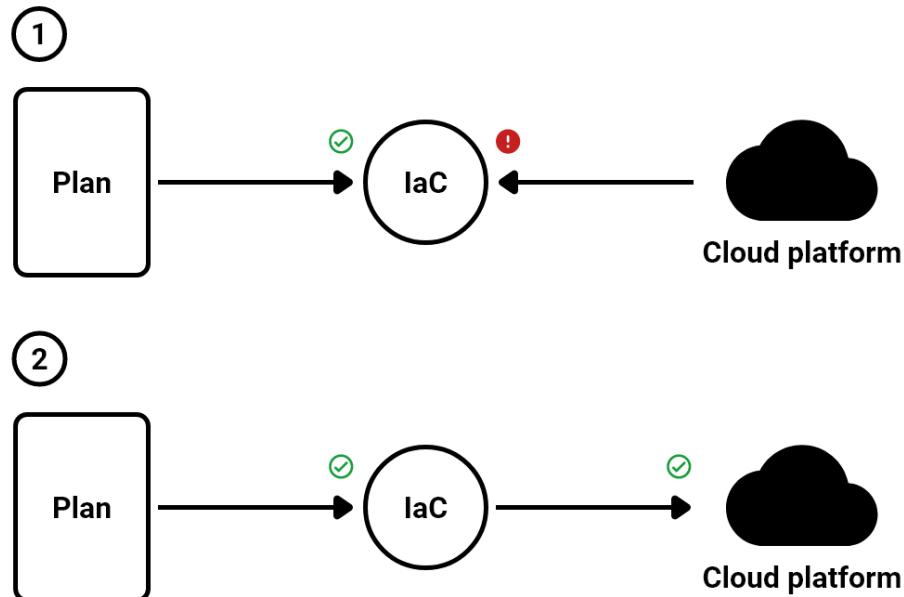
De manier waarmee een orkestratietool de infrastructuur aanmaakt, wijzigt of verwijderen is met een plan. In het plan staat welke resources moeten bestaan om aan de gewenste situatie te voldoen. Vaak gaat dit gepaard met configuratie zoals een naam, locatie of tags. In Figuur 5.1 is een voorbeeld van een plan als YAML bestand te zien. YAML is een bestandstype dat vaak wordt gebruikt voor configuratie. Het plan beschrijft op welke cloud platform dit uitgevoerd moet worden (lijn 12) en wat er aangemaakt moet worden. In dit geval is het een resource group (lijn 16) met als configuratie een naam (*myTFResourceGroup*) en locatie (*westus2*).

```
1 terraform {  
2   required_providers {  
3     azurerm = {  
4       source  = "hashicorp/azurerm"  
5       version = "> 2.26"  
6     }  
7   }  
8  
9   required_version = "> 0.14.9"  
10 }  
11  
12 provider "azurerm" {  
13   features {}  
14 }  
15  
16 resource "azurerm_resource_group" "rg" {  
17   name      = "myTFResourceGroup"  
18   location  = "westus2"  
19 }
```

Figuur 5.1: Voorbeeld van een infrastructure as code (IaC) plan [[terraform-plan-example](#)].

Een IaC volgt een proces om aan de gewenste situatie te voldoen. In Figuur 5.2 is te zien hoe een proces verloopt. Zodra de orkestratietool wordt gestart, wordt zowel het plan als de situatie in de cloud platform gecontroleerd en met elkaar vergeleken. In stap 1 is het plan valide, maar de situatie in de cloud platform niet. Dit betekent bijvoorbeeld dat er in het plan staat dat er een resource group moet bestaan met een naam en locatie zoals het beschreven staat in Figuur 5.1, maar dit niet bestaat in de cloud platform. In de volgende stap wordt de resource aangemaakt

door de IaC om aan de gewenste situatie te voldoen. De wijzigingen gebeuren programmatisch en wordt gedaan door de IaC. Er is geen tussenkomst van een persoon of interface nodig.



Figuur 5.2: Proces van een infrastructure as code (IaC) om aan de gewenste situatie te voldoen.

5.2 Orkestratietools vergeleken met elkaar

Om een keuze te maken met welke IaC orkestratietool verder gewerkt zal worden moet er een keuze gemaakt worden. Om de opties te beperken kan zogenoemde "knockout" criteria opgesteld worden. Dit betekent dat een IaC orkestratietool niet wordt meegenomen in de keuze als de tool niet voldoet aan alle criteria. In Tabel 5.1 zijn de knockout criteria te vinden. De criteria in samenwerking met NGTI opgesteld.

Criteria	Toelichting
Programmatisch beheren	Het orkestratietool moet via code een resources kunnen aanmaken, wijzigen en verwijderen.
Ondersteuning voor cloud computing platformen	Om platform-agnostisch te zijn moet de orkestratietool minstens twee cloud computing platformen ondersteunen waarop een ML model getraind kan worden.
Uitgebreide documentatie	De documentatie moet toegankelijk en duidelijk zijn. De documentatie moet tutorials, concepten en een reference bevatten.

Tabel 5.1: Knock-out criteria voor orkestratietools dat cloud computing platformen beheert.

Voor de keuzes uit de tools is onderzoek gedaan op het internet en een enquête geraadpleegd van Stack Overflow [stack-overflow-survey-2020]. De enquête is ingevuld door developers en bevat vragen over de ervaring met frameworks, technologieën en de website zelf. Uit de vraag over welke frameworks, libraries en tools het meest gebruikt werkt, kwam Ansible, Terraform, Puppet en Chef naar boven [stack-overflow-survey-2020-popular-framework-libraries-tools]. Volgens een vraag over de meest geliefd en gevreesde frameworks, libraries en tools zijn Ansible en Terraform het meest geliefd en Puppet en Chef het meest gevreesd [stack-overflow-survey-2020-loved-dreaded]. Uit het onderzoek naar orkestratietools is, naast de bovengenoemde tools, Pulumi naar voren gekomen als kandidaat [pulumi]. Ansible, Terraform en Pulumi zijn in Tabel 5.2 tegen de knockout criteria gehouden.

Orkestratie-tools	Programmatisch beheren	Ondersteuning voor cloud computing platformen	Uitgebreide documentatie
Ansible	Nee, orkestratie gaat via een YAML bestand [ansible-code]	AWS, Google Cloud en Azure. 11 platformen in totaal [ansible-cloud-platforms]	Uitgebreide documentatie met tutorials, references en migration [ansible-docs]
Pulumi	Ja, orkestratie via CLI of TypeScript, JavaScript, Python, .NET en Go [pulumi-code]	AWS, Google Cloud en Azure. 13 platformen in totaal [pulumi-cloud-platforms]	Uitgebreide documentatie met tutorials en references [pulumi-docs]
Terraform	Nee, orkestratie gaat via een YAML bestand [terraform-code]	AWS, Google Cloud en Azure. 5 platformen in totaal [terraform-cloud-platforms]	Uitgebreide documentatie met tutorials, references en videos [terraform-docs]

Tabel 5.2: Knock-out criteria tegen orkestratietools dat cloud computing platformen beheert.

