SAI UPDATE

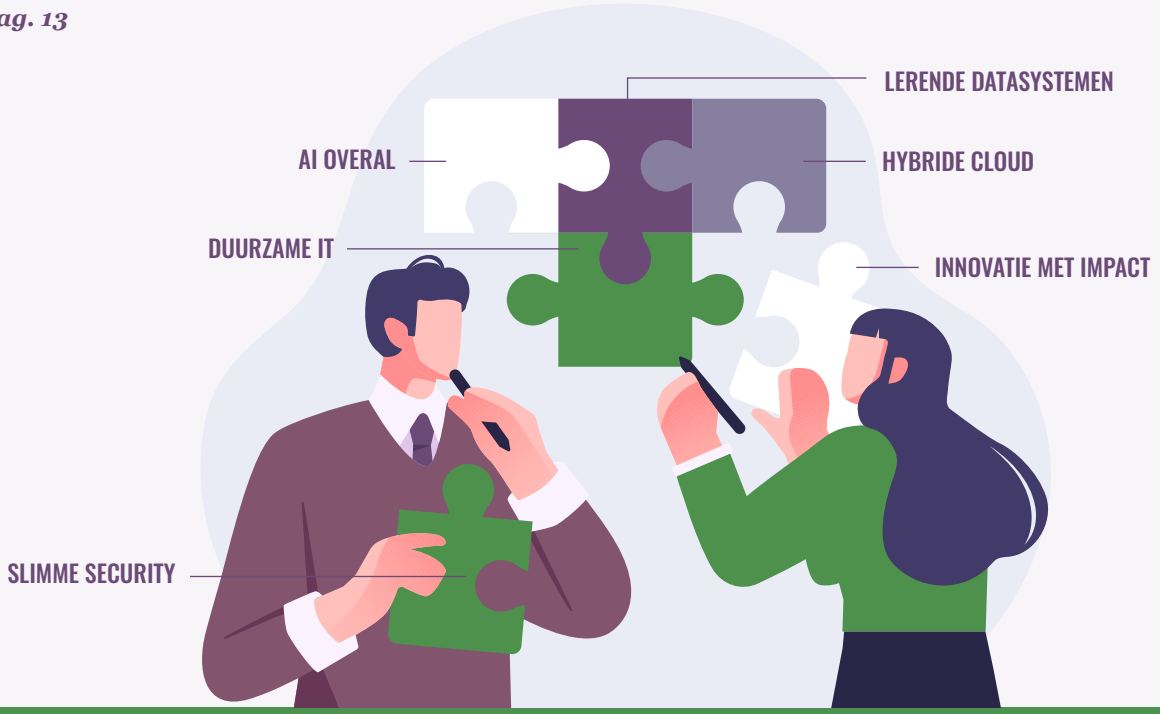
DIGITAAL TIJDSCHRIFT VOOR SAI.BE-LEDEN | NOVEMBER 2025 | SAI

SPECIALE EDITIE: SAI NEXT TECHNOLOGY GENERATION

DE TOEKOMST VAN IT

6 TRENDS EN 12 BIJDRAGEN VAN JONG IT-TALENT

Pag. 13



En verder:

SPIN-OFFS | DUURDERE SOFTWARE | CASE BRUSSELS AIRPORT | SNELST GROEIENDE SOFTWAREBEDRIJF OOIT
PHISHING: MEEST MISBRUIKTE MERKEN | ONLYFANS

CLOUD VOOR AI
DE OPMARS VAN DE NEOCLOUDS
pag. 6

MISVERSTANDEN OVER
VIBE CODING
pag. 7

VAN JUNIOR TOT SENIOR
LONEN VAN IT-PROFIELEN
pag. 10

EDITO

LOKAAL TALENT MAAKT HET VERSCHIL IN DE DIGITALE TOEKOMST

Alles wat je ziet – je smartphone, de apps die je leven gemakkelijker maken – draait op technologie. IT is overal. Maar wat echt telt, zijn niet de machines of de algoritmes, wel de mensen erachter.

SAI.BE nam het initiatief om een staalkaart te maken van wat studenten en onderzoekers vandaag ontwikkelen als antwoord op actuele digitale uitdagingen. En wat blijkt? In België is iets bijzonders aan de hand. Terwijl de wereld worstelt met technologische versnelling, artificiële intelligentie en digitale onzekerheden, groeit hier lokaal een generatie jonge talenten op met een scherp verstand, een kritische blik en een honger naar digitale kennis. Het is aangenaam om vast te stellen dat we nog altijd mogen beschikken over veel lokaal IT-talent dat vandaag al vorm geeft aan de digitale toekomst van morgen.

Er wordt in sommige kringen geopperd dat jongeren twijfelen aan de waarde van een opleiding of carrière in IT. “De markt is verzadigd”, “AI doet straks alles”, “cybersecurity is te complex”… Het zijn misverstanden die we dringend moeten doorbreken. IT is namelijk niet meer louter een vakgebied in de hogeschool of universiteit – het is de zuurstof van onze huidige en toekomstige samenleving. Van duurzame energie en slimme steden tot veilige digitale identiteiten en ethische algoritmes: elke digitale vooruitgang rust op de schouders van mensen die begrijpen hoe de technologie concreet werkt én wat ze kan betekenen in de praktijk, met aandacht voor alle facetten. Achter al die innovaties staan mensen met ideeën, lef en passie.

> *“The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn and relearn.”*
> ALVIN TOFFLER, AMERIKAANS FUTURIST EN AUTEUR

In België hebben we nog altijd een unieke mix van academische excellentie, ondernemerschap en maatschappelijke betrokkenheid. Onze universiteiten en hogescholen leveren topingenieurs en datawetenschappers af. We hebben opstartende en ervaren ondernemingen die vooroplopen in AI-toepassingen, cybersecurity en duurzame technologie. Onze jonge digitale experten beschikken over iets wat geen enkele machine kan of zal nabootsen: creativiteit, empathie, kritisch denkvermogen en verantwoordelijkheidszin. Ze kijken verder dan schermen en cijfers en beseffen dat technologie pas echt krachtig is als ze iets verbetert voor mens en maatschappij.

Artificiële intelligentie biedt nog altijd ongekende kansen, maar alleen als ze gevoed wordt door menselijk inzicht en gericht blijft op echte toegevoegde waarde. Cybersecurity beschermt niet alleen toestellen en netwerken, maar ook het vertrouwen van mensen in technologie. Duurzaamheid vraagt niet alleen groene energie, maar ook slimme technologie die verspilling tegengaat. En de maatschappelijke betekenis van IT? Die ontstaat wanneer technologie niet alleen winst oplevert, maar ook welzijn voor iedereen. Dat is precies waar ons lokaal IT-talent in uitblinkt: het verbinden van kennis met waarden.

Daarom is het essentieel dat jongeren blijven geloven in de kracht van IT-kennis. Niet als doel op zich, maar als middel om impact te maken. We hebben de lokale hersenkracht, de infrastructuur en de mentaliteit om in het koppeloton van internationale voorbeeldregio’s te blijven in ethische, duurzame en veilige technologie. Wat we vooral nodig hebben, is geloof in onze eigen capaciteiten, in samenwerking, kritisch denken en de positieve kracht van digitale innovatie.

De toekomst wacht niet. Ze wordt geschreven in code, beveiligd met inzicht en gedragen door mensen met visie. Daarom wil SAI.BE jonge talenten aanmoedigen om die toekomst niet te ondergaan, maar actief vorm te geven. De wereld heeft naast programmeurs ook denkers, ontwerpers, dromers en doeners nodig. Mensen die technologie gebruiken om het verschil te maken.

Ja, de toekomst is digitaal, maar ze is vooral menselijk. En SAI.BE rekent op dit talent – niet om zomaar te volgen wat anderen bouwen, maar om zelf te creëren, te beveiligen en te verbeteren.

Ik nodig je dan ook met veel plezier uit om dit speciaal SAI NXT-magazine te lezen en commentaar te geven aan voorzitter@sai.be.

Marc Vael
Voorzitter raad van bestuur SAI.BE

INHOUD

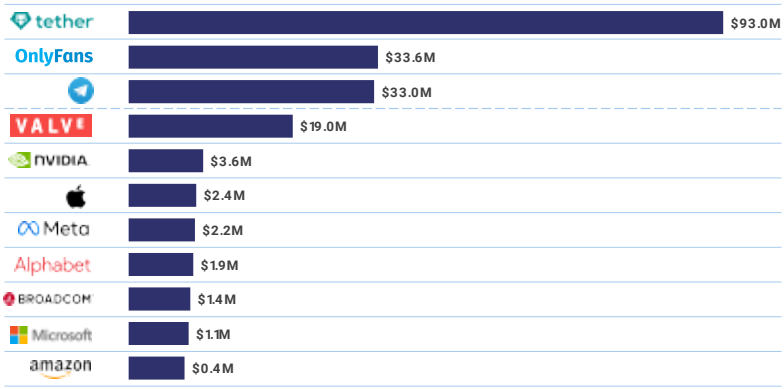
MEEST RENDABEL IN TECH? CRYPTO EN ONLYFANS

Twee techbedrijven staan bovenaan als het gaat om de omzet per werknemer: Tether en – jawel – OnlyFans.

Tether beheert de grootste zogenoemde stablecoin ter wereld, USDT — een digitale munt die altijd één op één aan de Amerikaanse dollar gekoppeld is. Voor elke uitgegeven munt houdt Tether echte dollars of obligaties aan in reserve. Die reserves leveren veel rente op, in vergelijking met hun kosten voor personeel of infrastructuur.

Nog indrukwekkender is OnlyFans, het direct-to-fan-platform waarop makers hun volgers laten betalen voor exclusieve content, vaak met een volwassen tintje. Volgens databedrijf Multiples genereert OnlyFans 33,6 miljoen dollar omzet per werknemer, tegenover 3,6 miljoen bij Nvidia. Met slechts 42 vaste medewerkers draait OnlyFans 1,4 miljard dollar omzet.

Toch kent hun model ook schaduwzijden. Meer dan 70 procent van alle uitbetalingen gaat naar slechts 10 procent van de makers. De gemiddelde content creator verdient er minder dan 150 dollar per maand. Dat maakt OnlyFans niet alleen een uitzonderlijke winstmachine, maar ook een spiegel voor de ongelijkheid in de digitale economie.



VIER OP DE TIEN PHISHINGAANVALLEN IMITEREN MICROSOFT-DIENSTEN

Microsoft is veruit het populairste merk bij phishers. Maar liefst 40 procent van alle wereldwijde phishingpogingen imiteerde het techbedrijf.

Dat blijkt uit het Brand Phishing Report Q3 2025 van Check Point Research, de Threat Intelligence-tak van Check Point Software Technologies. Google (9 procent) en Apple (6 procent) vervolledigen de top drie. Samen waren deze drie merken verantwoordelijk voor meer dan de helft van alle phishingactiviteiten in het afgelopen kwartaal.

Phishing draait niet langer alleen om e-mails met spelfouten of slecht ontworpen inlogpagina's, stelt Omer Dembinsky, data research manager bij Check Point Software. “Het is nu AI-gegenereerd, hyper-gepersonaliseerd en extreem misleidend”, waarschuwt hij.

Naast de technologiesector worden ook sociale netwerken en retail (zoals Booking.com) geviseerd. "Aanvallers richten zich op de diensten en tools die gebruikers het meest vertrouwen”, zegt Dembinsky. Met het hoogseizoen voor online winkelen in aantocht, verwacht Check Point dat phishingcampagnes binnen de reis- en logistieke sectoren verder toenemen.

Dembinsky benadrukt dat een preventiegerichte aanpak nodig is: “AI-gedreven beveiliging, sterke authenticatie en voortdurende gebruikerseducatie zijn essentieel om deze nieuwe golf van phishing het hoofd te bieden.”

TOP 10 MEEST GEÏMITEERDE MERKEN

1. Microsoft – **40%**
2. Google – **9%**
3. Apple – **6%**
4. Spotify – **4%**
5. Amazon – **3%**
6. PayPal – **3%**
7. Adobe – **3%**
8. Booking.com – **2%**
9. LinkedIn – **2%**
10. DHL – **2%**

Bron: Brand Phishing Report, Q3 2025

IT-UITGAVEN 10 PROCENT HOGER, SOFTWARE DUURDER

Ook in 2026 groeit de wereldwijde IT-markt met zowat 10 procent. Daarmee zouden de IT-bestedingen voor het eerst de grens van 6 biljoen dollar overschrijden, blijkt uit prognoses van onderzoeksbureau Gartner. Maar die stevige groei lijkt niet voor iedereen weggelegd.

De groei wordt vooral gedreven door investeringen in AI-infrastructuur en devices. “De onzekerheid die in het tweede kwartaal van 2025 begon, is verminderd. Er wordt een aanzienlijke budgetinjectie verwacht voor het einde van het jaar”, zegt John-David Lovelock, Distinguished VP Analyst bij Gartner.

GENAI MAAKT SOFTWARE DUURDER

Een opvallende trend is de stijgende kostprijs van software. “GenAI-functies zijn nu alomtegenwoordig in software die bedrijven al bezitten en gebruiken, en deze functies kosten meer geld”, aldus Lovelock. De kosten van zowel de software zelf als de functionaliteit stijgen door de integratie van GenAI-mogelijkheden.

De groei verloopt echter niet uniform over alle segmenten. “Software- en services-uitgaven in 2025 herstellen niet op dezelfde manier als devices en datacentersystemen. Verticaal-specifieke software is bijvoorbeeld sterker getroffen, omdat kopers op brancheniveau gevoeliger zijn voor beleidswijzigingen en onzekerheden”, legt Lovelock uit.

AI VOOR DEVICES EN DATACENTERS

De devicemarkt profiteert van sterke smartphone- en pc-verkopen in de eerste helft van 2025, met een stijging van 8,4 procent. “Deze groei wordt vooral aangedreven door mobiele telefoons”, zegt Lovelock.

Voor datacentersystemen blijft de vraag hoog door de race om AI-infrastructuur uit te bouwen, met name AI-geoptimaliseerde serverracks. "De toenemende vraag blijft echter beperkt door aanbodproblemen”, merkt Lovelock op. De vraag is of leveranciers in 2026 deze supplychainuitdagingen kunnen oplossen.

WERELDWIJDE IT-BESTEDINGEN (IN MILJOEN US DOLLAR)

Segment	Uitgaven 2025 (in miljoen $)	Groei 2025 (%)	Groei 2026 (%)
Datacentersystemen	489.451	46,8	19,0
Devices	783.157	8,4	6,8
Software	1.244.308	11,9	15,2
IT services	1.719.340	6,5	8,7
Communicatiediensten	1.304.165	3,8	4,5
Totaal IT	5.540.421	10,0	9,8

Bron: Gartner (oktober 2025)

NA DE HACK BIJ BRUSSELS AIRPORT

WAT NIS2 ÉCHT BETEKENT VOOR TOELEVERANCIERS

Toen Brussels Airport recent getroffen werd door een ransomwareaanval, wees de luchthaven deels naar leverancier Collins Aerospace. Maar de Europese NIS2-wetgeving is formeel: essentiële organisaties blijven zélf verantwoordelijk voor hun volledige digitale keten, ook voor wat ze uitbesteden.