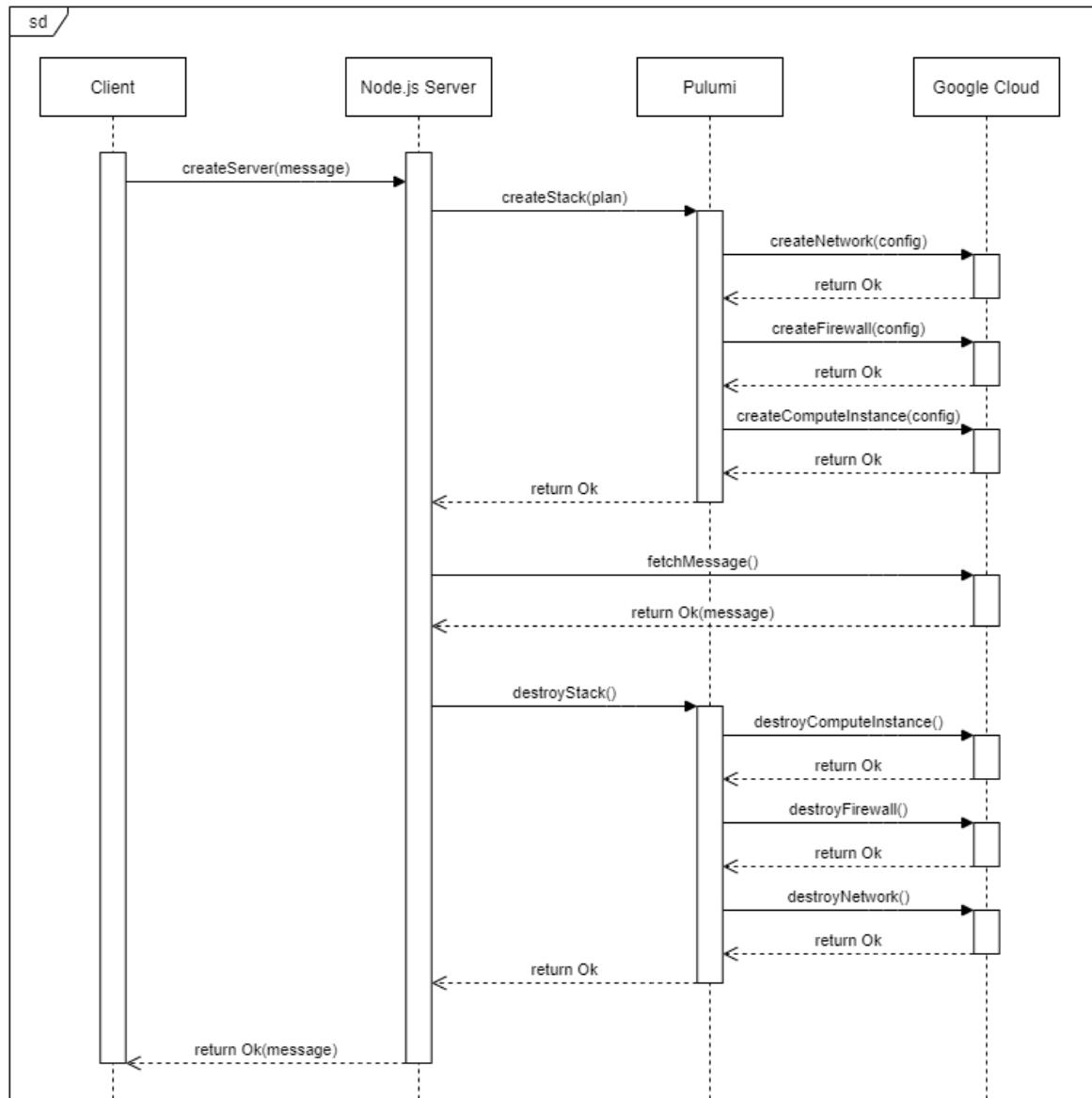
In Tabel 5.2 is te zien dat de drie orkestratietools gelijk zijn als het gaat om de ondersteuning van cloud platform en documentatie. Programmatisch beheren kan met Ansible en Terraform alleen door middel van een YAML bestand in tegenstelling met Pulumi dat via code een plan kan uitvoeren. Omdat het praktischer voor de PoC om via code een plan uit te voeren, is er voor gekozen om met Pulumi verder te werken. In het volgende hoofdstuk zal een experiment met Pulumi uitgevoerd worden om te valideren of Pulumi geschikt is.

5.3 Experiment met de orkestratietool Pulumi

Het idee achter het experiment is om te achterhalen of Pulumi een geschikte orkestratietool is. Op dit moment in het afstudeerproces wordt er verwacht dat de PoC een frontend krijgt dat praat door middel van een representational state transfer (REST) API met een backend. De backend zal vervolgens gebruik maken van de orkestratietool om te praten met een cloud platform. Om het PoC na te bootsen op kleinere schaal wordt er bij het experiment gebruik gemaakt van een client waarbij een opdracht met behulp van een REST API naar een Node.js server wordt verstuurt. De Node.js server stuurt om zijn beurt opdrachten naar Pulumi die communiceert

met Google Cloud. Voor het experiment is arbitrair gekozen voor het cloud platform.

Het experiment is als sequence diagram uitgewerkt in Figuur 5.3. Hierin is goed te zien welke acties gedaan worden en door welke speler.