De aanval trof het check-in- en bagagesysteem, dat door Collins Aerospace werd geleverd én beheerd. Het gevolg: een resem geschrapte vluchten. Het zou gaan om HardBit, een variant van de gijzelsoftware Loki Locker.

Pogingen om via back-ups het systeem te herstellen mislukten aanvankelijk. Zodra de servers opnieuw opgestart werden, infiltreerden de aanvallers opnieuw. Uiteindelijk besliste Brussels Airport om het volledige systeem te vervangen.

BOETE

Juridisch gezien kan de luchthaven zich niet zomaar achter Collins verschuilen. Onder de Belgische NIS2-wet – die Europese verplichtingen omzet in nationale regels én waarvan België een van de eerste landen was die dit deed – moeten essentiële bedrijven aantonen dat ze hun volledige toeleveringsketen actief controleren en beveiligen. Volgens juristen riskeert Brussels Airport, als blijkt dat deze controle onvoldoende was, een boete tot 2 procent van de omzet of 10 miljoen euro.

De wet verplicht niet alleen tot technische maatregelen, maar ook tot governance, transparantie en controle, dus ook over partners, leveranciers en subcontractors.

Dat betekent concreet: risicoanalyses uitvoeren, leveranciers auditen en erop toezien dat ook externe partners voldoen aan cybersecurity-normen. Met andere woorden: NIS2 verankert een cultuurverandering waarbij cyberveiligheid niet langer kan worden 'uitbesteed'.

BESEF

Volgens Christian Verhoeve, lead auditor bij BSI en voorheen security officer, is NIS2 alvast geen uitzondering. "In de ISO27001 staat ook dat bijna sneaky zinnetje dat uitbestede processen *shall ensure (to be) controlled*. Een klein zinnetje met veel impact dat te vaak over het hoofd wordt gezien", zegt Verhoeve.

10 miljoen euro

Mogelijke boete voor Brussels Airport

Maar dergelijke zinnetjes hebben dus gevolgen. "Bij Brussels Airport worden ze nu met hun neus op de feiten gedrukt: uitbesteden ontslaat niet van verantwoordelijkheid. Hoe leeft dat besef in jouw organisatie?"

INFRASTRUCTUUR VOOR AI

DE OPMARS VAN DE NEOCLOUDS

De wereld van IT-infrastructuur is in de ban van een nieuwe term: neoclouds. Een nieuwe generatie cloudproviders gooit de markt op zijn kop met infrastructuur die vanaf nul is opgebouwd voor één ding: AI. Wat betekent dat voor de toekomst van cloud computing en voor jou?

De term 'neocloud' verwijst naar een nieuwe generatie cloudproviders die zich toeleggen op GPU-as-a-Service (GPUaaS). In tegenstelling tot traditionele cloudproviders zoals AWS, Azure en Google Cloud, bouwen neoclouds hun volledige stack – infrastructuur, networking en software – specifiek voor AI-taken.

WAAROM HEBBEN BEDRIJVEN NEOCLOUDS NODIG?

Hoewel de grote hyperscalers investeren in GPU-gerichte diensten, beperkt hun *general-purpose design* hoe ver ze zich werkelijk kunnen specialiseren. Hun brede focus – van legacy-enterpriseapplicaties tot IoT – brengt voor AI-gebruikers vaak extra complexiteit en inefficiënties met zich mee.

"Neoclouds transformeren cloud computing door *purpose-built*, kosteneffectieve infrastructuur voor AI-workloads aan te bieden. Ze zullen het marktaandeel van traditionele cloudproviders uitdagen", voorspelt David Linthicum, cloudexpert, auteur en columnist bij Infoworld.

WIE ZIJN DE SPELERS?

CoreWeave is de grootste en meest dominante speler, met OpenAI als vooraanstaande klant. Het is gespecialiseerd in high-performance GPU-resources voor AI-workloads en positioneert zich als alternatief voor traditionele cloudproviders. Lambda Labs behoort tot de weinige aanbieders die zowel cloud als on-premises GPU-oplossingen leveren, specifiek voor deep learning en AI-onderzoek. Andere partijen zijn Crusoe, WhiteFiber, het Europese Nebius en Together AI, dat zich focust op open-source LLM's.

WAT MAAKT NEOCLOUDS INTERESSANT?

Enerzijds beantwoorden ze aan een duidelijke behoefte. Ook in België staat AI hoog op de prioriteitenlijst van IT-beslissers. "Uit een wereldwijd onderzoek dat we recent uitvoerden met *Enterprise Strategy Group* blijkt dat 84% van de respondenten AI als cruciaal beschouwt voor de toekomst van hun organisatie", stelt Simon Robinson, Principal Analyst bij Omdia. "89% maakt significante infrastructuurinvesteringen om AI-initiatieven te ondersteunen."

Naast de vraag is er het aanbod. Neoclouds zijn nichespelers zonder de noodzaak om alles te ondersteunen. Ze overtreffen hyperscalers in wendbaarheid en gerichte prijszetting, wat hen steeds aantrekkelijker maakt voor AI-onderzoekers, startups en grotere ondernemingen.

WAT ZIJN DE UITDAGINGEN UITDAGINGEN VOOR NEOCLOUDS?

The money. Het verwerven van de krachtigste GPU's, die ook snel in waarde dalen bij elk nieuw model, vereist significant kapitaal, ook voor energie. In dynamische en multi-tenant omgevingen is het bovendien behoorlijk complex om piekprestaties te leveren. Ook vendor lock-in is een reëel risico: Nvidia domineert de GPU-, networking- en software-aanvoer. Aanhoudende tekorten kunnen hierbij vooral kleinere neoclouds raken.

HOE NEOCLOUDS INZETTEN?

Voor organisaties die het potentieel van AI willen benutten, bieden neoclouds kansen om architectuur te optimaliseren en kosten te verlagen. Drie stappen zijn cruciaal, volgens David Linthicum: planning (identificeer welke AI-workloads baat hebben bij gespecialiseerde GPU-infrastructuur), architectuur (zorg voor modulaire designs die workloads tussen platforms laten bewegen) en test deployments (valideer prestatie- en kostenclaims via pilots voor de uitrol).

WANNEER?

De transitie gebeurt niet van de ene op de andere dag, maar de behoefte en trend is er zeker. De vraag is niet langer *óf* we neoclouds moeten omarmen, maar *wanneer* en *hoe*, stelt David Linthicum. "Organisaties die zich aanpassen, optimaliseren niet alleen hun AI-capaciteiten maar blijven ook competitief", zegt hij. "Neoclouds zijn geen tijdelijke trend, maar een fundamentele verschuiving in hoe we over cloud-infrastructuur denken."

VIER VRAGEN OVER VIBE CODING

“HET GROOTSTE MISVERSTAND IS DAT JE GEEN PROGRAMMEURS MEER NODIG HEBT”

Vibe coding laat ontwikkelaars experimenteren, prototypen en bestaande code optimaliseren – sneller dan ooit. “De code die AI genereert, is vaak efficiënter en leesbaarder dan wat een doorsnee ontwikkelaar met de hand schrijft”, zo klinkt het. Maar er zijn ook valkuilen.

Vibe coding is een informele manier van programmeren waarbij ontwikkelaars AI-tools, zoals *large language models*, inzetten om code te laten genereren op basis van losse beschrijvingen, schetsen of minimale aanwijzingen.

“Vibe coding lijkt niet op klassiek handmatig coderen, maar eerder op een nieuwe manier van software ontwikkelen waarbij AI, no-code en co-creatie centraal staan”, zegt Roel Verbeeck van softwarebedrijf Ixor, die het op gepaste momenten inschakelt. “Het verlaagt de drempel om ideeën om te zetten naar prototypes en maakt itereren veel sneller.”

Zowel junior als senior ontwikkelaars kunnen baat hebben bij vibe coding. “Juniors komen sneller tot resultaat, seniors versnellen creativiteit, innovatie en samenwerking.” Het helpt ook om de vaardigheden van ontwikkelaars uit te breiden. “Een senior backendontwikkelaar met twintig jaar ervaring kan zo ook snel een front-end opzetten. Ze zeggen in IT vaak dat het een kwestie is om meer gespecialiseerd te zijn. Maar dit nieuwe concept gaat daar eigenlijk tegenin. Je wordt als ontwikkelaar breder qua skills en mogelijkheden.”

1/ WANNEER IS VIBE CODING (NIET) GESCHIKT?

Wel geschikt:

- Exploratie en creatief prototypen: voor snelle experimenten, proof-of-concepts of het integreren van nieuwe API’s is vibe coding bijzonder waardevol. “Het geeft ontwikkelaars inspiratie en versnelt de eerste stappen”, stelt Verbeeck.
- Routinewerk versnellen: boilerplate, documentatie en tests laten genereren bespaart veel tijd en maakt dat onze teams zich kunnen focussen op de échte uitdagingen.
- Bestaande code verbeteren en optimaliseren: “Zeker in combinatie met profilingtools zien we indrukwekkende resultaten. AI kan bestaande code herschrijven en sneller en efficiënter maken dan wat je manueel zou doen”, zegt hij.

Niet geschikt:

- Architectuur en fundamenten: voor keuzes rond architectuur, security en schaalbaarheid blijft menselijke expertise cruciaal. “AI komt hier vaak slechts met *hello world*-starters die later tot problemen leiden.”
- Securitygevoelige of *mission-critical code*: “AI maakt nog te vaak slordige fouten. Voor deze domeinen vertrouwen we op strikte interne reviewprocessen.”
- Wanneer kwaliteit boven snelheid gaat: AI kan een vals gevoel van zekerheid geven. “Werkende code en slagen van tests zijn niet automatisch gelijk aan robuuste kwaliteit.”
- Opschaling zonder expertise: “Voor prototypes is vibe coding nuttig, maar voor duurzame systemen blijven ervaren ontwikkelaars onmisbaar.”

Roel Verbeeck van softwarebedrijf Ixor.

Op sommige momenten is vibe coding dan weer uitermate geschikt. “We gebruiken vibe coding bijvoorbeeld intensief tijdens onze Agentic AI Days, waar we samen met een klant op één dag een probleem uitwerken”, stelt Roel Verbeeck. “Het resultaat is al enkele keren echt verbluffend geweest: duidelijk te begrijpen en werkende prototypes, die meteen de aanzet vormden voor een aantal concrete projecten.”

2/ WAT ZIJN DE GROOTSTE MISVERSTANDEN?

- Je hebt geen programmeurs meer nodig: integendeel. “Je hebt betere programmeurs nodig die AI-resultaten begrijpen, valkuilen herkennen en kwaliteit waarborgen.”
- AI levert productiecode: “In werkelijkheid levert AI een eerste versie, nooit een finale. Iteraties en reviews zijn noodzakelijk.”
- Geslaagde tests wijzen op kwaliteit: “AI genereert tests die vaak oppervlakkig zijn en zelfbevestigend. Slagen van gegenereerde tests betekent niet dat de code robuust is.”
- Met vibe coding gaat software creëren vanzelf: “We merken dat er meer dan ooit moet nagedacht worden over wat we juist willen dat de software doet en dat de impact van onduidelijke instructies leidt tot slecht of fout werkende software.”

“Zelf benadrukken we altijd dat vibe coding geen vervanging is van expertise, maar een versneller die juist méér vraagt van ontwikkelaars én van business owners of analisten”, benadrukt Roel Verbeeck. “*Garbage in-Garbage out*, is ook in de vibe coding-wereld een waarheid, maar dan tien keer sneller.”

3/ WELKE VAARDIGHEDEN HEEFT EEN ONTWIKKELAAR NODIG VOOR VIBE CODING?

- Sterke technische basiskennis: kennis van architectuur, security en clean code is noodzakelijk. “AI kan invullen, maar de grenzen bewaak je zelf.”
- Prompting en contextmanagement: tools die de hele codebase zien, zoals Cursor, geven betere resultaten. “Wij trainen onze teams in context aanbieden, loops doorbreken en problemen opsplitsen.”
- Analytische vaardigheden: AI kan snel en verblindend overtuigen. “Daarom is het belangrijk om heel goed te begrijpen wat het einddoel van de software is.”
- Reviewcultuur: “Omdat vibe coding sneller produceert, leggen wij de nadruk op peer reviews en kwaliteitsborging.”
- Mentale discipline: “We bewaken bewust het evenwicht: vibe coding gebruiken waar het waarde toevoegt, maar niet uit gemakzucht.”

In de nieuwe wereld van AI en co-creatie is de aanpak om dicht bij de klant of opdrachtgevers te staan cruciaal. “Technologie verandert razendsnel, maar het echte verschil krijg je nu door kristalhelder de technologie toe te passen op de uitdagingen van de klant.”

4/ HOE HERKEN JE DAT EEN AI-CODEVOORSTEL BETROUWBAAR GENOEG IS OM TE GEBRUIKEN IN PRODUCTIE?

- Ook gegenereerde code moet begrijpelijk zijn: “Als je het niet kunt uitleggen, is het niet goed genoeg.”
- Doe de test: “Er wordt extra nadruk gelegd op het schrijven van tests en het kritisch in vraag stellen van de bestaande tests.”
- Checken: “We duiden aan wat AI gegenereerd is en alles passeert een extra menselijke review.”

“DOORDAT AI-CODE GOED OOGT, ONTSTAAT ER SOMS EEN VALS GEVOEL VAN KWALITEIT”

Bij softwarebedrijf Ixor zien ze de voordelen, maar zeker ook de aandachtspunten of zelfs gevaren van vibe coding.

“De code die AI genereert, is vaak efficiënter en leesbaarder voor andere ontwikkelaars dan wat een doorsnee programmeur met de hand schrijft”, zegt Roel Verbeeck van Ixor.

Volgens hem ligt de kracht van vibe coding vooral in de manier waarop moderne tools de context van een volledige codebase meenemen. “Tools zoals Cursor, die de hele codebase analyseren, leveren merkbaar betere resultaten dan traditionele AI-assistenten die alleen lokale bestanden bekijken.”

DODE CODE

AI neemt veel routinewerk uit handen, maar het ontwikkelproces blijft iteratief. “Het gaat sneller, maar je moet blijven bijsturen”, benadrukt Verbeeck. Er schuilen risico’s achter het gemak: “**We zien geregeld valkuilen zoals inefficiënte loops, dode code, security-fouten of te oppervlakkige tests**. Het gevaar is dat AI-code op het eerste gezicht goed oogt, waardoor er een vals gevoel van kwaliteit kan ontstaan.”

Volgens Verbeeck komt vibe coding vooral tot zijn recht bij het optimaliseren van bestaande code. Voor fundamentele architecturale keuzes is het minder geschikt. “Daar blijft menselijke analyse onmisbaar”, zegt hij. Daarom moeten ontwikkelaars volgens hem extra waakzaam blijven voor de klassieke disciplines van softwareontwikkeling: grondige analyse, degelijk testen en zorgvuldige peer review.

Lovable-oprichters Anton Osika en Fabian Hedin.

LOVABLE: HET SNELST GROEIENDE SOFTWAREBEDRIJF OOIT

Vibe coding is ook hot in de start-upwereld. De Zweedse start-up Lovable – een GenAI- en vibe coding-frontrunnner – bereikte 100 miljoen omzet in acht maanden, sneller dan welk softwarebedrijf ooit.

Met Lovable kan iedereen in een paar uur een volledig werkende online onderneming bouwen, inclusief geldstromen, facturatie, verzending en nog veel meer. Het systeem van oprichters Anton Osika en Fabian Hedin stelt niet-technische gebruikers in staat om apps of websites te bouwen op basis van eenvoudige tekstprompts. “Ik besloot dat we iets moesten bouwen voor de 99 procent die geen software maakt”, aldus Anton Osika bij de oprichting. Of zoals op zijn LinkedIn-bio staat: *building the last piece of software*.

De twee beseften dat er honderden tools bestonden waarmee je vlot een website kon bouwen, maar ze misten een tool die met een simpele prompt en enkele kliks een volledige online onderneming kon ontwikkelen. Dus bouwden ze die zelf, met succes. Lovable wil volgend jaar een jaaromzet van 1 miljard dollar halen.

Door niet-technische oprichters in staat te stellen succesvolle bedrijven op te zetten zonder enige voorafgaande ervaring met coderen of software, gelooft Osika dat het bedrijf ‘een nieuwe economie ontsluit’.

Lovable heeft intussen meer dan 20.000 bedrijven als klant, goed voor ruim 2,3 miljoen actieve gebruikers. Volgens het bedrijf worden er elke dag tienduizenden nieuwe projecten gecreëerd. Het bedrijf is intussen naar eigen zeggen ‘volledig agentic’, wat betekent dat het platform op het internet content kan zoeken, code kan debuggen en applicaties kan bewerken met volledige context, allemaal zonder menselijke tussenkomst.

KINDERZIEKTES?

Natuurlijk zijn er concurrenten in dit domein zoals Cursor, Replit, StackBlitz en WeWeb, maar vooral Lovable lijkt de wind in de zeilen te hebben. Toch zijn er kritische geluiden. In zijn recente Medium-artikel *Lovable is doomed* uit de Europese tech-analist Derick David scherpe kritiek op het razendsnel gegroeide Lovable.

Volgens David verliest het bedrijf het vertrouwen van zijn gebruikers snel door technische problemen, zoals vastgelopen deploys, niet-bijgewerkte analytics en verschillen tussen test- en productieomgevingen. “Snelle groei mag niet ten koste gaan van betrouwbaarheid en gebruikerservaring”, zegt hij.

STARTERS BEGINNEN AAN 2.750 À 4.000 EURO

EEN LOOPBAAN IN IT: WAT SCHUIFT DAT?

Een carrière in IT biedt perspectief voor zowel starters als ervaren profielen. Ook qua loonpakket. Waar een IT-directeur gemiddeld 8.912 euro bruto per maand verdient, ligt het instaploon voor starters tussen 2.750 en 4.000 euro bruto, afhankelijk van de functie. Een overzicht van de lonen voor een twintigtal IT-profielen op starters- en gemiddeld niveau.

Goed nieuws voor wie de ICT-sector instroomt: maar liefst 38 procent van de bedrijven is van plan om hun IT- en digitale teams uit te breiden. Bedrijven willen hun techbasis versterken, systemen futureproof maken en strategische groei stimuleren.

1/ HOE GROOT IS HET SALARISVERSCHIL TUSSEN STARTER EN ERVAREN PROFIEL?

Voor de lonen zelf baseren we ons op onderzoek van Robert Half, meer bepaald hun Salarisgids voor 2026.

Wout Van de Wijer (Robert Half): "Automated machine learning, business intelligence, cybersecurity en cloud: dat zijn de topvaardigheden waar hiring managers vandaag naar zoeken."

Wat je verdient in de IT-sector kan flink verschillen tussen starters en ervaren profielen. Robert Half hanteert het 25ste percentiel voor juniorprofielen met weinig of geen ervaring, het 50ste percentiel voor kandidaten met gemiddelde ervaring en het 75ste percentiel voor een erg ervaren iemand met gespecialiseerde kwalificaties en (zo goed als) alle nodige vaardigheden. Het verschil kan oplopen tot duizenden euro's per maand.

Een IT-servicedeskagent start bijvoorbeeld aan 2.782 euro, maar verdient met meer ervaring gemiddeld 3.246 euro. Voor een softwaredeveloper ligt het instaploon op 4.029 euro, met een groei naar 4.584 euro bij een gemiddelde ervaring.

2/ WIE VERDIENT HET MEEST?

De hoogste lonen vinden we bij de managementfuncties, met op kop de IT-director, gevolgd door de PMO-manager en application manager. Leidinggevenden maken vaak ook de grootste salarissprong: een IT-manager begint bijvoorbeeld aan 5.811 euro en groeit door naar 7.639 euro gemiddeld. Al gaat het hier vaak niet om juniorprofielen, managementprofielen – een ook beginnende IT-managers of IT-directors – hebben vaak wel al ervaring in een andere IT-functie en groeien vaak door uit een andere IT-rol.

3/ WAT ZIJN GEWILDE VAARDIGHEDEN VOOR STARTERS?

Starters die zich willen onderscheiden op de arbeidsmarkt doen er goed aan om in te zetten op specifieke vaardigheden. De topvaardigheden waar hiring managers vandaag naar zoeken zijn, volgens Robert Half, *automated machine learning*, business intelligence en rapportage, cybersecurity en cloud. "Wie over deze skills beschikt, kan daar zijn voordeel mee doen op de arbeidsmarkt",

aldus Wout Van de Wijer, manager bij Robert Half. Vooral talent met ervaring en kennis van cybersecurity is gewild. “Bijna de helft (46 procent) van de ondervraagde werkgevers zegt bereid te zijn een hoger start- of top-salaris te betalen als een kandidaat cybersecurityvaardigheden bezit”, weet Wout Van de Wijer.

4/ WAT WILLEN IT-PROFESSIONALS ZELF?

IT-professionals in de sector geven, volgens Robert Half, zelf aan vooral cybersecurity, AI-gestuurde softwareontwikkeling, cloudplatformen en ontwikkeling van generatieve AI te willen aanleren of verbeteren.

Ten slotte nog dit: het aanhoudende tekort aan gekwalificeerd personeel speelt in het voordeel van starters. Maar liefst 55 procent van de Belgische hiring managers in IT biedt meer loon wanneer er een tekort is aan gekwalificeerde kandidaten.

MEEST GEVRAAGDE CERTIFICATEN

- CISSP
- Prince 2
- Agile
- Azure Certifications
- ITIL

MEEST GEVRAAGDE FUNCTIES

- Helpdesk support
- Systems engineer
- Projectmanager
- ERP/CRM-analist
- IT-coördinator

Bron: Robert Half, Salarisgids 2026

VAN JUNIOR NAAR (VEEL) ERVARING: SALARISSEN PER PROFIEL

Hieronder een overzicht van de lonen voor een twintigtal IT-functies, van starters (25ste percentiel) via profielen met gemiddelde ervaring (50ste percentiel) tot bovengemiddeld veel ervaring (75ste percentiel).

1. Businessanalyse	**STARTER**	**MEDIAAN**	**ERVAREN**
• ERP-/Application Consultant:	€ 3.611	€ 4.238	€ 5.018
• Functioneel analist:	€ 3.694	€ 4.342	€ 5.269
• IT-businessanalist:	€ 3.768	€ 4.464	€ 6.022
2. Data & Business Intelligence			
• BI-consultant:	€ 3.698	€ 4.529	€ 5.253
• BI-analist:	€ 4.063	€ 5.020	€ 5.547
3. IT-infrastructuur			
• IT-servicedeskagent:	€ 2.782	€ 3.246	€ 3.565
• IT-support engineer:	€ 3.056	€ 3.692	€ 4.456
• Systems engineer:	€ 3.589	€ 4.584	€ 5.729
• Network engineer:	€ 4.072	€ 5.220	€ 6.126
• Service delivery manager:	€ 4.703	€ 5.729	€ 6.247
4. IT-management			
• IT-coördinator:	€ 4.028	€ 4.769	€ 5.197
• IT-manager:	€ 5.811	€ 6.747	€ 7.639
• Application manager:	€ 5.937	€ 6.875	€ 8.822
• IT-director:	€ 7.670	€ 8.912	€ 10.822
5. Project- en productmanagement			
• IT-projectmanager:	€ 4.454	€ 5.729	€ 6.875
• PMO-manager:	€ 6.429	€ 7.384	€ 8.657
• Product owner:	€ 4.193	€ 5.428	€ 6.170
• Productmanager:	€ 5.353	€ 6.065	€ 6.796
6. Softwareontwikkeling			
• Softwaredeveloper:	€ 4.029	€ 4.584	€ 5.474

Bron: Robert Half, Salarisgids 2026
Het gaat om gemiddelde bruto-maandsalarissen in België. Er werd geen rekening gehouden met bonussen, voordelen en andere compensatievormen. Door de salarissen te vermenigvuldigen met 13,92 bereken je doorgaans het bruto-jaarsalaris per functie.

De UGent (foto 1: Tech Lane Ghent Science Park), KU Leuven (foto 2: het Arenbergkasteel in Heverlee) en Université de Liège (foto 3: Campus Sart-Tilman).

VAN LAB NAAR MARKT

BELGISCHE SPIN-OFFS BLOEIEN ALS NOOIT TEVOREN

In de afgelopen 25 jaar is het aantal universitaire spin-offs verzesvoudigd, zo blijkt uit onderzoek van hardwareontwikkelaar Comate. De meeste spin-offs zijn actief in sectoren als biotech, medtech, industriële technologie, ICT en energie en software, met AI op kop.

Zo'n spin-off is een nieuw bedrijf dat ontstaat uit een bestaande organisatie, zoals een universiteit, onderzoeksinstelling of groot bedrijf. Ze zetten veelbelovend wetenschappelijk onderzoek om in commerciële toepassingen. Zo creëren ze nieuwe jobs, economische groei en technologische innovatie. "Beloftevolle onderzoeksresultaten moeten de stap kunnen maken naar schaalbare producten. Spin-offs zijn daarbij essentieel, omdat ze een belangrijke brug slaan tussen onderzoek en innovatie", stelt Sander Van den Dries, director bij Comate.

Simon De Corte, spin-offadviseur bij UGent.

De UGent, KU Leuven en Université de Liège zijn samen goed voor bijna 60 procent van alle spin-offs, maar ook kleinere instellingen zoals UCL, UAntwerpen, UHasselt, UMons en UNamur dragen stevig bij. Tussen 2000 en 2025 zagen 641 nieuwe universitaire spin-offs het levenslicht.

SAMENWERKING

Bij de universiteiten zelf is de aanpak de laatste jaren veranderd, vertelt Simon De Corte, spin-off-adviseur bij UGent. "Waar spin-offs vroeger voornamelijk reactief ontstonden op initiatief van onderzoekers die toevallig ervaring hadden in ondernemen of zelfs externe ondernemers, hanteren we nu een proactieve strategie", vertelt hij. "We scouten actief naar technologieën met marktpotentieel en potentiële ondernemers binnen de universiteit, en kijken ook nadrukkelijk naar de onderzoekers zélf."

Ook Rudi Cuyvers, hoofd van de afdeling Spin-off & Innovatie bij KU Leuven Research & Development, benadrukt het belang van samenwerking: "Naast de universiteiten en onderzoekscentra, spelen ook het bedrijfsleven, de financiële sector en de overheid een belangrijke rol in het succes van spin-offs. Het is een én-énverhaal."

641
universitaire spin-offs opgericht tussen 2000 en 2025

POTENTIEEL

De verzesvoudiging van het aantal spin-offs toont het enorme potentieel van Belgisch onderzoek, maar volgens Sander Van den Dries is dit pas het begin: "Er is een enorm potentieel aan onderzoek dat via spin-off-creatie zijn weg naar de markt zou kunnen vinden. Juist in deze onzekere tijden is het cruciaal om de stap naar innovatie te versnellen."

SAI NEXT TECHNOLOGY GENERATION

DE TOEKOMST VAN IT IN 6 TRENDS

Voor dit SAI NXT-dossier dienden vooraanstaande onderwijsinstellingen – van AP Hogeschool en KU Leuven tot Universiteit Hasselt en VIVES – hun beste IT-onderzoek en -eindwerken in. Een staalkaart van waar technologie vandaag naartoe evolueert.

1/ AI IS OVERAL

Artificial intelligence vormt zonder twijfel de rode draad in de young talent-inzendingen. Driekwart heeft een uitgesproken AI-invalshoek. Het doordringt ook elk IT-domein: van een AI-tool die oude software begrijpt (p. 28) tot eentje om veilige infrastructuurcode te genereren (p. 24). Zelfs in het dagelijkse leven, met bijvoorbeeld een tool voor speelpleinwerking (p. 26). Wat het internet dertig jaar geleden was, is AI voor de generatie van nu.

2/ LERENDE DATASYSTEMEN ALS NORM

Data science verschuift van verzamelen naar continu verbeteren. Van MLOps-pipelines (p. 18) die modellen automatisch hertrainen bij nieuwe data, tot PU Learning (p. 20) dat aantoont hoe AI kan leren uit onvolledige datasets. Ook de multi-agent-aanpak (p. 17), waarbij meerdere AI-modellen elkaars uitspraken controleren om desinformatie tegen te gaan, past in deze trend.

3/ DE CLOUD IS HYBRIDE

In verschillende projecten wordt gezocht naar centrale technologie. Cloud en on-premises raken steeds nauwer met elkaar verweven. Het onderzoek naar AKS op Azure Stack HCI (p. 22) toont aan dat hybride omgevingen kosten drukken en data-soevereiniteit versterken. De toekomst ligt in hybride cloudstrategieën die flexibiliteit, compliance en kostenefficiëntie combineren. Open source is ook een belangrijke pijler.

4/ SECURITY SLIMMER EN PERSOONLIJKER

Beveiliging is niet langer puur reactief. Self-Sovereign Identity (p. 32) geeft gebruikers cryptografische controle over hun identiteit, terwijl malwaredetectie via machine learning (p. 34) afwijkend gedrag leert herkennen zonder dure tools.

5/ DUURZAAMHEID ALS IT-PRINCIPE

Het project rond Green Enterprise Architecture (p. 30) toont aan dat milieubewustzijn in de kern van de digitale transformatie thuishoort. Door duurzaamheid in elke laag van enterprise-architectuur te verankeren, wordt ecologische impact een ontwerpcriterium.

6/ TECHNOLOGIE MET MAATSCHAPPELIJKE BETEKENIS

AP Terra (p. 14) gebruikt Internet of Things en AI om overstromingen in Oeganda te voorspellen en zo mensenlevens te redden. De Speelplein Assistent helpt bij de ontspanning van kinderen. De nieuwe generatie koppelt innovatie aan sociale impact – van klimaatadaptatie tot inclusieve digitale tools.