Figuur 5.3: Sequence diagram van het experiment met orkestratietool Pulumi

In Figuur 5.3 is ook te zien wat voor taak wordt uitgevoerd aan de hand van de naam tussen de spelers. Deze taken zullen in de volgende code snippets verduidelijkt worden. De Node.js server is vrij simpel en bevat één endpoint op lijn 12 genaamd /api/run-python-code (Figuur 5.4).

```
1 import express, { response } from 'express'
2 import fetch from 'node-fetch'
3 import { compute } from '@pulumi/gcp'
4 import { LocalWorkspace } from "@pulumi/pulumi/automation"
5
6 const app = express()
7 const port = 8080
8
9 app.use(express.json())
10 app.use(express.urlencoded({ extended: true }))
11
12 app.post("/api/run-python-code", async (req, res) => { ... })
13
14 app.listen(port, () => {
15   console.log(`server started at http://localhost:${port}`)
16 })
```

Figuur 5.4: Node.js server voor het experiment met orkestratietool Pulumi

In deze *POST* endpoint wordt een stack aangemaakt, een *GET* request uitgevoerd naar de aangemaakte compute instance en vervolgens wordt de stack weer verwijderd. Een stack is de manier hoe Pulumi een plan beschrijft. In de stack worden drie resources aangemaakt: een network, een firewall en een compute instance (Figuur 5.5). De compute instance moet een HTML bestand serveren met een bericht dat de client heeft gespecificeerd.

```
1 const CreateResource = (message: string) => async () => {
2   // Create a network
3   const computeNetwork = new compute.Network("network", {
4     // Configuration
5   })
6
7   // Create a firewall in the network
8   const computeFirewall = new compute.Firewall("firewall", {
9     // Configuration
10  })
11
12  // Define script that runs when the compute instance runs
13  const startupScript = `#!/bin/bash
14 echo "${message}" > index.html
15 nohup python -m SimpleHTTPServer 80 &
16
17  // Create a compute instance that runs startupScript
18  const computeInstance = new compute.Instance("instance", {
19    // Configuration
20  }, { dependsOn: [computeFirewall] })
21
22  const ip = computeInstance.networkInterfaces.apply(ni => ni[0].accessConfigs![0].natIp);
23
24  return { name: computeInstance.name, ip: ip }
25 }
```

Figuur 5.5: De stack voor het experiment

Elke resource heeft zijn eigen configuratie om ervoor te zorgen dat de HTML bestand beschikbaar

is voor de buitenwereld. De code met de configuratie is te vinden in [BIJLAGE LINK].

In Figuur 5.6 is te zien wat er in de POST endpoint gebeurd. Als eerst wordt een stack in geheugen aangemaakt met behulp van de code in Figuur 5.5. Na het aanmaken wordt de stack uitgevoerd met de *stack.up()* functie op lijn 12. Nadat de stack is aangemaakt in Google Cloud wordt de een *GET* request uitgevoerd naar de server op lijn 15. Nadat de request voltooid is wordt de stack verwijderd uit Google Cloud (lijn 21) met *stack.destroy()* en wordt het bericht teruggestuurd naar de client.

```
1 app.post("/api/run-python-code", async (req, res) => {
2   const stackName = 'mlpa-py'
3   const projectName = 'disco-sky-312109'
4
5   const stack = await LocalWorkspace.createOrSelectStack({
6     stackName,
7     projectName,
8     program: CreateResource(req.body.message)
9   })
10
11 // Comparing stack against Google Cloud
12 const upRes = await stack.up({ onOutput: console.info })
13
14 // Fetch HTML file with message
15 const action_response = await fetch(`http://${upRes.outputs.ip.value}`)
16   .then(async r => await r.text())
17   .then(t => t)
18   .catch(e => console.log(e))
19
20 // Destroying stack in Google Cloud
21 await stack.destroy({ onOutput: console.info })
22
23 res.send({ returned_response: action_response })
24 })
```

Figuur 5.6: POST endpoint van de Pulumi experiment

5.4 Conclusie

In dit hoofdstuk is er onderzoek gedaan naar het antwoord op de deelvraag: **D2: Hoe kan een orkestratietool verschillende cloud computing platformen beheren om een machine learning pipeline op te zetten?** Het onderzoek is uitgevoerd met behulp van digitale bronnen en een experiment.

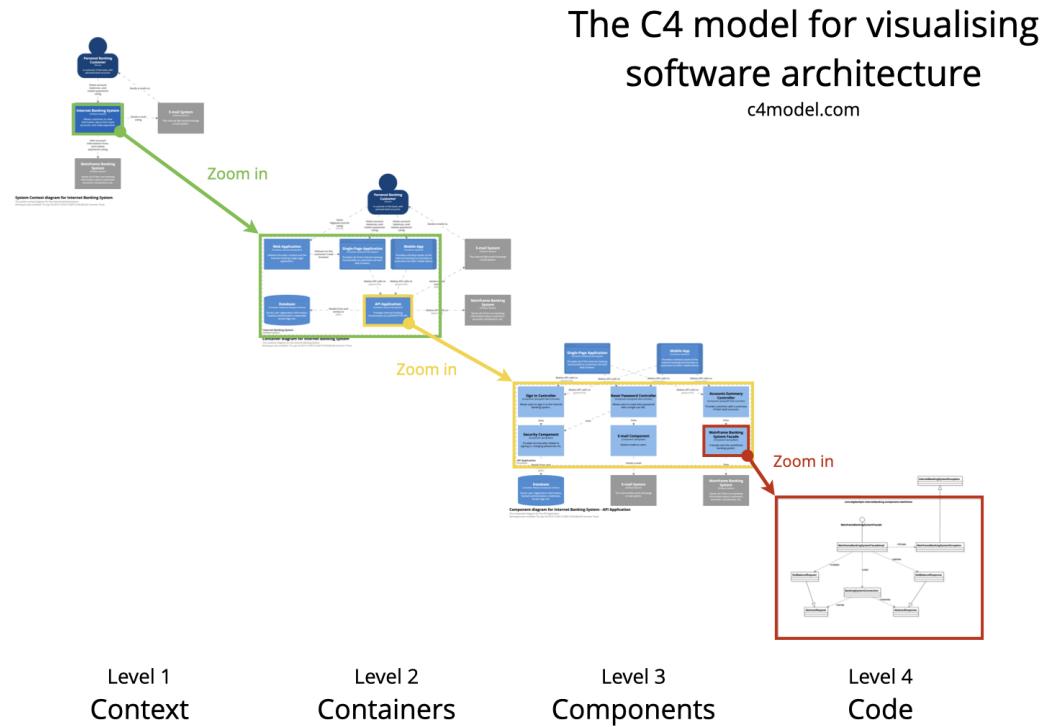
Een orkestratietool is een manier om resources aan te maken, aan te passen en te verwijderen. De tool doet dit zonder het gebruik van een online portal of interventie van een developer. Het managen van resources wordt gedaan op basis van een plan en de huidige situatie binnen de cloud platform. In het plan staat welke resources moeten bestaan en met welke configuratie. Het plan kan beschreven worden in een YAML bestand of door middel van code. De orkestratietool vergelijkt vervolgens het plan met de huidige situatie en zorgt ervoor dat de situatie voldoet aan het plan.

6 Architecturale ontwerp van de oplossing

Nu het bekend is hoe ML pipelines en orkestratietools werken, kan er gekeken worden naar hoe de PoC architecturaal eruit gaat zien. De technische tekeningen laten zien hoe verschillende componenten in de PoC interacteert met elkaar en met componenten buiten de scope van de PoC. De tekeningen zijn gemaakt volgens het C4 model [**c4-model**]. In dit hoofdstuk zal worden uitgelegd hoe C4 gelezen moet worden waarna de technische tekeningen wordt uitgelegd.