HOE GINGEN WE TE WERK?

We namen contact op met twaalf universiteiten, hogescholen en onderwijsinstellingen met de vraag om hun meest spraakmakende IT-eindwerken en -projecten te bezorgen. Deze inzendingen werden door de redactie doorgenomen en verwerkt, in samenspraak met de auteurs en promotoren. Uiteindelijk stapten zeven organisaties mee in ons (en hun) verhaal: AP Antwerpen, INNOCOM, KdG, KU Leuven, PXL, Universiteit Hasselt en VIVES.

De eerste installatie van AP Terra vond plaats in Oeganda, waar het systeem nu waardevolle realtime klimaatgegevens levert.

TECHNOLOGIE TEGEN HET WATER

HOE AI EN IOT DE STRIJD TEGEN OVERSTROMINGEN IN OEGANDA ONDERSTEUNEN

Overstromingen treffen steeds vaker kwetsbare regio's in het Globale Zuiden, waar betrouwbare klimaatgegevens schaars zijn. Met AP Terra ontwikkelden studenten van AP Hogeschool een autonoom IoT-platform dat lokale gemeenschappen in staat stelt om zelf weer- en rivierdata te verzamelen en te analyseren. Het project toont hoe AI, automatisering en internationale samenwerking samen technologie met maatschappelijke impact creëren.

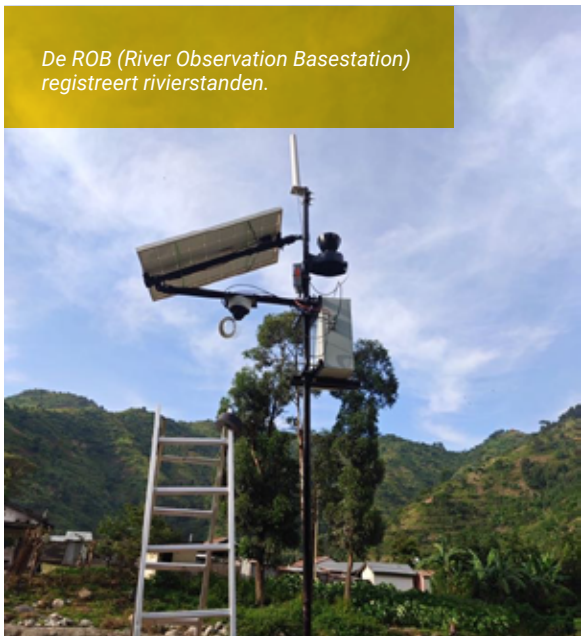
Vanuit de nood aan betrouwbare waarschuwingssystemen ontwikkelde het project B-SaFFeR (Building socio-ecological Awareness for Flood Emergency Response) het platform AP Terra: een modulair systeem dat lokale gemeenschappen helpt om klimaatgegevens te verzamelen, te analyseren en te delen.

AP Terra is een IoT-platform dat met betaalbare sensoren en camera's weer- en rivierdata verzamelt. Twee kernmodules vormen de basis: de WIM (Weather Integrated Module) meet temperatuur, luchtdruk, vochtigheid en neerslag, terwijl de ROB (River Observation Basestation) rivierstanden registreert. De data worden verzonden via het lichtgewicht MQTT-protocol en verwerkt op energiezuinige hardware. Via een webdashboard kunnen gebruikers zonder technische kennis lokale klimaattrends opvolgen.

DATACAPTATIE, VISUALISATIE EN OPSLAG

Studenten van AP Hogeschool Antwerpen namen een sleutelrol op in het ontwerp en de automatisering van AP Terra. Ze zorgden ervoor dat het platform grotendeels autonoom functioneert en minimaal onderhoud vraagt. De automatische dataverzameling via IoT-integraties garandeert een continue stroom van meetgegevens, terwijl slimme waarschuwingsfuncties onmiddellijk een melding sturen bij een systeemuitval. Het live dashboard, ontwikkeld door AP, maakt de data realtime zichtbaar, zelfs bij een beperkte internetverbinding.

De WIM (Weather Integrated Module) meet temperatuur, luchtdruk, vochtigheid en neerslag.



De ROB (River Observation Basestation) registreert rivierstanden.

Daarnaast ontwierpen de studenten een efficiënt systeem voor dataretentie en opslagbeheer, zodat gegevens veilig bewaard en snel raadpleegbaar blijven. Omdat veel pilootlocaties geen stabiele energievoorziening hebben, werd een zonne-energiemodule geïntegreerd die een off-grid werking mogelijk maakt. Dankzij het energiezuinige ontwerp en het hergebruik van lokale onderdelen daalden de operationele kosten aanzienlijk, een essentiële voorwaarde voor toepassingen in kwetsbare regio's.

AI EN BEELDHERKENNING VOOR RISICODETECTIE

Naast sensoren worden camera's ingezet. "Het systeem gebruikt beeldanalyse om op basis van videobeelden de stromingsdynamiek van rivieren te berekenen", vertelt Hakim Ghanoudi, praktijk lector bij AP en betrokken bij het project.

FLOW

Camera → Raspberry Pi → LTE Router → AP-Terra

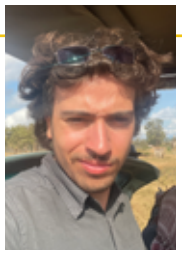
"AP Terra is een IoT-platform dat met betaalbare sensoren en camera's weer- en rivierdata verzamelt."

Zo kunnen stroomsnelheden en veranderingen in waterbeweging nauwkeurig gemonitord worden. "Door deze visuele informatie te koppelen aan sensordata ontstaat een krachtig hulpmiddel om riviergedrag te analyseren en lokale waarschuwingssystemen te verbeteren."

De eerste installatie van AP Terra vond plaats in Oeganda, waar het systeem nu waardevolle realtime klimaatgegevens levert. Het platform vormt de datalaag waarop toekomstige *early warning*-systemen kunnen bouwen, bijvoorbeeld via sms-alerts of mobiele notificaties. Zo groeit AP Terra uit tot een fundament voor digitale klimaatactie. Ervoor werd alles er manueel gedaan.

INTERNATIONALE SAMENWERKING

Het project verenigde partners uit verschillende landen en onderwijsniveaus: AP Hogeschool Antwerpen, Vrije Universiteit Brussel, TU Delft en de Oegandese universiteiten MMU en UMU. Die brede samenwerking zorgde voor kennisuitwisseling tussen graduaatsstudenten, bachelors en onderzoekers, en voor oplossingen die zowel technisch als contextueel relevant zijn.



Titel eindwerk: B-SaFFeR en AP Terra: klimaattechnologie en AI voor het Globale Zuiden

Auteur: Hakim Ghanoudi (AP Hogeschool Antwerpen)

Instelling: AP Hogeschool Antwerpen, Vrije Universiteit Brussel, TU Delft, UMU en MMU

Waarom dit eindwerk bijzonder is

Dit project toont hoe AI, IoT en onderwijsinnovatie kunnen samenkomen om een tastbare maatschappelijke impact te realiseren. AP Terra bewijst dat digitale innovatie, als ze open en inclusief wordt ontworpen, een verschil kan maken waar de (waters)nood het hoogst is.

Key takeaways

- Modulair IoT-platform voor klimaatmonitoring
- Twee standaardmodules: WIM (weerstation) en ROB (rivierobservatie)
- Dataoverdracht via MQTT en opslag op lichte hardware
- Live dashboard en automatische dataretentie
- AI en beeldherkenning in ontwikkeling
- Zonne-energie en lage operationele kosten
- Pilootproject in Oeganda

WHEN AIS CHECK EACH OTHER

A MULTI-AGENT APPROACH TO FACT-CHECKING

In an era where misinformation spreads faster than facts, the demand for reliable fact-checking tools has never been greater. As a part of his master's studies at UHasselt, Xander Vervaecke developed LieSpy.ai, a fact-checking system powered by a multi-agent AI architecture. His tool demonstrates how multiple large language models (LLMs) can collaborate, challenge one another, and ultimately converge on the truth.

The process begins when a user enters a claim – for instance, "Obama's birth certificate is fake." The system first analyzes whether the claim can be fact-checked and breaks down compound statements into individual components. Then, it gathers information from multiple online sources, each assigned a trustworthiness score based on their reputation. A site like FactCheck.org might score 9/10, while a conspiracy blog could receive only 2/10.

MULTI-MODEL

At this stage, several AI models – such as GPT, Gemini and Mistral – are deployed. Each independently evaluates the claim using the gathered evidence and produces its own verdict on a true-to-false scale. The outcomes are then aggregated into a single verdict that reflects both consensus and confidence levels.

The approach is: don't rely on a single AI model, but on collaboration and comparison between multiple agents.

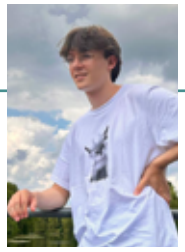
What sets LieSpy.ai apart is that it doesn't rely on a single AI model but on collaboration and comparison between multiple agents. "The fact-checker externalizes the confidence of each model and combines their findings into one coherent verdict," explains Vervaecke. This layered approach ensures that biases or inaccuracies from one model can be balanced out by others, making the system more robust and transparent.

TRANSPARENCY

LieSpy.ai's interface not only provides a final answer but also reveals how that answer was reached. Users can inspect each model's reasoning, see the evidence it relied upon, and view the relevance of each source. This level of transparency transforms the tool from a black box into a learning instrument for journalists, researchers, and policymakers seeking to understand AI reasoning.

Currently, LieSpy.ai supports three large language models, but expansion is on the horizon. Future versions will feature cross-validation, allowing AIs to evaluate one another's reasoning. The system will also handle time-sensitive queries more effectively, which struggle with questions like "Who is the current pope?" as world events change.

Looking ahead, Vervaecke plans to integrate image and video analysis into the system to verify visual content such as deepfakes. This would transform LieSpy.ai from a text-only fact-checker into a multimodal verification platform capable of evaluating text, images, and video in unison. "The approach works just as well for more complex or challenging questions,", notes Vervaecke, underscoring the system's potential beyond simple factual checks.



Thesis title: Fact Checker with Multi-Agent Approach

Author: Xander Vervaecke

Institution: Hasselt University (UHasselt)

Why this thesis stands out

LieSpy.ai redefines fact-checking by introducing a self-reflective AI ecosystem where multiple models cooperate to establish truth.

Key takeaways

- Multi-agent collaboration: multiple AI models verify claims independently and compare their findings.
- Transparent reasoning: users can see how reliable sources are and how each model formed its verdict.
- Cross-validation and multimodality: future iterations will allow AIs to evaluate each other and analyze images or videos.
- Educational and ethical impact: LieSpy.ai bridges the gap between AI performance and human understanding.

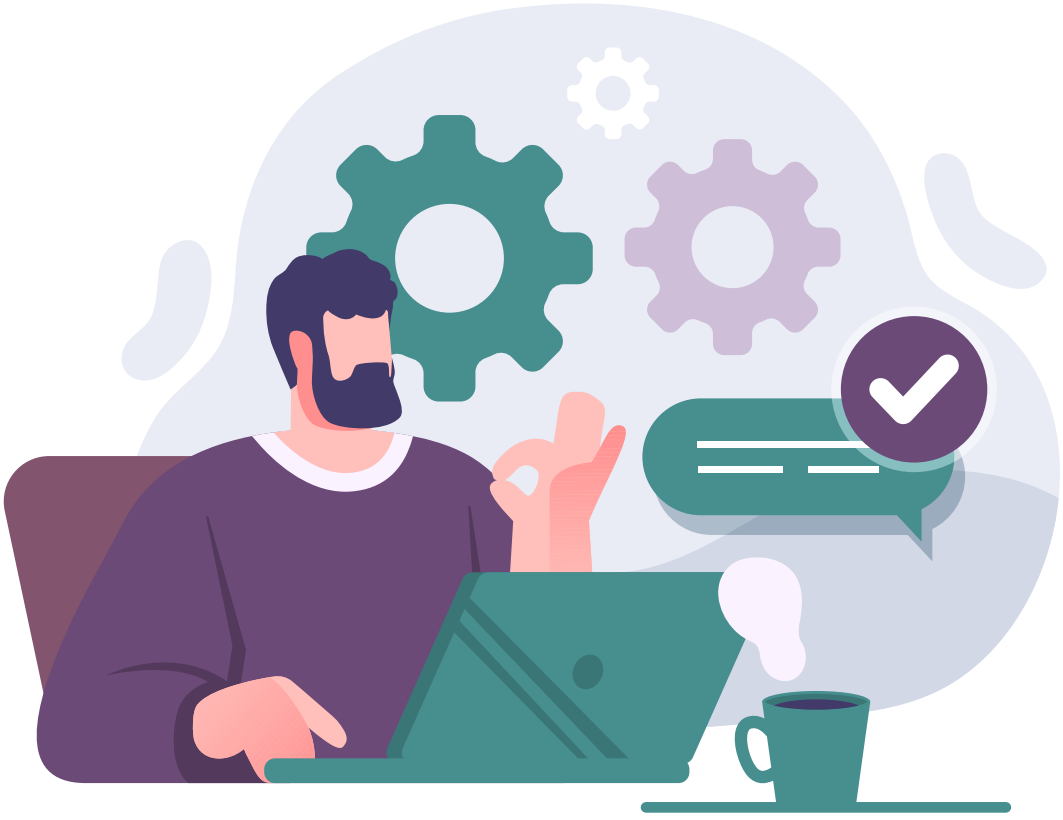
WANNEER AI ZICHZELF VERBETERT

OPEN-SOURCE MLOPS IN ACTIE

Bedrijven draaien vandaag meer dan ooit op data. Maar zelfs de slimste machinelearningmodellen verliezen na verloop van tijd hun scherpte. Wanneer de onderliggende data veranderen, verschuiven ook de voorspellingen en daarmee de bedrijfswaarde.

Precies dat probleem pakte Stijn Hilkens, student aan PXL, aan tijdens zijn stage bij de Limburgse data-adviseur DataSense, een consultancybedrijf dat zich richt op data-integratie, analytics en machinelearningoplossingen.

Zijn project bewijst dat het mogelijk is om een volledig geautomatiseerde, open-source MLOps-pipeline te bouwen voor het detecteren van anomalieën in multivariate tijdreeksdata – inclusief herkenning van *model drift* en automatische hertraining.



"Het komt erop aan te bewijzen dat AI zichzelf kan verbeteren zonder tussenkomst van een data scientist", legt Stijn Hilkens uit. "Door monitoring, detectie en hertraining te automatiseren, blijft het model accuraat, ook wanneer de werkelijkheid verandert."

MLOps (Machine Learning Operations) is de discipline die het ontwikkelproces van machinelearningmodellen beheert en automatiseert – van dataverzameling en training tot uitrol en onderhoud. Ze brengt de principes van DevOps naar de wereld van AI. Een MLOps-pipeline is een geautomatiseerde keten die dit proces uitvoert.

VAN DATASTREAM NAAR BESLISSINGSONDERSTEUNING

Binnen DataSense ontwierp Hilkens een end-to-end proof of concept waarin data-engineering, machinelearning en DevOps samenkomen.

Het is mogelijk om een volledig geautomatiseerde, open-source MLOps-pipeline te bouwen voor het detecteren van anomalieën in multivariate tijdreeksdata.

De pipeline streamt tijdreeksdata via Apache Kafka (real-time datastreaming), bewaart resultaten in PostgreSQL (een relationele open-source database) en orkestreert alle taken met Apache Airflow (workflow-orchestratie).

Elke modelversie wordt opgevolgd via MLflow (een platform voor het beheren en volgen van machinelearning-experimenten), verpakt in Docker (containertechnologie die applicaties en hun afhankelijkheden isoleert), uitgerold met Kubernetes (orchestratieplatform voor het beheren van containers op schaal). De modellen worden ook automatisch opnieuw getraind wanneer nieuwe data of code beschikbaar zijn. "Zo wordt machinelearning een continu proces, van dataverzameling tot productie", zegt hij.

MODEL DRIFT AUTOMATISCH BESTRIJDEN

De grootste innovatie ligt in de automatische detectie van model drift – het fenomeen waarbij een model slechter presteert door veranderende datapatronen.

Met behulp van de Alibi Detect-bibliotheek (een open-source toolkit voor het opsporen van afwijkingen en model drift) en het Kolmogorov–Smirnov-algoritme (een statistische test die verschillen tussen dataverdelingen meet) wordt die drift automatisch herkend.

Wanneer prestatieverlies wordt vastgesteld, activeert Airflow automatisch een hertraining. Daarna vergelijkt het nieuwe model zich met de vorige versie aan de hand van aangepaste evaluatiemetrieken en rolt het – bij betere resultaten – automatisch uit via een CI/CD-pipeline (*Continuous Integration / Continuous Delivery*, de geautomatiseerde keten die nieuwe code of modellen voortdurend test, integreert en uitrolt). Dankzij de Docker-containerarchitectuur is dit geheel inzetbaar in de cloud of on-premise.

TESTEN, FLEXIBILITEIT EN HERBRUIKBAARHEID

Om realistische omstandigheden te simuleren, genereerde Stijn Hilkens multivariate sensordata met seizoens- en trendpatronen via GutenTAG, de tool voor het genereren van gesimuleerde tijdreeksdata met realistische patronen.

Verschillende anomaliedetectiemodellen en evaluatiemethoden, waaronder de Proximity Aware Time Series Evaluation (PATE), werden getest en vergeleken. Een belangrijk ontwerpprincipe was modulariteit. "Zowel het model als de databron kunnen eenvoudig vervangen worden zonder de architectuur aan te passen", stelt Hilkens. Mede dankzij het gebruik van uitsluitend open-source-technologieën is de oplossing flexibel inzetbaar, van industriële omgevingen tot IoT-toepassingen.

Titel eindwerk:
Opensource MLOps voor tijdreeksstreaming

Auteur: Stijn Hilkens

Instelling: Hogeschool PXL Hasselt

Waarom dit eindwerk bijzonder is
Autonome MLOps op basis van open-source-componenten is niet alleen theoretisch, maar ook praktisch haalbaar. Real-time monitoring en zelfcorrigerende hertraining is mogelijk, zonder afhankelijk te zijn van commerciële platforms.

Key takeaways
- Volledig geautomatiseerde ML-pipeline voor anomaliedetectie in multivariate tijdreeksen.
- Gebouwd met opensourcetools: Kafka, Airflow, MLflow, Docker, Kubernetes en PostgreSQL.
- Detectie van model drift via Alibi Detect en Kolmogorov–Smirnov.
- Automatische hertraining en heruitrol via CI/CD.
- Draaibaar op lokale hardware én in de cloud.

POSITIVE–UNLABELLED (PU) LEARNING

GRAPHS, ANOMALIES, AND THE ART OF LEARNING WITH INCOMPLETE INFORMATION

In the fast-evolving landscape of data science, the ability to learn from incomplete or uncertain data has become a challenge. Positive–unlabelled (PU) learning offers a promising solution: it trains algorithms to make reliable predictions even when only partial truth is known.

In many applications, crucial information is missing: a few fraudsters hide among millions of legitimate transactions, rare diseases go unrecorded in medical data and online communities form long before anyone notices them. Traditional algorithms that learn from clear examples of both good and bad cases are often unreliable and fail in these messy, incomplete realities.

ENTER PU LEARNING

That's where positive–unlabelled (PU) learning comes in. Instead of relying on perfect data, PU learning assumes we only know some of the positives, confirmed fraud cases for instance, while the rest of the data is unlabelled. Some of those unlabelled cases may also be fraudulent, but we can't directly observe them. Training reliable models under such uncertainty remains an ongoing challenge in modern data science.

A recent thesis named *Scalable Two-Step Imbalanced PU Learning with Graph Neural Networks* by Matthias Aerts and Romain Bérard addresses this challenge. The thesis

combines two exciting ideas in machine learning: graph neural networks (GNN) and anomaly detection.

Graphs allow computers to reason about relationships. They capture the notion of who trades with whom, which papers cite each other, which node is the central node in a network or how information flows through a social network. The iconic idea of PageRank is built on top of Graph Theory. In Machine Learning, graph applications have become very popular. The most common application of this field is a GNN. This is a neural network that can perform all the functions of a regular neural network, but on graphs. A celebrated application of a GNN is Deepmind's AlphaFold which predicts protein 3D structure from its amino acid sequence, the elementary protein building blocks.

MATHEMATICAL SPACE

In this thesis, GNNs are used not for biology but for financial and relational data. In short, a GNN transforms a complex web into a mathematical space where similar nodes, for instance users with comparable behavior, are positioned close together.

This mathematical or latent space is a lower-dimensional representation of the network. The latent space is a commonly used concept in machine learning to extract the most dominant features of data. First, the raw graph is processed to obtain the representations of nodes in the latent space. This low dimensional representation summarizes its local graph structure and features. To achieve this, a GraphSAGE-inspired architecture based on mini-batch training and sampling strategies is used. This means that the method can be used for large network sizes.

NEAREST-NEIGHBOUR ISOLATION FOREST

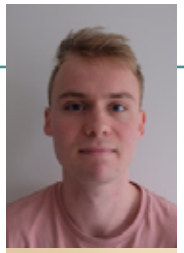
To filter out suspicious or ambiguous cases from these large graphs, the method uses a Nearest-Neighbour Isolation Forest. This technique is a combination of two data science techniques: Nearest-Neighbour and Isolation Forests. Isolation Forests use the premise that anomalous data points are easier to separate from the rest of the sample. The Nearest-Neighbour method exploits the possibility that fraudsters tend to occur in groups. In essence, fraudsters or anomalies are more separate from the usual behaviour and might come in groups. This yields a set of suggested positives and negatives. It leads to a cleaner dataset without needing to know how many bad actors exist.

The second step is then to use the node embeddings from GraphSage and the earlier obtained positives and reliable negatives to learn to predict which other nodes are positive among the unlabelled ones. This is done by XGBoost which draws the final line between whether nodes are likely positive or negative.

Graphs allow computers to reason about relationships.

IT PERSPECTIVE

From an IT perspective, this research opens up powerful new avenues. Its scalable design means it can process networks with hundreds of thousands of nodes, making it practical for deployment in operational environments. Think of financial institutions detecting illicit transactions in real time, or cybersecurity platforms identifying compromised devices before damage spreads.



Thesis title: Scalable Two-Step Imbalanced PU Learning with Graph Neural Networks

Authors: Matthias Aerts & Romain Bérard

Institution: KU Leuven

Why this thesis stands out
Aerts and Bérard's work bridges a gap between academic machine learning and enterprise-scale IT applications. It is an illustration of how intelligent systems can learn from incomplete data, adapt to complex relationships, and scale to the real world. It's a major step toward more robust, data-driven infrastructures in finance, healthcare, and beyond.

Key takeaways
- PU learning enables reliable predictions when only partial ground truth is available.
- Graph Neural Networks transform complex relational data into learnable structures.
- The two-step approach (anomaly filtering + classification) scales to enterprise-sized graphs.
- Applicable to fraud detection, cybersecurity, and healthcare analytics where data is incomplete.

AZURE KUBERNETES SERVICE ON AZURE STACK HCI

DE TOEKOMST VAN HYBRIDE CONTAINERS

Steeds meer organisaties verplaatsen hun IT-infrastructuur naar een hybride model, waarin de voordelen van de publieke cloud worden gecombineerd met de controle van on-premises systemen. Containertechnologie speelt daarbij een sleutelrol: applicaties worden losgekoppeld van de onderliggende infrastructuur en kunnen daardoor sneller uitgerold, opgeschaald en beheerd worden.

"De initiële installatie van Azure Stack HCI en AKS vereist aanzienlijke technische kennis."

Binnen dit kader onderzocht Michiel Verhoye tijdens zijn stage bij Savaco de prestaties en het beheer van Azure Kubernetes Service (AKS) op Azure Stack HCI, Microsofts lokale cloudplatform dat de brug slaat tussen het datacenter en Azure.

KUBERNETES

De overstap naar containerisatie en hybride cloudarchitecturen is niet louter een technologische trend, maar een noodzakelijke stap in de evolutie naar flexibele en schaalbare IT-systemen. Containers – geïsoleerde runtime-omgevingen die applicatiecode, libraries en configuraties bundelen – zorgen voor consistentie over verschillende infrastructuren. In combinatie met Kubernetes, de industriestandaard voor containerorkestratie, kunnen organisaties workloads dynamisch beheren en automatisch schalen.

Tijdens zijn stage bij Savaco, een Belgische IT-dienstverlener gespecialiseerd in hybride cloudoplossingen, richtte Michiel Verhoye zich op het implementeren en analyseren van AKS binnen een Azure Local-omgeving. De studie bekeek hoe containergebaseerde applicaties zich gedragen in een hybride infrastructuur, met aandacht voor prestaties, schaalbaarheid en kosten. "Door AKS on-premises uit te rollen op Azure Stack HCI kun je de voordelen van containerisatie benutten zonder volledig afhankelijk te worden van publieke cloudinfrastructuur", luidt het achterliggende idee.

CONTAINERS EN HYBRIDE BEHEER IN DE PRAKTIJK

De praktische testopstelling bestond uit twee fysieke servers waarop Azure Stack HCI draaide. Hierop werd een AKS-cluster uitgerold met drie nodes (elk 8 vCPU's en 32 GB RAM), vergelijkbaar met een middelgrote productieomgeving. Dankzij deze setup kon het onderzoek reële belastingscenario's simuleren en de grenzen van de infrastructuur aftasten.

Via custom deploymentbestanden werden stresstests uitgevoerd die verschillende soorten workloads genereerden, van lichte microservices

tot compute-intensieve taken. De prestaties werden gemeten met LogicMonitor, een krachtige observability-oplossing waarmee CPU-, geheugen- en netwerkverbruik in real time werden gevolgd.

CLUSTERS BEHEREN

Uit de resultaten bleek dat de lokale AKS-omgeving stabiel presteerde, met een consistente respons onder variabele belasting. De pod-scheduling- en autoscaling-mechanismen reageerden adequaat, wat wijst op een goed geïntegreerde implementatie van Kubernetes binnen Azure Stack HCI.

Een bijkomend voordeel van deze hybride opzet is de integratie met Azure Arc, waarmee beheerders on-premises clusters rechtstreeks via het Azure-portaal kunnen beheren. Zo kun je vanuit één dashboard zowel lokale als cloudgebaseerde workloads monitoren, policies toepassen en updates automatiseren. Voor organisaties met strikte data residency-eisen of lage latency-behoeften biedt dit model een duidelijke meerwaarde.

PRESTATIES, KOSTEN EN STRATEGISCHE KEUZES

Verhoye vergeleek de operationele kosten tussen Azure Local en Azure Cloud. De lokale setup kostte omgerekend ongeveer 500 euro per maand, gebaseerd op een investering van 30.000 euro over vijf jaar. Een identieke configuratie in de publieke cloud kwam uit op ruim 1.097 euro per maand. Deze berekening benadrukt het kostenvoordeel van een hybride of lokale uitrol, zeker bij continue workloads met voorspelbare belasting.

Toch zijn er enkele aandachtspunten. De initiële installatie van Azure Stack HCI en AKS vereist aanzienlijke technische kennis. De configuratie van networking, node pools en persistent storage bleek complexer dan verwacht, vooral bij integratie met bestaande on-premises netwerken. “Hoewel de lokale oplossing financieel voordeliger is, blijft de initiële installatie complex en vereist deze aanzienlijke kennis van zowel Azure Stack HCI als Kubernetes”, stelt Michiel Verhoye.

Daarnaast is er het vendor lock-in-argument: organisaties blijven afhankelijk van Microsofts ecosysteem voor licenties, updates en compatibiliteit. Voor bedrijven die een multi-cloudstrategie nastreven, kan dit de flexibiliteit beperken.

NAAR EEN VOLWASSEN HYBRIDE CLOUDSTRATEGIE

De studie toont aan dat AKS op Azure Stack HCI een technisch stabiele en kostenefficiënte oplossing biedt voor organisaties die willen experimenteren met containerisatie zonder hun infrastructuur volledig naar de cloud te verplaatsen. Tegelijk maakt ze duidelijk dat hybride cloudbeheer een doordachte strategie vereist, met aandacht voor monitoring, beveiliging, lifecyclemanagement en kennisopbouw.

Het implementatieproject bij Savaco biedt een waardevolle blauwdruk: het demonstreert hoe lokale infrastructuur geïntegreerd kan worden met cloud-native tools en hoe organisaties realistische performantie- en kostenanalyses kunnen uitvoeren voordat ze grootschalig migreren.

VAN 1.097 EURO NAAR 500 EURO: LOKAAL HALVEERT DE PRIJS

Een opvallende conclusie uit het onderzoek van Michiel Verhoye is het verschil in operationele kosten. De lokale Azure Stack HCI-omgeving kwam neer op ongeveer 500 euro per maand, gebaseerd op een investering van 30.000 euro over vijf jaar.

Een identieke configuratie in Azure Cloud kostte ruim 1.097 euro per maand. Zo’n lokale of hybride uitrol, die dus flink goedkoper kan zijn, is vooral interessant bij continue workloads met voorspelbare belasting.

Titel eindwerk: Azure Kubernetes Service on Azure Stack HCI: De toekomst van hybride containers

Auteur: Michiel Verhoye

Instelling: Hogeschool VIVES – Campus Kortrijk

Waarom dit eindwerk bijzonder is

Dit eindwerk vertaalt een abstract concept – hybride containerbeheer – naar een concreet, getest en financieel onderbouwd scenario. Het biedt zowel technische diepgang als praktische inzichten die relevant zijn voor IT-beslissers en cloudarchitecten.