6.1 Het C4 model

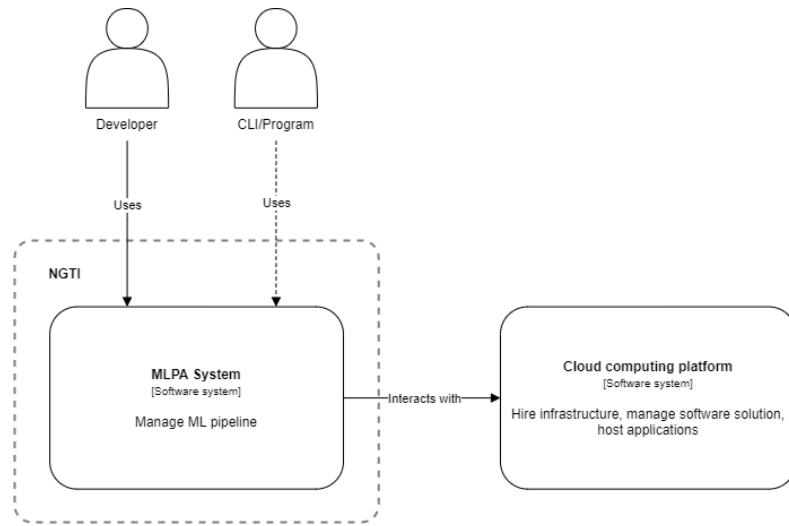
Het C4 model is een notatietechniek om de architectuur van een systeem te communiceren en is bedacht door Simon Brown [**c4-model**]. Bij het tekenen van de modellen wordt er gedacht in vier niveaus: context, containers, components en code. In Figuur 6.1 is een voorbeeld van een C4 model te zien. De context level is het eerste niveau waarbij wordt gekeken naar het systeem, gebruikers en contexten buiten de scope. Het systeem binnen de scope kan uitgebreid worden door middel van de volgende niveau, containers. Dit niveau laat op een hoog niveau zien waar het systeem uit bestaat. Elk container kan verder verduidelijkt worden met het component niveau. Hierbij worden containers verder opgebroken in components. Het laatste niveau is de code niveau en wordt doorgaans weergegeven via een klassendiagram.



Figuur 6.1: Voorbeeld van een C4 model [**c4-model**].

6.2 Architecturaal ontwerp

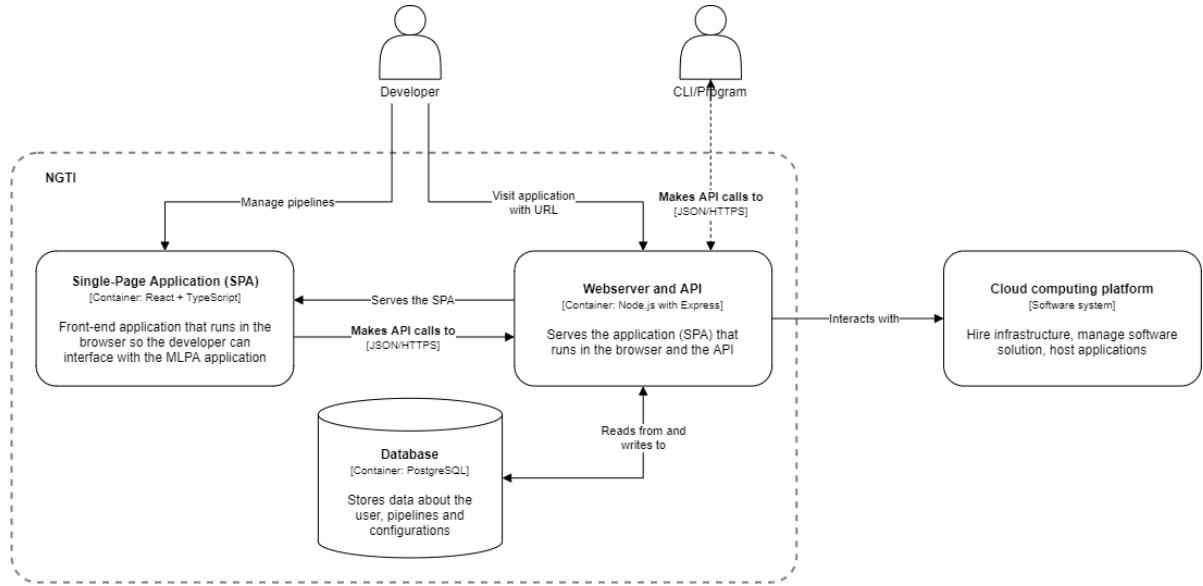
Op context niveau is het vrij simpel met het machine learning pipeline automation (MLPA) systeem binnen de scope waarmee een developer interacteert en cloud computing platformen die buiten de scope vallen (Figuur 6.2). In deze diagram is ook te zien dat developers alleen gebruik maken van het systeem en indirect van cloud platformen. In de context diagram is ook een command line interface (CLI)/program te zien dat gebruik kan maken van de MLPA systeem. Deze valt echter buiten de scope en is daarom aangegeven met een stippellijn.



Figuur 6.2: Context niveau diagram van het architecturaal ontwerp.

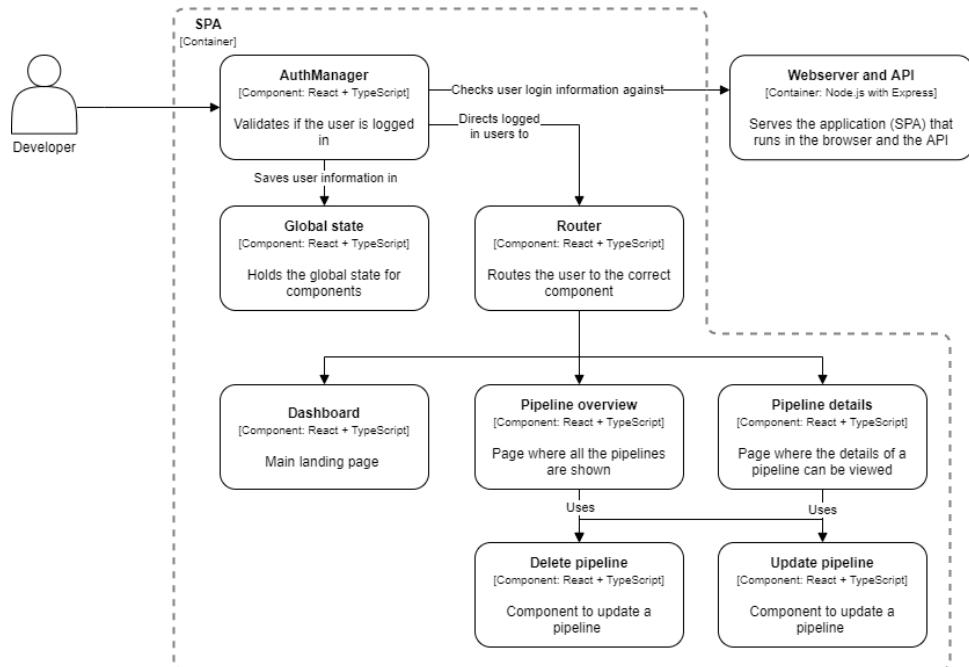
In Figuur 6.3 is de container niveau van het MLPA systeem te zien. Het systeem bestaat uit een single page application (SPA) frontend, een Node.js met Express backend en een PostgreSQL database. Een developer krijgt van de backend de SPA geserveerd waarmee waarmee een pipeline beheert kan worden. De frontend stuurt API requests naar de backend die vervolgens interacteert met de database en cloud platformen.

Voor de keuze van frameworks is rekening gehouden met de populariteit en kwaliteit van documentatie. Voor de populariteit is nogmaals de enquête van Stack Overflow geraadpleegd [[stack-overflow-survey-2020](#)]. Volgens de resultaten scoren zowel React.js, Node.js en Express hoog [[stack-overflow-survey-2020-technology-web-frameworks](#)] [[stack-overflow-survey-2020-popularity](#)]. Daarnaast hebben alle drie frameworks robuuste documentatie met references en tutorials [[reactjs-docs](#)] [[nodejs-docs](#)] [[expressjs-docs](#)].



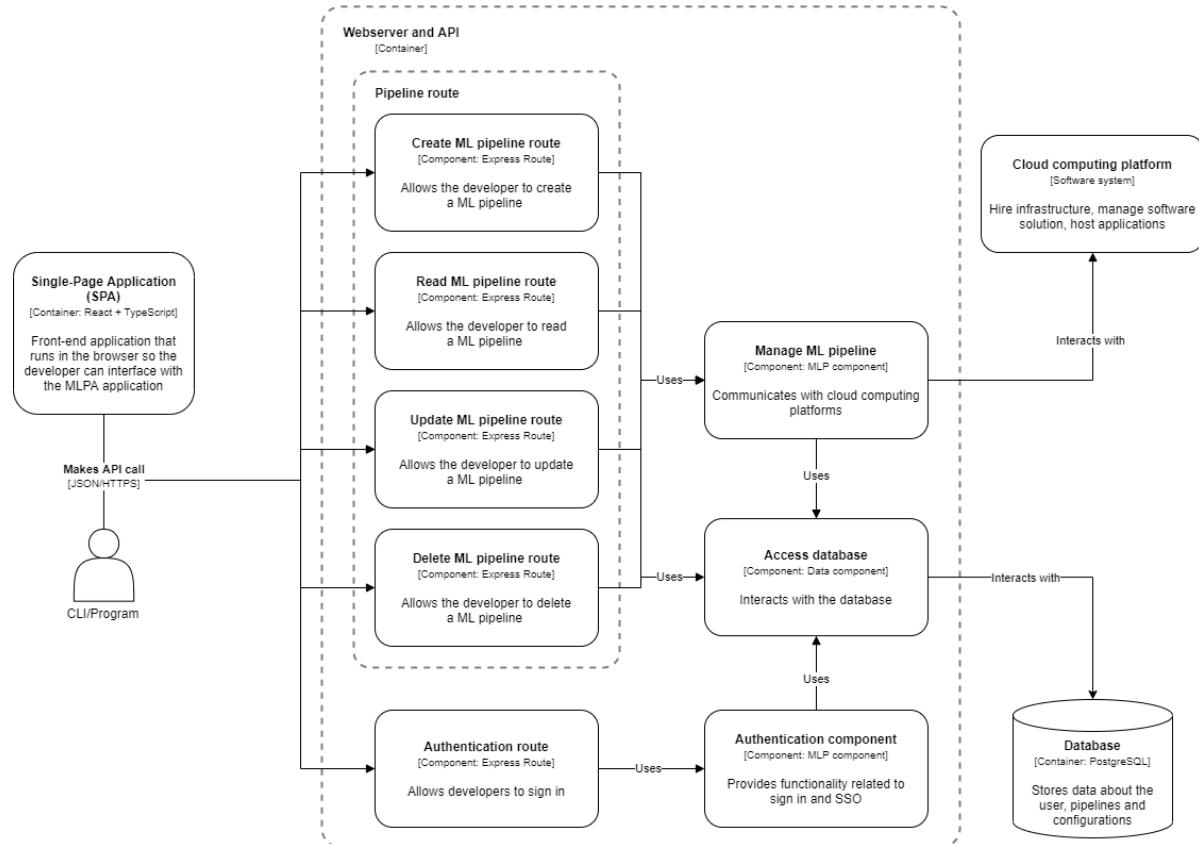
Figuur 6.3: Container niveau diagram van het architecturaal ontwerp.

Als laatste is de component overview van de SPA te zien in Figuur 6.4 en van de webserver met API in Figuur 6.5. De SPA bevat een *AuthManager* component dat controleert of de developer is ingelogd. Als dat het geval is, stuurt de *Router* component de developer door naar de *Dashboard*, *Pipelineoverview* of *Pipelinedetails* pagina.



Figuur 6.4: Single page application (SPA) component niveau diagram van het architecturaal ontwerp.

De component diagram van het MLPA systeem bevat het complexe gedeelte (Figuur 6.5). Hier komt een API request binnen in een *ExpressRoute*. De route maakt vervolgens gebruik van Pulumi en het database om taken uit te voeren zoals het starten van een pipeline, het uploaden van een dataset of de status van een run bekijken.



Figuur 6.5: Node.js server component niveau diagram van het architecturaal ontwerp.