Key takeaways

- AKS op Azure Stack HCI biedt cloudgebaseerd beheer met behoud van lokale controle en lage latency.
- Performantie en kostenefficiëntie: lokaal draaien van AKS kan prijsefficiënter zijn dan bij gebruik van de Azure Cloud.
- Aandachtspunten: complexe setup, vereiste technische expertise en afhankelijkheid van Microsofts ecosysteem.

SKYPIA

AI THAT MAKES TERRAFORM SMARTER AND SAFER

Infrastructure as Code (IaC) and cloud environments are the backbone of modern IT, yet developers and infrastructure engineers still face daily challenges with faulty or insecure Terraform configurations.

The Skypia project explores whether a specialized, fine-tuned large language model (LLM) can deliver better and safer Terraform suggestions for the AzureRM provider – and whether such a system can be effectively deployed for engineers in real environments.

FROM FINE-TUNING TO GROUNDED INTELLIGENCE

The idea started from a familiar pain point: generic LLMs often generate syntax errors, use outdated APIs, or miss crucial security best practices. To address this, the team experimented with various fine-tuning techniques – RLHF, PEFT/LoRA, and full fine-tuning – while building a high-quality dataset through scraping GitHub and Stack Overflow, supplemented with additional samples generated with Google's Gemini model.

The goal was to create an AI model that truly understands AzureRM and produces secure, compliant Terraform code that follows best practices.

However, during testing, fine-tuning turned out to be less effective than expected. The real progress came when the team pivoted to a Retrieval-Augmented Generation (RAG) approach. In this architecture, an always up-to-date

knowledge layer – in this case Terraform documentation accessed via Vertex AI Search – "grounds" the model's responses in real data. This combination of contextual retrieval and LLM reasoning reduces hallucinations and keeps the generated code aligned with the latest APIs and policies.

SMARTER WORKFLOWS, SAFER CODE

The resulting system provides a streamlined workflow: the user uploads a Terraform file, the LLM optimizes it. Terrascan performs automated compliance and security checks, and the model then refines its output based on those results.

Because no standard benchmark exists for Terraform on AzureRM, the team designed its own evaluation rubric, measuring relevance, clarity, security, and real-world viability. Testing showed clear performance gains for the RAG-based system.

How to create an AI model that produces secure, compliant Terraform code.

Additionally, running the solution locally – using the Belgian-deployed Gemini 2.0 Flash or even self-hosted models – ensures full GDPR compliance and strengthens data sovereignty for organizations handling sensitive infrastructure code.

WHAT'S NEXT?

Looking ahead, Skypia's roadmap includes a CLI tool for infrastructure engineers, GitLab integration for automated code reviews, and multi-cloud expansion to AWS and Google Cloud. The key takeaway from this project? For specialized infrastructure tasks, context-aware AI models – combining live documentation with targeted retrieval – outperform heavy fine-tuning in both accuracy and efficiency.

More info on: **https://medium.com/generative-ai/analyze-terraform-files-using-fine-tuned-llm-af94b39919f8**

Thesis title: Skypia: Improving Terraform Code with a Fine-Tuned LLM

Authors (left to right): Yevhen Zinenko, Josiane Popa, Leonid Romaniukha

Institution: Karel de Grote Hogeschool (KdG)

Why this thesis stands out

Skypia demonstrates that context- and document-driven LLMs (RAG + grounding) outperform purely fine-tuned models for Infrastructure as Code. The project bridges AI research and DevOps practice.

Key takeaways

- Goal: Improve the accuracy and security of Terraform (AzureRM) code using AI.
- Approach: Transitioned from fine-tuning to Retrieval-Augmented Generation (RAG) using Vertex AI Search grounding.
- Data: Combined scraping and Gemini-generated examples; explored LoRA optimization.
- Workflow: Upload > LLM optimization > Terrascan checks > refinement.
- Next steps: CLI tool, GitLab integration, multi-cloud support.

SPEELPLEIN ASSISTENT

HOE AI HET JEUGDWERK SLIMMER MAAKT

In tijden waarin generatieve AI zijn weg vindt naar bedrijfssoftware en productiviteitsplatformen, kan diezelfde technologie ook maatschappelijke meerwaarde creëren. De Speelplein Assistent toont aan hoe een goed ontworpen LLM-toepassing repetitieve taken automatiseert, contextueel redeneert en zich flexibel aanpast aan de noden.

Wie ooit mee een speelpleinweek heeft voorbereid, weet hoeveel tijd en creativiteit daarin kruipt. Voor Linsey Helsen, masterstudent informatica aan de universiteit Hasselt met een specialisatie in data en AI, is het ook een jaarlijks ritueel. “Speelplein zit echt in je bloed”, vertelt ze. “Maar de voorbereiding is vaak langdradig: spelletjes zoeken, aanpassen aan een thema en hopen dat je het juiste materiaal hebt.” Tijdens haar project voor het vak *Human-AI Interaction* aan de universiteit Hasselt ontwikkelde Linsey de Speelplein Assistent, een AI-toepassing die jeugdleiders ondersteunt bij de voorbereiding van thematische speelpleinweken. Het idee ontstond uit frustratie én enthousiasme: frustratie over repetitieve taken en enthousiasme over de mogelijkheden van grote taalmodellen (LLM’s) zoals Gemini. “Ik wilde een toepassing bouwen die het creatieve aspect van jeugdwerk versterkt, in plaats van het te vervangen.”

EEN SLIMME ASSISTENT MET VIER GEZICHTEN

De Speelplein Assistent bestaat uit vier samenwerkende modules. De spelgenerator is de **interface**: een zoek- en suggestietool die via filters (leeftijd, duur, intensiteit, locatie en thema) een passend spel selecteert uit een databank van meer dan 2.900 activiteiten van spelensite.be. Zodra het juiste spel gevonden is, zorgt de Gemini-API voor een thematische aanpassing, volledig afgestemd op het beschikbare materiaal. “Het grote verschil met ChatGPT is dat mijn assistent wéét welk materiaal het speelplein heeft. Zo worden de suggesties niet alleen creatief, maar ook uitvoerbaar.”

Daarnaast bevat de toepassing een **dagplanningsmodule**, waarin de structuur van een speelpleindag

wordt vastgelegd en gekoppeld aan de **chatbot**, en een digitale inventaris die alle beschikbare materialen bijhoudt. Het hart van de toepassing – en de vierde module – is de **thema-assistent**, een centrale chatbot die alle componenten verbindt. Die chatbot beslist autonoom welke tool ze moet aanroepen – bijvoorbeeld om een spel aan te passen of automatisch toe te voegen aan Google Calendar – en geeft contextueel correcte antwoorden op basis van de ingestelde planning.

TECHNOLOGIE ACHTER DE GLIMLACH

Achter de vrolijke interface schuilt een doordachte technische architectuur. Helsen maakte gebruik van Gemini 2.0 Flash als LLM, LangGraph om de verschillende tools met elkaar te verbinden en Streamlit (het framework voor snelle webinterfaces in Python) voor de gebruiksvriendelijke interface. De integratie met Google Calendar API zorgt ervoor dat gegenereerde activiteiten rechtstreeks ingepland kunnen worden.

Het grote verschil met ChatGPT is dat mijn assistent wéét welk materiaal het speelplein heeft.

Linsey Helsen toont met dit project aan hoe AI ook buiten de bedrijfswereld betekenisvol kan zijn. We denken bij AI vaak aan corporate toepassingen of automatisering, maar dit project bewijst dat het ook in vrijwilligerswerk een meerwaarde kan bieden.

Titel eindwerk: De Speelplein Assistent – een AI-toepassing ter ondersteuning van jeugdleiding

Auteur: Linsey Helsen

Instelling: Universiteit Hasselt

Waarom dit eindwerk bijzonder is

De Speelplein Assistent is een concreet voorbeeld van mensgerichte AI. Het toont hoe technologie vrijwilligers kan ondersteunen door repetitieve taken te automatiseren en ruimte te creëren voor wat echt telt: de beleving van kinderen.

Key takeaways

- AI-assistent voor speelpleinvoorbereiding met vier modules: spelgenerator, dagstructuur, inventaris en thema-chatbot.
- Gebouwd met Gemini, LangGraph, Streamlit en Google Calendar API.
- Slim gebruik van thematische prompting en lokale context (materiaal, planning).
- Autonome chatbot die tools aanroept op basis van gesprekscontext.

SMART CODE ANALYSIS

AI HELPT ONTWIKKELAARS OUDE CODE BEGRIJPEN

Wie ooit aan een oud softwareproject heeft gewerkt, weet hoe frustrerend het kan zijn: geen documentatie en ontbrekende context. De vraag 'Wat doet dit stukje code eigenlijk?' is dagelijkse kost voor ontwikkelaars.

Daar wilden drie studenten Toegepaste Informatica aan Karel de Grote Hogeschool iets aan doen. Hun project *Smart Code Analysis* onderzoekt hoe AI – en meer bepaald Large Language Models (LLM's) – kan helpen om complexe codebases te doorgronden, mét kennis van de bedrijfscontext waarin ze zijn geschreven.

De centrale onderzoeksvraag was: kan een lokaal draaiend AI-model met inzicht in de volledige codebasis én de businesscontext betere antwoorden geven dan een generieke cloudgebaseerde LLM zoals ChatGPT?

CODE DIE CONTEXT BEGRIJPT

Veel AI-tools begrijpen code technisch, maar missen de reden waarom ze ooit geschreven werd. Smart Code Analysis voegt daarom bedrijfscontext toe aan de AI: informatie over de werking, regels en doelstellingen van het systeem. Zo weet de AI bijvoorbeeld dat een *bunker*

operation in een havenapplicatie niet over bunkers gaat, maar over het bijtanken en onderhoud van schepen.

Die context wordt opgeslagen in Qdrant, een zogeheten vectordatabank die teksten omzet in numerieke representaties. Wanneer een ontwikkelaar een vraag stelt, zoekt de AI naar de meest relevante tekst- en codefragmenten in de databank. Vervolgens gebruikt de AI die context om een antwoord te formuleren dat niet alleen technisch klopt, maar ook zakelijk relevant is.

AI ONDER DE MOTORKAP

De technische ruggengraat van het project bestaat uit Python, *FastAPI* en *PydanticAI*. FastAPI is een Python-framework voor het bouwen van API's. PydanticAI is een uitbreiding van de Pydantic-bibliotheek voor datavalidatie. Volgens student Jarne Aerts was dat een bewuste keuze: "FastAPI is licht en performant, en met PydanticAI konden we de structuur van de AI-antwoorden afdwingen zodat de resultaten voorspelbaar en bruikbaar bleven."

Aan de AI-kant testte het team verschillende modellen: DeepSeek, Llama en uiteindelijk Qwen 2.5 van Alibaba. Dat laatste model bood de beste balans tussen snelheid, nauwkeurigheid en ondersteuning voor tools, wat essentieel is voor lokale AI-integraties. "Qwen bleek efficiënter en had een beter begrip van code dan we verwacht hadden", vertelt medeonderzoeker Rob Hellemans.

ALLES LOKAAL

Een belangrijk aspect van het project is dat alles lokaal draait via Ollama als lokale LLM-engine, waardoor gevoelige bedrijfsdata niet naar de cloud hoeven. Dat maakt de oplossing geschikt voor organisaties die strikte privacy- of compliance-eisen hebben.

Het systeem haalt niet de volledige codebase of documentatie op, maar alleen de meest relevante stukken. Daardoor krijgt de AI minder ruis en verkleint de kans op hallucinaties, verzonnen antwoorden. Door context slim te combineren met code, geeft het systeem antwoorden die beter aansluiten bij de reële werking van het programma.

RESULTATEN EN TOEKOMST

De tests tonen aan dat een contextbewuste, lokale LLM inderdaad meer relevante en correcte antwoorden geeft dan een generiek model. Door automatisch alle relevante contextinformatie aan te reiken, stijgt de nauwkeurigheid aanzienlijk. Toch blijkt uit de resultaten ook dat de lokale uitvoerbaarheid niet vanzelfsprekend is.

Kleinere modellen – zoals de varianten van Qwen met 7 tot 8 miljard parameters – kunnen op consumentenhardware draaien, maar vragen nog altijd veel rekenkracht en geheugen. Grotere modellen leveren merkbaar betere antwoorden, maar vereisen GPU's en opslagcapaciteit die zelden in standaard ontwikkelomgevingen beschikbaar zijn. Er is dus een duidelijke afweging tussen prestaties en toegankelijkheid: lokaal draaien garandeert privacy en controle, maar cloudmodellen blijven voorlopig efficiënter voor complexe analyses.

Veel AI-tools begrijpen code technisch, maar missen de reden waarom ze ooit geschreven is.

Zoals de studenten in hun conclusie samenvatten: "LLM's kunnen aanzienlijk beter worden zodra ze automatisch alle relevante context krijgen aangereikt. Lokaal draaien is haalbaar met kleinere modellen, maar de grootste kracht blijft voorlopig in de cloud."

Titel eindwerk: Smart Code Analysis – Unraveling codebases with AI

Auteurs: Jarne Aerts, Rob Hellemans & Seppe Van Hoof

Instelling: Karel de Grote Hogeschool

Waarom dit eindwerk bijzonder is
Smart Code Analysis toont hoe artificiële intelligentie evolueert tot een echte developer assistant die code begrijpt in haar functionele context. Het project koppelt academisch onderzoek aan praktische softwareontwikkeling.

Key takeaways
- AI met kennis van de bedrijfscontext begrijpt code veel beter dan generieke modellen.
- Qdrant, FastAPI en PydanticAI vormen de technische basis van het systeem.
- Qwen 2.5 levert sterke prestaties als lokaal LLM met toolondersteuning.
- Lokale verwerking via Ollama garandeert privacy en controle over data.