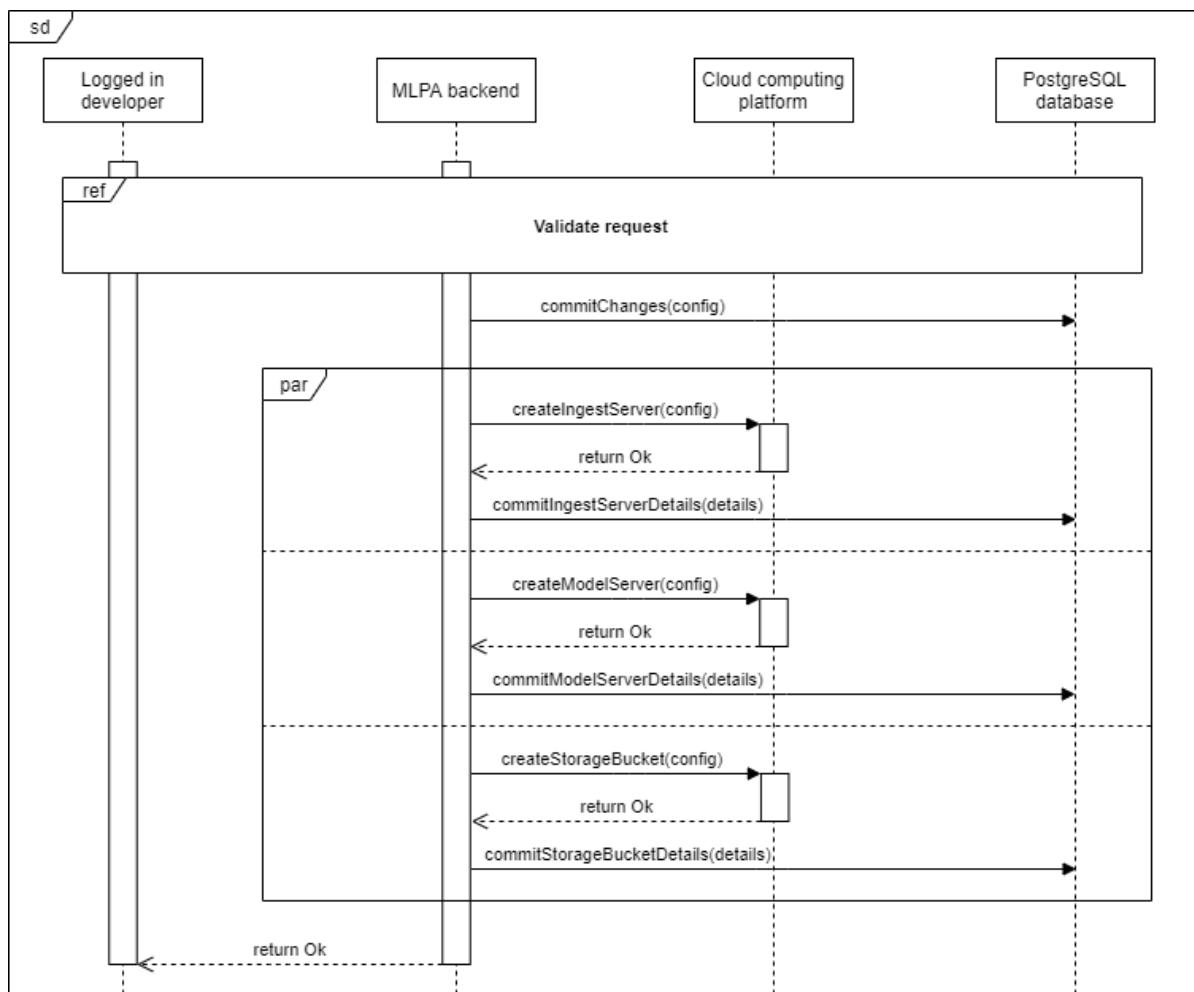
De architectuur van de Node.js applicatie is ontworpen met de separation of concerns principe en de single responsibility, open-closed, liskov substitution, interface segregation and dependency inversion (SOLID) principe in gedachte [**dijkstra-separation-of-concerns**] [**solid-principle**]. Dit betekent dat functies zoals het ophalen van pipeline-details opgebroken is kleinere functies. De functies bekommeren zich alleen om een functionaliteit. in [SUBKOP LINK] zal dit uitgelegd worden met voorbeelden.

Diagrammen voor de laatste niveau, code, zijn achterwege gelaten door de vereiste tijd om de diagrammen te maken en het feit dat de diagrammen vaak tijdens het programmeerproces zullen veranderen. Brown geeft ook als advies om de diagrammen niet te maken of automatisch te laten genereren [**c4-model-faq**].

6.3 Sequence diagrammen

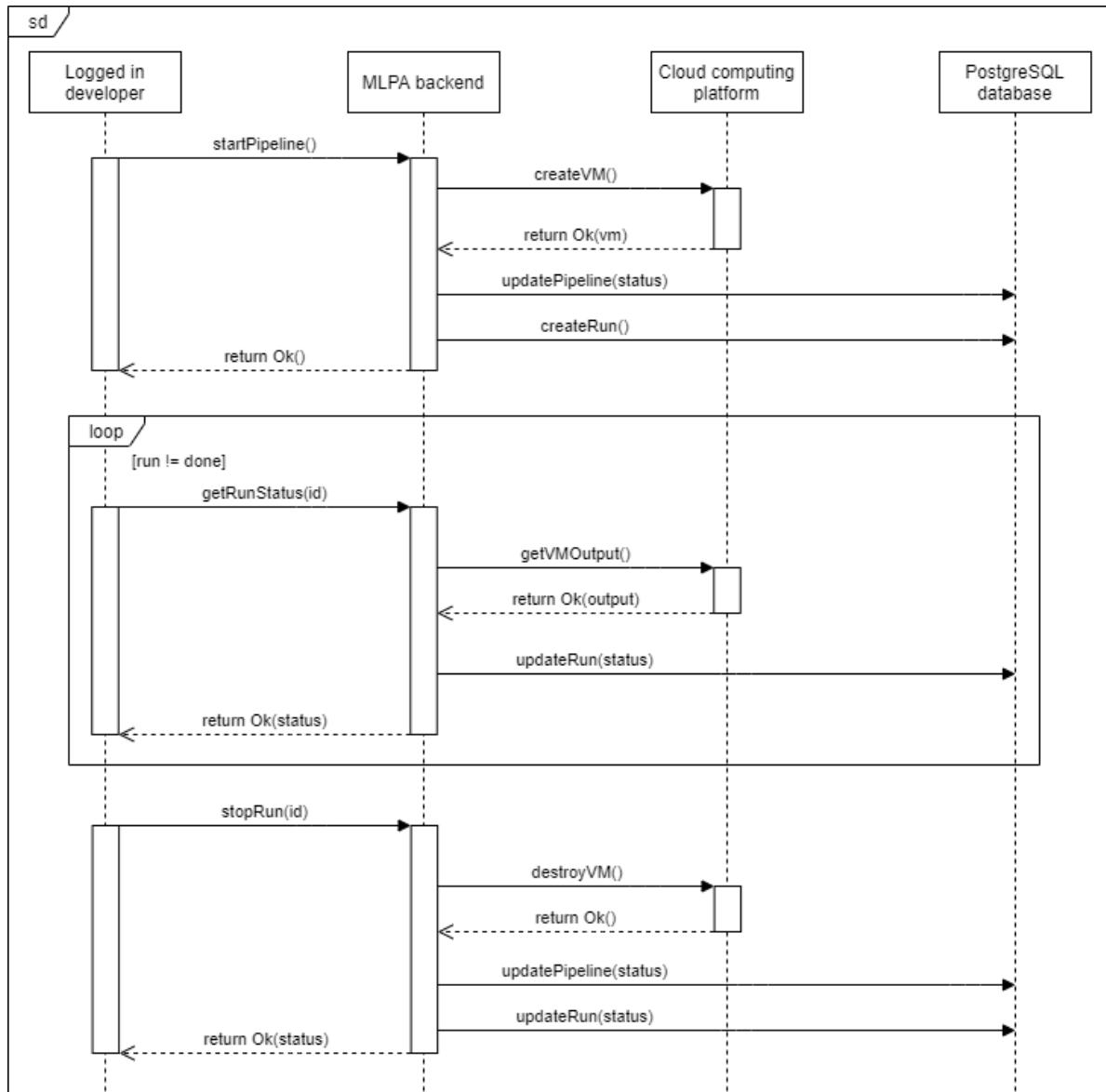
Naast de C4 model diagrammen is het behulpzaam om uit te leggen wat er gebeurd als er een actie wordt uitgevoerd. Dit kan met behulp van sequence diagrammen. Voor belangrijke acties zoals het aanmaken of uitvoeren van een pipeline is een sequence diagram gemaakt. Daarnaast is een entity relation diagram (ERD) gemaakt om de structuur van het database weer te geven. In deze kop wordt door een aantal diagrammen gelopen.