GREEN ENTERPRISE ARCHITECTURE

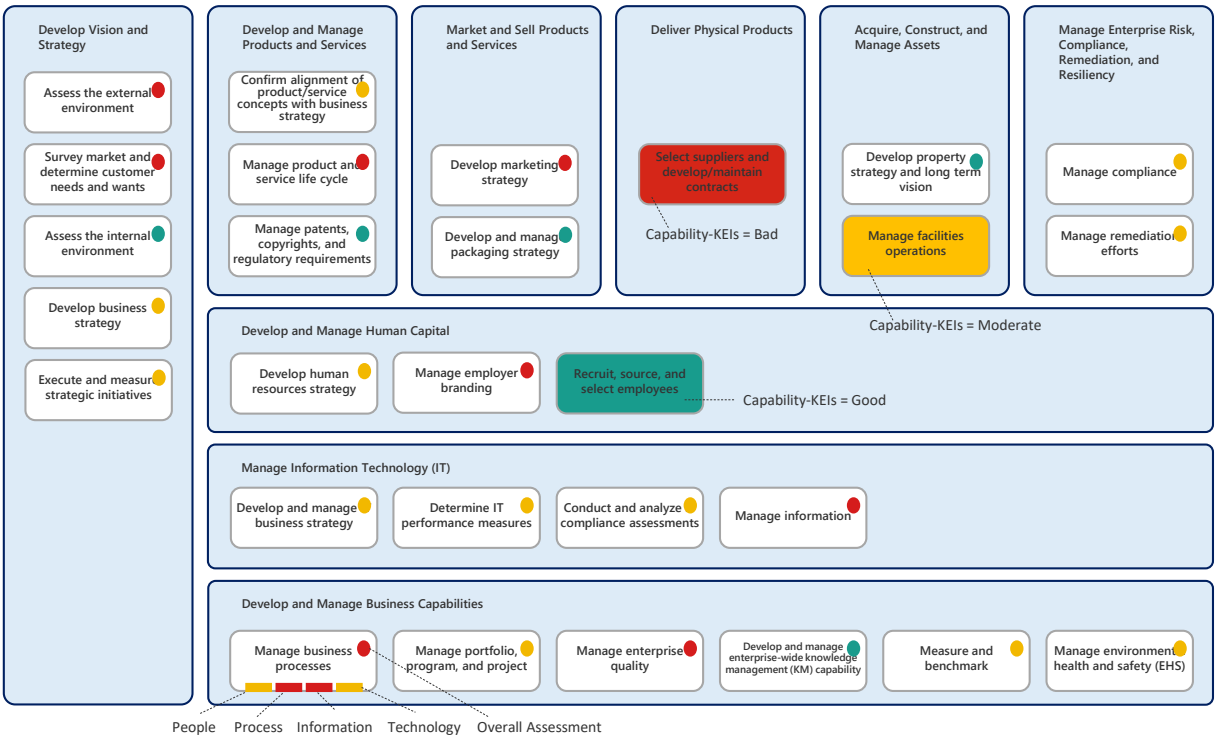
ALIGNING DIGITAL TRANSFORMATION WITH ENVIRONMENTAL SUSTAINABILITY

As organizations face increasing pressure from ESG regulations and stakeholder expectations, Green Enterprise Architecture (Green EA) offers a foundation for truly sustainable enterprise transformation.

Digital transformation (DT) has become an essential lever for innovation, efficiency, and competitiveness. Yet, as organizations embrace AI, cloud computing, IoT, and data-driven decision-making, one critical dimension is too often ignored: environmental sustainability (ES). Despite the potential of digital technologies to reduce waste and emissions, their growing energy demand and material footprint risk undermining global climate efforts.

In his master's thesis *Green Enterprise Architecture: Leveraging EA for Environmentally Sustainable Digital*

A generic example of an ES-aware business capability map combining a traditional dimension assessment (people, process, information, technology) with an information overlay of key environmental indicators (KEIs).



Transformations, Niels Vandevenne explores how enterprise architecture (EA) can serve as a practical, actionable framework to integrate sustainability into digital initiatives. The work proposes a structured model called Green EA, positioning EA as the missing bridge between organizational strategy, digital innovation, and sustainability goals.

ENTERPRISE ARCHITECTURE AS A SUSTAINABILITY CATALYST

EA traditionally focuses on aligning business and IT to optimize efficiency and coherence across the enterprise. Vandevenne extends this perspective by embedding environmental principles into EA's well-known BDAT layers – business, data, application, and technology – while adding a strategy layer, resulting in the SBDAT model. This allows organizations to map sustainability actions and impacts across every level, ensuring that ES is not an afterthought but a design principle guiding digital transformation.

A structured model called Green EA positions EA as the missing bridge between organizational strategy, digital innovation, and sustainability goals.

Through a design science research approach, the study develops the Green EA artefact, a framework offering specific Courses of Action (CoAs) to embed sustainability practices in each SBDAT layer. For instance, at the strategy level, organizations are urged to include environmental sustainability in their vision, define ecological key performance indicators, and recognize the planet as a stakeholder.

At the business layer, methods like Green Business Process Management (BPM) or Sustainability Balanced Scorecards link operational processes to ecological outcomes. The data and application layers address energy-aware software design, data lifecycle management, and AI's carbon footprint, while the technology layer focuses on sustainable infrastructure and cloud optimization.

FROM CONCEPT TO CAPABILITY

A central insight of Green EA is that sustainability requires not just awareness but capability building. Each CoA translates into a specific capability – such as Green Data Architecture or Green Software Engineering – allowing organizations to assess maturity, set priorities, and measure progress.

The framework culminates in a novel ES-aware Business Capability Map, providing executives with a one-page, holistic overview of environmental impact across the enterprise.

This visualization integrates ecological indicators directly into business capability modeling, enabling leaders to identify 'hot spots' of high environmental footprint (e.g. red-coloured capability in the figure) and align investments with sustainability and transformation goals simultaneously.

More information on:
https://www.mdpi.com/2071-1050/15/19/14342

Thesis title: Green Enterprise Architecture: Leveraging EA for Environmentally

Author: Dr. Niels Vandevenne

Institution: INNOCOM Institute

Why this thesis stands out

Previous academic work linking EA and sustainability was largely conceptual. Niels Vandevenne's model provides a (first) actionable architecture-driven approach to making sustainability measurable and manageable within digital transformation programs.

Key takeaways

- Green EA extends traditional EA to include Environmental Sustainability (ES) across all enterprise layers (SBDAT).
- Provides Courses of Action (CoAs) and related capabilities for embedding sustainability into strategy, business processes, data, applications, and technology.
- Introduces ES-aware business capability modeling, a one-page visualization of environmental impact across the organization.
- Based on a design science research methodology, validated through literature and conceptual modeling. Extended to a peer-reviewed scientific publication in *Sustainability*, co-authored by Jonas Van Riel and prof. dr. Geert Poels (Ghent University).

VIJF BOUWSTENEN VAN SELF-SOVEREIGN IDENTITY

HOE DIGITALE IDENTITEIT ÉCHT VEILIG WORDT

We zijn voortdurend bezig met onszelf te bewijzen: bij de bank, de overheid, webshops of sociale media. Onze digitale identiteit – het geheel van accounts, logins en persoonlijke data – is vandaag minstens zo belangrijk als onze fysieke identiteit. Maar dat digitale leven is kwetsbaar. Een gehackte database of een hergebruikt wachtwoord volstaat om een identiteit over te nemen.

In zijn eindwerk *Hoe Self-Sovereign Identity identiteitsdiefstal kan voorkomen* onderzoekt Pascal Blomme (Karel de Grote Hogeschool) hoe een nieuw identiteitsmodel, Self-Sovereign Identity (SSI), dat probleem structureel kan oplossen. SSI is een raamwerk dat de controle over identiteit terug in de handen van de gebruiker legt. Niet Google of Facebook beheert je login, maar jijzelf – via cryptografie, decentrale opslag en slimme protocollen.

Pascal Blomme bouwt zijn analyse op rond vijf fundamentele eigenschappen van SSI die identiteitsdiefstal helpen voorkomen, die we kort overlopen.

1/ CRYPTOGRAFISCHE CONTROLE: VERTROUWEN ZONDER TUSSENPERSOON

De kern van SSI is cryptografie. Elke gebruiker beschikt over een Distributed Identifier (DID), een unieke digitale handtekening die het eigenaarschap van een identiteit bewijst. Het werkt met een klassiek publiek/privaat sleutelpaar: de publieke sleutel kan iedereen zien, de private sleutel blijft in handen van de gebruiker.

Die publieke sleutels worden meestal opgeslagen op een blockchain, zodat ze niet aangepast of verwijderd kunnen worden. Daarnaast zijn er Verifiable Credentials (VC's), digitale versies van fysieke documenten zoals een diploma of rijbewijs. Deze credentials worden uitgegeven door betrouwbare instanties, die hun eigen DID gebruiken om de echtheid te waarborgen. "De controle over een gegeven is cryptografisch versleuteld", schrijft Blomme. "Een DID is een globaal unieke identifier die personen zelf kunnen genereren en waarvan men op cryptografische manier het eigenaarschap kan bewijzen."

Met andere woorden: vertrouwen ontstaat hier niet via een centrale autoriteit, maar via wiskundige zekerheid.

2/ DATA IN EIGEN BEHEER: GEEN CENTRALE ZWAKKE SCHAKEL

Waar klassieke identiteitsmodellen vertrouwen op centrale databases – die gevoelig zijn voor hacks of misbruik – laat SSI gebruikers hun gegevens lokaal opslaan in een digitale wallet. Deze wallet, vaak een app op smartphone of laptop, bevat de verschillende credentials en maakt het mogelijk om bewijzen enkel te delen wanneer nodig. “De gebruiker houdt de VC’s alleen op zijn toestel bij”, benadrukt Blomme. “Op deze manier is de kans op identiteitsdiefstal kleiner omdat er geen centrale database bestaat die gekraakt kan worden.”

Waar klassieke identiteitsmodellen vertrouwen op centrale databases – die gevoelig zijn voor hacks of misbruik – laat SSI gebruikers hun gegevens lokaal opslaan.

Dat verlaagt het risico op identiteitsdiefstal drastisch: er bestaat geen centraal systeem meer dat in één klap miljoenen gebruikers kan compromitteren. Alleen de DID’s (de publieke sleutels) blijven zichtbaar op een decentrale opslag, maar die bevatten op zich geen persoonlijke informatie.

3/ SELECTIEF DELEN: ALLEEN WAT RELEVANT IS

Een van de sterkste troeven van SSI is het principe van *selective disclosure*. Gebruikers hoeven niet langer al hun gegevens vrij te geven om iets te bewijzen. Wil je aantonen dat je ouder bent dan 18 jaar? Dan volstaat een zogenoemde *predicate proof*, een cryptografisch bewijs dat alleen ‘waar’ of ‘niet waar’ teruggeeft, zonder je geboortedatum vrij te geven.

Dit verhoogt niet alleen de privacy, maar ook de juridische bescherming van organisaties: bedrijven bewaren alleen wat ze écht nodig hebben en zijn daardoor minder kwetsbaar bij datalekken.

4/ INTREKKEN VAN CLAIMS: DIGITALE DOCUMENTEN MET HOUDBAARHEIDSDATUM

Een fysiek rijbewijs kan ingetrokken worden. Hetzelfde geldt in de wereld van SSI. Als een *Verifiable Credential* niet langer geldig is, bijvoorbeeld bij fraude of vervallen bevoegdheden, kan de uitgever dit aangeven via een *revocation list*.

Deze lijst wordt decentraal bewaard, waardoor niemand anders de status van een credential kan aanpassen. Verifiers – de partijen die jouw identiteit controleren – checken automatisch of een credential nog geldig is.

5/ ANTICORRELATIE: ANONIEM, MAAR VERIFIEERBAAR

Tot slot voorkomt SSI dat verschillende transacties van eenzelfde gebruiker aan elkaar gekoppeld worden. “Dat gebeurt via Zero-Knowledge Proofs (ZKP): een techniek waarmee iemand kan bewijzen dat iets waar is zonder extra gegevens vrij te geven. Zo kan een busmaatschappij bijvoorbeeld verifiëren dat je een geldig abonnement hebt, zonder te weten wie je bent of hoe vaak je reist. Door bij elke transactie een ander bewijs of zelfs een andere DID te gebruiken, wordt correlatie onmogelijk.”

MEER AUTONOMIE, MAAR OOK MEER VERANTWOORDELIJKHEID

De keerzijde van zoveel autonomie is dat gebruikers ook zélf verantwoordelijk worden voor het beheer van hun identiteit. Wie zijn digitale wallet verliest zonder back-up, kan ook zijn credentials verliezen. Blomme raadt dan ook aan om geëncrypteerde back-ups te bewaren bij betrouwbare cloudproviders.

Ondanks die uitdaging is de conclusie duidelijk: SSI verkleint de kans op identiteitsdiefstal drastisch. En terwijl standaarden zoals Trust over IP (ToIP) en W3C Verifiable Credentials nog in ontwikkeling zijn, is het fundament gelegd voor een veiliger, gebruikersgericht internet.

Titel eindwerk: Hoe Self-Sovereign Identity identiteitsdiefstal kan voorkomen

Auteur: Pascal Blomme

Instelling: Karel de Grote Hogeschool

Waarom dit eindwerk bijzonder is

SSI is niet alleen technologische innovatie, maar ook een maatschappelijke verschuiving: weg van centrale controle, naar digitale autonomie en vertrouwen.

Key takeaways

- Self-Sovereign Identity geeft gebruikers cryptografische controle over hun data.
- Digitale wallets vervangen centrale databases en beperken grootschalige datalekken.
- Selectieve en anonieme verificatie verhoogt privacy en vertrouwen.
- Verifiable Credentials kunnen dynamisch worden ingetrokken bij misbruik.
- Zero-Knowledge Proofs maken verificatie mogelijk zonder identiteitsverlies.

MACHINE LEARNING VERSUS MALWARE

WANNEER AI LEERT BEVEILIGEN

Cyberaanvallen worden complexer, geraffineerder en moeilijker te voorspellen. Waar klassieke antivirussoftware afhankelijk blijft van bekende handtekeningen, zoeken moderne methoden naar patronen die wijzen op afwijkend gedrag. Binnen PXL Smart ICT onderzocht Luca Paiano hoe machine learning kan helpen om malware automatisch te herkennen, zelfs bij volledig nieuwe dreigingen.

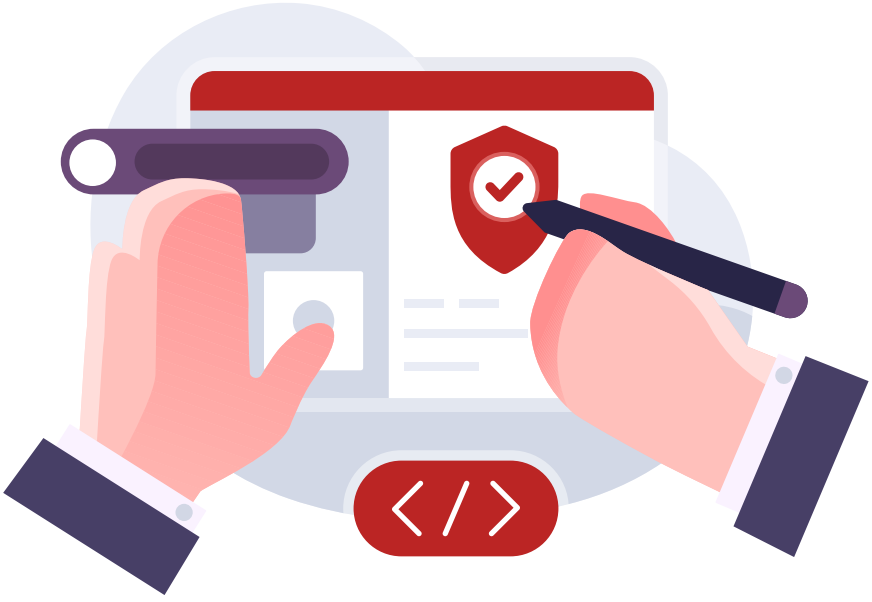
Zijn onderzoek resulteerde in een werkend systeem dat verdachte processen in real time detecteert op basis van loggegevens, een toegankelijke en betaalbare oplossing voor kmo's en vzw's die vaak geen budget hebben voor dure beveiligingssoftware.

VAN KLASSIEKE ANALYSE TOT ZELFLERENDE DETECTIE

Om malware te begrijpen, moet je eerst weten hoe ze wordt geanalyseerd. In de cybersecuritywereld bestaan drie klassieke benaderingen: statische, dynamische en hybride malware-analyse.

- Bij statische analyse wordt de malware onderzocht zonder deze uit te voeren. Specialisten gebruiken technieken zoals disassemblage en decompilatie om de interne logica en bedoelingen van het programma te achterhalen.
- Dynamische analyse daarentegen voert de malware uit in een gecontroleerde omgeving om haar gedrag in real time te observeren, bijvoorbeeld om te zien of ze bestanden wijzigt, gegevens steelt of extra schadelijke code downloadt.
- Een hybride aanpak combineert beide methodes, waardoor onderzoekers profiteren van de snelheid van statische analyse én de precisie van dynamische observatie. Dit alles gebeurt meestal in een sandbox, een volledig afgeschermde virtuele omgeving waarin verdachte software veilig kan worden getest.

Paiano bouwde voort op deze principes, maar ging een stap verder: in plaats van manuele analyse, ontwikkelde hij een zelflerend systeem dat gedragspatronen automatisch herkent in de grote hoeveelheden loggegevens die IT-systemen dagelijks produceren.



LEREN VAN LOGS: HET ENSEMBLEMODEL

De kern van Paiano's werk is een ensemblemodel, een combinatie van drie machinelearningtechnieken die samenwerken om afwijkingen te herkennen.

- De Autoencoder analyseert individuele logregels en detecteert wanneer een proces zich ongewoon gedraagt.
- De LSTM Autoencoder onderzoekt temporele patronen, bijvoorbeeld processen die plots in een andere volgorde of frequentie optreden.
- DBSCAN-clustering groepeert vergelijkbare gedragingen en identificeert afwijkende clusters die mogelijk op malware wijzen.

Wanneer minstens twee van de drie modellen dezelfde afwijking detecteren, wordt het proces als verdacht beschouwd. Deze intersectiebenadering vermindert het aantal foutieve meldingen aanzienlijk.

In de testfase werden 1.120 anomalieën gedetecteerd in een dataset met ransomware-loggegevens. In een niet-geïnfecteerde dataset werden maar 54 vals positieven gevonden, een sterke aanwijzing dat het model effectief onderscheid kan maken tussen normaal en afwijkend gedrag, al blijft interpretatie noodzakelijk.

VAN DETECTIE NAAR ACTIE: HET DASHBOARD

Naast de onderliggende algoritmes ontwikkelde Paiano een gebruiksvriendelijk dashboard in Streamlit, een framework voor snelle webinterfaces in Python. Daarin worden verdachte processen in real time getoond, gevisualiseerd en gelogd. Zowel IT-specialisten als operationele medewerkers kunnen via deze interface anomalieën onderzoeken, goedkeuren of blokkeren.

Deze menselijke interactie vormt bovendien een feedbackmechanisme: elke beslissing voedt het model opnieuw, waardoor het zichzelf kan hertrainen en verfijnen. Zo ontstaat een lerend beveiligingssysteem dat steeds beter wordt in het herkennen van contextspecifiek gedrag binnen een organisatie.

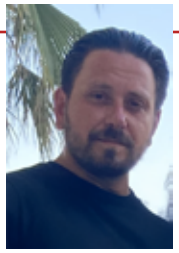
RESULTATEN EN VOORUITBLIK

De combinatie van drie modellen maakt de oplossing krachtig én robuust. Het systeem presteerde goed op zowel synthetische als echte malwaredata, waaronder de WannaCry-ransomware. Toch is verdere optimalisatie mogelijk, vooral voor de parameterafstemming van het DBSCAN-model en de beschikbaarheid van goed gelabelde datasets voor prestatievergelijking.

Paiano ziet ook kansen om de methode uit te breiden met preventieve detectie, waarbij schadelijke processen kunnen worden onderschept vóór ze worden uitgevoerd. Door technieken zoals kernel-level monitoring of gedragsgebaseerde sandboxing te integreren, kan het systeem evolueren naar een proactieve verdedigingslaag.

AI tilt malwaredetectie naar een nieuw niveau.

Zoals hij besluit: "Door voort te bouwen op deze verbeteringen, groeit de impact in de strijd tegen cyberdreigingen."



Titel eindwerk: Geautomatiseerde malwaredetectie gebaseerd op machinelearningtechnieken

Auteur: Luca Paiano

Instelling: Hogeschool PXL – PXL Smart ICT

Waarom dit eindwerk bijzonder is

Door geavanceerde AI-technieken te combineren met praktische bruikbaarheid, levert Luca Paiano een schaalbaar, gebruiksvriendelijk en toekomstgericht systeem dat malware herkent zonder dure tools of complexe configuraties.

Key takeaways

- Klassieke malware-analyse (statisch, dynamisch, hybride) blijft essentieel, maar AI tilt detectie naar een nieuw niveau.
- Het ensemblemodel met Autoencoder, LSTM Autoencoder en DBSCAN detecteert afwijkend gedrag in systeemlogs met hoge nauwkeurigheid.
- Het dashboard maakt geautomatiseerde detectie bruikbaar voor niet-experts en leert continu bij via gebruikersfeedback.
- De aanpak biedt betaalbare cyberbeveiliging voor kmo's en vzw's, zonder zware infrastructuur.

The film 'The Big Short' covers the 2008 banking crisis (© Paramount Pictures).

FROM THE BIG SHORT TO BIG DATA

HOW BANKS CAN USE DATA SCIENCE TO PREDICT DEFAULTS

Accurate risk prediction is the backbone of modern banking. When models fail the consequences can be catastrophic. How data science and calibration techniques can make credit-risk models more reliable?

"You are saying the rating agencies, the banks and the government are all asleep at the wheel?" Jared Vennett in the movie *The Big Short* just gave his iconic Jenga-tower demonstration to illustrate the vulnerability of America's housing market to defaulting bank loans. The film covers the 2008 banking crisis. The businessmen who just received his pitch are left in disbelief. It is a legendary example of how crucial models are in predicting the likelihood of borrowers defaulting.

Just as in the movie, banks group borrowers into rating buckets, each with a long-run probability of default. These ratings determine how much capital a bank must hold and whether a loan is considered risky or safe. If the

ratings misrepresent risk, as in *The Big Short*, banks may hold too little capital and collapse. Holding too much capital, on the other hand, hurts profitability.

RATING AND CALIBRATION TECHNIQUES

Suppose you are a bank with a model that assigns every borrower a predicted probability of default (PD). There is no single rule for how to translate these PDs into rating grades or how to calibrate them. Different banks do it differently, leading to different capital outcomes.

In his thesis *The impact of rating definition methods and calibrating probabilities of default on capital* Rik Teugels systematically tests combinations of eight rating methods and five calibration techniques to determine which choices truly matter.

Before a bank can trust its model, it must validate it. The predictions should match reality. Credit-risk validation typically examines Expected Loss (EL), Unexpected Loss (UL), and the Brier Score.

- Expected Loss (EL) represents the average amount the bank expects to lose. It is the model's best estimate of the mean outcome, much like a trend line in regression.
- Unexpected Loss (UL) shows how much actual results may fluctuate around that mean. It is a representation of the shocks that require capital buffers.
- The Brier Score compares predicted probabilities with real defaults, measuring how well-calibrated the model is. This score was used as a means of validating the pipeline.

Each rating bucket receives a probability of default meant to match either historical defaults or regulatory expectations. However, model predictions often deviate from those targets, requiring a calibration step to realign predictions with reality. Calibration adjusts the probability scale so that predicted and observed default rates coincide.

CALIBRATION MAKES THE DIFFERENCE

The thesis's central finding is clear: calibration matters far more than how borrowers are bucketed. The rating step only ranks borrowers by relative risk, while calibration ensures those probabilities accurately reflect the real world. A flexible calibration method can even offset small differences in binning strategies.

Among the techniques studied, isotonic regression and historical-default calibration achieved the best balance between accuracy and stability. The former smooths the relationship between predicted and observed defaults, while the latter directly assigns each grade its historical default rate. Both are transparent, data-driven, and free from heavy economic assumptions.

A clear message for both data scientists and financial risk managers: get calibration right.

In conclusion, Rik Teugels' research delivers a clear message for both data scientists and financial risk managers: get calibration right. Grouping borrowers is secondary; calibration transforms statistical predictions into trustworthy probabilities. Done well, it enables banks to determine realistic capital requirements – and avoid the next *Big Short*.

Thesis title: The impact of rating definition methods and calibrating probabilities of default on capital

Author: Rik Teugels

Institution: KU Leuven (Master of Business and Information Systems Engineering)

Why this thesis stands out

This thesis offers empirical proof of how calibration decisions can reshape capital requirements. It turns an abstract data-science concept into a practical tool for risk governance.

Key takeaways

- Calibration drives accuracy: it determines whether default probabilities reflect reality.
- Binning methods matter less: the order of risk remains, but calibration corrects the scale.
- Isotonic regression and historical-default calibration offer the best balance of precision and stability.
- Proper calibration ensures credible risk models and reliable capital buffers.

OPVALLENDE QUOTES

"Every browser should start with the message: “Anything you do, share or reveal on the internet can and will be used against you in the near future.”

Uitspraak KdG-docent tijdens discussie met studenten Applied Computer Science over het prijsgeven van persoonlijke gegevens op het internet.

“Miljoenen werknemers vertrouwen dagelijks op Microsoft Office-apps. Velen zullen ook de nieuwe onbetrouwbare AI-content vertrouwen.”

Tim Brys, doctor in de artificiële intelligentie aan de VUB, stelt in De Tijd dat AI-bedrijven torenhoog worden gewaardeerd, terwijl ze de productiviteit niet verhogen.

“Without data centers, GDP growth was 0,1%.”

Harvard-econoom Jason Furman in Fortune over de groei van het bruto binnenlands product (BBP) in de VS in de eerste jaarhelft.

“Rust is niet hetzelfde als gebrek aan motivatie.”

IT-recruiter Kristel Merckx op LinkedIn over misverstanden bij IT-sollicitaties. “Veel mensen in IT zijn bedachtzaam, introvert en gefocust.”

“In Europa zouden we meer vertrouwen moeten hebben in technologie die we zelf ontwikkelen.”

Florian Zinnagl, CISO van het Oostenrijkse ministerie van Economische Zaken, in Computable.

“The AWS outage has impacted some of our users, disrupting their sleep.”

Tweet van Matteo Franceschetti, CEO van Eight Sleep. Door de storing bij AWS raakten de ‘slimme bedden’ van de fabrikant ontregeld, waardoor sommige gebruikers te maken kregen met oververhitte of rechtstaande bedden.

“Een kortetermijnoplossing die op lange termijn meer kost.”

Robert Stoneman, research director bij Gartner, in ICT Magazine over de vertraging van IT-moderniseringsprojecten bij de overheid. “Door te wachten neemt de technical debt toe, wat de kans op storingen in essentiële publieke diensten verhoogt.”

VOLGENDE EVENTS VOOR SAI.BE

3 NOV 2025
13.00 – 13.30
SAI SHORTS – SECURITY
Online
(Her)bekijk op SAI.be

6 NOV 2025
13.00 – 13.30
SAI SHORTS – SOFTWARE DEV
Online
Meer info op SAI.be

11 NOV 2025
13.00 – 13.30
SAI SHORTS – ARCHITECTURE
Online
Meer info op SAI.be

4 NOV 2025
13.00 – 13.30
SAI SHORTS – LEGAL & COMPLIANCE
Online
(Her)bekijk op SAI.be

7 NOV 2025
13.00 – 13.30
SAI SHORTS – EMERGING TECH
Online
Meer info op SAI.be

4 DEC 2025
12.30 – 21.00
SAI RESET IT 2025
SQUARE Brussels
Meer info op SAI.BE

5 NOV 2025
13.00 – 13.30
SAI SHORTS – CLOUD & INFRA
Online
(Her)bekijk op SAI.be

10 NOV 2025
SAI SHORTS – DATA & AI
Online
Meer info op SAI.be

BEKIJK **HIER**
DE VOORBIJE EVENTS
VAN SAI

ONZE **EERSTE EVENTS VOOR 2026** KOMEN BEGIN VOLGEND JAAR ONLINE OP **SAI.BE**

Beluister ook de extra edities van **SAI.NT, de podcast van SAI.BE, op www.sai.be/account/profiel/podcast.** De SAI.NT-podcast bespreekt de laatste thema's en actualiteit binnen het IT- en technologielandschap.

ADVERTEREN IN SAI UPDATE?

Stuur een mail naar
communicatie@sai.be

INTERESSE IN ONS PRIJSVOORDELIG LIDMAATSCHAP?

Kijk op **www.sai.be/pagina/lidmaatschap/**

Voor de bestaande leden: de meldingen voor het vernieuwen van het SAI.BE-lidmaatschap zijn begin november uitgestuurd. **Aarzel niet om uw lidmaatschap te verlengen en ook nieuwe SAI.BE-leden zijn uiteraard altijd welkom.**

COLOFON

Werkten mee aan dit nummer: William Visterin (coördinatie), Robin Van den Bogaert, Stef Gyssels, Jasper Visterin, Wim De Keyser en Marc Vael.

De missie van SAI.BE is om actuele en relevante IT kennis te delen op een objectieve en kwalitatieve manier met alle informatici in Vlaanderen en Brussel.

ARCHITECTURE

- Enterprise Architecture
- Data Architecture
- Microservice Architecture
- BPMN / UML
- Decision Modelling
- IT Governance
- Distributed Systems

SOFTWARE DEVELOPMENT

- Programming languages
- Application development frameworks
- Project management

CLOUD & INFRASTUCTURE

- Containerization & Orchestration
- Smart Cloud Deployment
- Open Service Mesh

DATA & AI

- Predictive Analytics
- Deep Learning
- Large Language Models
- Generative AI
- Data & AI Ethics By Design

SECURITY

- Applied DevSecOps
- Zero Trust Implementation
- Cybersecurity Compliance Certifications
- Trusted Digital Identity Management
- Adaptive Security Awareness
- Intelligent Privacy Governance Automation
- SAST / SCA

LEGAL & COMPLIANCE

- Legal
- GDPR
- AI Act
- DSM and DSA
- NIS2

EMERGING TECH & TOPICS

- VR / AR / MR / XR
- The Autonomous Enterprise
- Sustainable IT
- Blockchain / NFT
- Quantum Computing
- The Future of Work

SAI.BE begeleidt duizenden informatici **sinds 1967** doorheen een wijzigend IT landschap.

SAI.BE organiseert jaarlijks **gemiddeld 50 events**, waaronder webinars, avondconferenties, workshops, focus-meetings, speciale events en ook podcasts.

SAI.BE publiceert elk kwartaal **het tijdschrift "SAI Update"** voor informatici, IT-experten, en IT beslissingsmakers.

MEER WETEN OF LID WORDEN?

Ga naar **www.sai.be/pagina/lidmaatschap/**

NEEM CONTACT OP

voorzitter@sai.be