In Figuur 6.6 is te zien wat er gebeurt als een pipeline wordt aangemaakt. De developer stuurt een request naar de backend waar het wordt gevalideerd. De validatie sequence diagram is te vinden in [BIJLAGE LINK]. De backend slaat vervolgens de gegevens op waarna, in parallel, een ingest server, model server en storage bucket worden aangemaakt. De ingest server zorgt voor de intake van datasets, de model traint het model en in de storage bucket wordt alle datasets en modellen opgeslagen. Als deze drie resources zijn aangemaakt, wordt de request voltooid.



Figuur 6.6: Sequence diagram van het aanmaken van een pipeline.

Een sequence diagram is gemaakt om te laten zien wat er gebeurt als een pipeline wordt gestart (Figuur 6.7). De developer zal een request maken om de pipeline te starten. Om dit te doen stuurt de backend een request naar de cloud platform om een virtual machine (VM) te starten. Na het opstarten wordt het trainen van het model automatisch gestart. De backend past de status van de pipeline aan en voltooid de request. De developer weet nu dat een VM is gestart en kan vragen voor de output van de VM. In de output is te zien waar de VM mee bezig is. Dit gebeurt continu totdat het model getraind is en de artefacten veilig zijn opgeslagen. Dit zijn afbeeldingen, modellen en datasets die bewaard moeten worden. Hierna zal de developer een laatste request sturen om de VM te verwijderen en de status in het database aan te passen.



Figuur 6.7: Sequence diagram van het starten van een pipeline.

7 Proof of concept

Om de PoC daadwerkelijk te maken moet er eerst gedefinieerd worden wat de scope is en hoe de PoC eruit gaat zien. De scope brengt in beeld wat er gedaan moet worden en wat de minimal viable product (MVP) is. Op de MVP kan de mock up gebaseerd worden. In dit hoofdstuk wordt de scope bepaald, delen van de mock up doorgelopen, uitleg gegeven over de PoC en kwaliteit van de code. Het hoofdstuk wordt afgesloten met een conclusie en advies

7.1 User requirements verzamelen

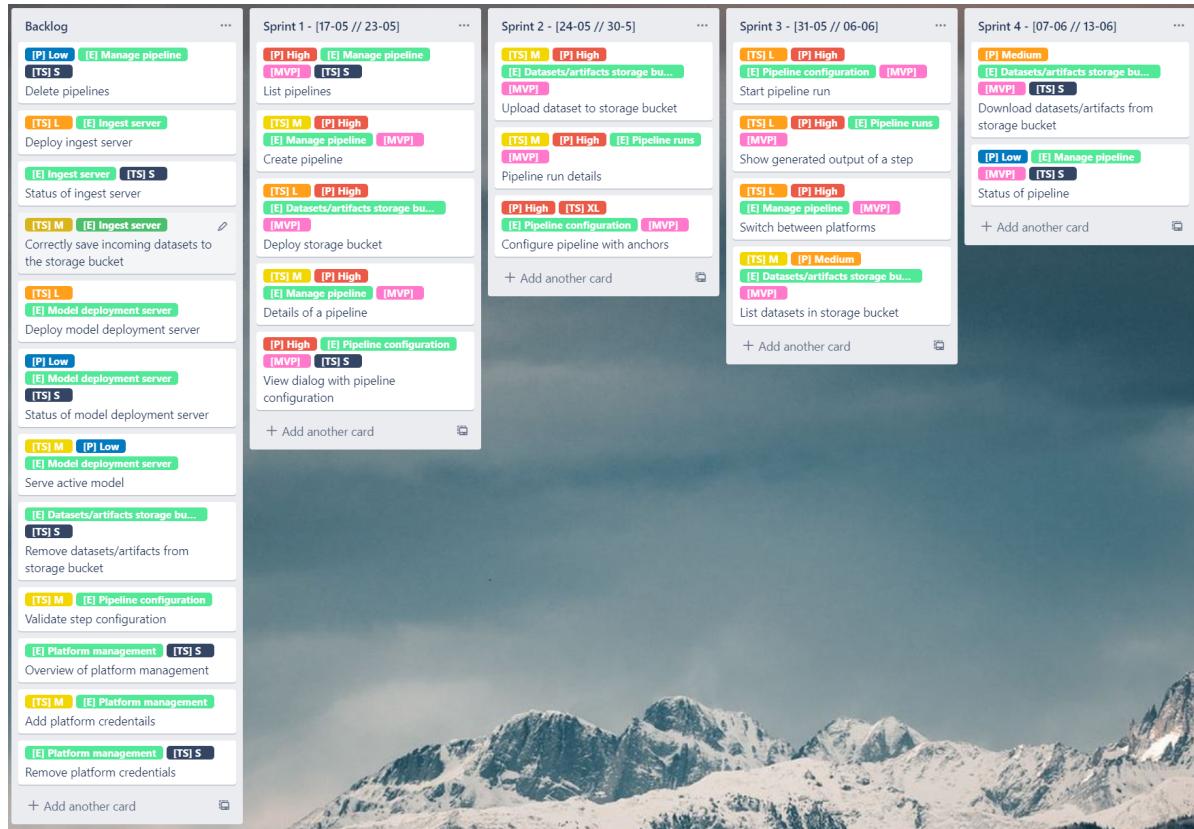
Om te begrijpen wat er gebouwd moet worden kunnen de behoeftes opgeschreven worden in de vorm van user stories. Een user story is de behoefte opgeschreven in een specifieke formaat om belangrijke informatie te achterhalen [[agile-user-story-template](#)]. Een bekende formaat is de *Connextra template* van Mike Cohn [[agile-user-story-template](#)]: "**As a [role], I can [capability], so that [receive benefit]**". De template zorgt ervoor dat de rol (role), functie (capability) en reden (benefit) bekend is. In Figuur 7.1 zijn alle user stories opgesteld, gegroepeerd in Epics. Bij elke user story is ook aangegeven of het MVP is, welk prioriteit het heeft en de t-shirt size. De t-shirt size is een manier om op een hoog niveau aan te geven hoeveel werk een user story vereist. Een **S** vereist weinig werk terwijl **XL** veel werk vereist.

ID	Epic	As a/an...	i want to...	so that...	MVP [Y/N]	P [L/M/H]	T-Shirt [S/M/L/XL]	Notes
1	Manage pipeline	Developer	create a pipeline with a name, project and platform	I can create a pipeline configuration and train ML models	Y	H	M	
2	Manage pipeline	Developer	see the status of a pipeline	I know if a pipeline works or not	Y	L	S	
3	Manage pipeline	Developer	switch between platforms	I am not vendor-locked in	N	H	L	
4	Ingest server	Developer	see the status of the ingest server	I know if the ingest server is available and works correctly	N		S	
5	Ingest server	Developer	upload data from an application to the ingest server with specification on how it's saved	I can use the data in a dataset when a new ML model is being trained	N		M	
6	Model deployment server	Developer	see the status of the model deployment server	I know if the model deployment server is available and works correctly	N		S	
7	Model deployment server	Developer	get a prediction from the model deployment server via an endpoint	I can use a ML model without downloading it and using it locally	N		M	
8	Datasets/artifacts storage bucket	Developer	upload datasets	I can use the dataset when training ML models	Y	H	M	
9	Datasets/artifacts storage bucket	Developer	download datasets	I can experiment locally	Y	L	S	
10	Datasets/artifacts storage bucket	Developer	download dataset artifacts	I can experiment and debug locally	Y	L	S	
11	Datasets/artifacts storage bucket	Developer	download model artifacts	I can use a ML model offline	Y	M	S	
12	Pipeline configuration	Developer	configure the input, action and output of a step	I can use this step in the pipeline	Y	H	XL	
13	Pipeline configuration	Developer	be warned with detailed explanation if the configuration is invalid	I can correct the errors	N		M	
14	Pipeline runs	Developer	see the steps that have been performed in a run	I know what the MLPA did	N	H	XL	
15	Pipeline runs	Developer	see the output a step might have generated	I can see the analysis of datasets and models in a run	N	H	L	
16	Pipeline runs	Developer	start a pipeline run	I can train a model	Y	H	L	
17	Platform management	Developer	save platform keys or pats	I can access resources in platforms when using pipelines	N		S	

Figuur 7.1: Requirements opgesteld voor de proof of concept.

De user stories zijn opgesteld in samenwerking met de begeleiders van NGTI over het hele afstudeerproces. Nu de requirements zijn opgesteld, kan een Kanban bord opgericht worden om sprints te maken.

7.1.1 Requirements vertalen naar een Kanban bord



Figuur 7.2: Sprint 1.

7.2 Mock up van de proof of concept

7.3 De proof of concept

7.3.1 Aanmaken van pipelines

7.3.2 Datasets uploaden

7.3.3 Configuratie definiëren

7.3.4 Pipeline starten

7.3.5 Model downloaden

7.4 Kwaliteit van de code

7.5 Conclusie

7.6 Advies

8 Discussie

8.1

9 Reflectie

Bibliografie

Bijlagen

Scope hoofd- en deelvragen

Scope deelvraag 1

D1: Uit welke stappen bestaat een machine learning pipeline?	
Scope	<p>Binnen de scope:</p> <ul style="list-style-type: none">• In kaart brengen uit welke stappen een pipeline bestaat• Acties die in een stap worden uitgevoerd• Of het mogelijk is om stappen te versimpelen / abstraheren voor developers• Of het mogelijk is om stappen en acties te automatiseren <p>Buiten de scope:</p> <ul style="list-style-type: none">• Automatisering van stappen en acties• Een versimpeling van machine learning
Toelichting	Er wordt gekeken naar welke stappen er in een pipeline zitten. De theorie wordt vervolgens toegepast in een experiment. De nadruk ligt vooral of de mogelijkheid er is om stappen en acties te automatiseren en of machine learning versimpeld kan worden, niet dat er een uitwerking is.

Tabel 1: Scope deelvraag 1

Scope deelvraag 2

D2: Hoe kan een orkestratietool verschillende cloud computing platformen beheren om een machine learning pipeline op te zetten?	
Scope	<p>Binnen de scope:</p> <ul style="list-style-type: none">• High-level uitleg over hoe een orkestratietool werkt• Inventarisatie met de "knock-out" methode• Criteria lijst voor orkestratietools• Opmerkelijke features die relevant zijn voor de PoC• Ervaring opdoen doormiddel van een pipeline te maken op twee cloud computing platformen <p>Buiten de scope:</p> <ul style="list-style-type: none">• Performance en snelheid
Toelichting	Frameworks dat cloud computing platformen beheert worden in kaart gebracht. Met knock-out criteria wordt de lijst verkort. Met een framework wordt een pipeline opgezet.

Tabel 2: Scope deelvraag 2

Scope deelvraag 3

D3: Hoe ziet de architecturale blauwdruk van een applicatie, waarmee een platform-onafhankelijk machine learning pipeline opgezet kan worden, eruit?	
Scope	<p>Binnen de scope:</p> <ul style="list-style-type: none">• Technische tekeningen <p>Buiten de scope: -</p>
Toelichting	De literatuuronderzoek slaat op of de technische tekeningen gemaakt zijn volgens een standaard zoals UML. Dit komt niet terug als theorie maar de bronnen worden wel vermeld.

Tabel 3: Scope deelvraag 3

Scope hoofdvraag

H: In welke mate kan een machine learning pipeline worden geautomatiseerd onafhankelijk van de onderliggende cloud computing platform?	
Scope	De scope wordt bepaald na de requirement analyse.
Toelichting	Onderzoek naar documentatie van gebruikte framework(s).

Tabel 4: Scope hoofdvraag