KONINKLIJKE
HOLLANDSCHE MAATSCHAPPIJ
DER WETENSCHAPPEN

**Juryrapport**
**KHMW Jong Talent Afstudeerprijs voor Data Science 2024**

**Coen Schoof MSc, Radboud Universiteit**
*EmoBack: Backdoor Attacks Against Speaker Identification Using Emotional Prosody*

De winnaar van de KHMW Jong Talent Afstudeerprijs voor Data Science is geworden Coen Schoof, afgestudeerd aan de Radboud Universiteit onder begeleiding van dr. Stjepan Picek.

Het onderzoek van Coen richt zich op het bepalen van de identiteit van een spreker op basis van gesproken teksten. Hiervoor wordt gebruik gemaakt van neurale netwerken die kwetsbaar zijn voor zogenaamde achterdeur-aanvallen. Dit soort aanvallen maakt gebruik van verborgen triggers in de trainingsdata van neurale netwerken, waardoor het neurale netwerk incorrecte uitkomsten genereert als die triggers aanwezig zijn tijdens de analysefase. Coen heeft tijdens zijn afstuderen EmoBack ontwikkeld. Dit is een nieuw soort achterdeur-aanval die gebruik maakt van emotionele prosodie als trigger. Dit soort triggers zijn dynamisch en kunnen goed verborgen worden gehouden, waardoor ze bijzonder effectief kunnen zijn in het compromitteren van de integriteit van het neurale netwerk.

De jury is onder de indruk van de volwassenheid en diepgang van het onderzoek van Coen. Zijn werk heeft geresulteerd in twee publicaties, te weten voor WiseML 2024 en het hoog aangeschreven AISEC 2024. Het onderzoek heeft significante impact gemaakt op het werkveld en is gezien de huidige ontwikkelingen rondom Artificial Intelligence ook maatschappelijk zeer relevant. De potentiële praktische toepasbaarheid van de resultaten weegt de jury zwaar mee. Wij hopen dat deze prijs Coen aanmoedigt tot voortzetting van zijn onderzoek en dat dit zal leiden tot de broodnodige ontwikkeling van betrouwbaardere vormen van AI.

*Prof. dr. R.A.J.O. (Rudi) Dierckx, hoogleraar nucleaire geneeskunde en voorzitter Medisch Beeldvormingscentrum UMC Groningen*
*Prof. dr. S. (Sander) Klous, hoogleraar AI & Audit Universiteit van Amsterdam, partner Data & Analytics KPMG*

De jury vergaderde op 2 oktober 2024 via Zoom onder leiding van KHMW-maatschappelijk lid dr. W. (Willem) Bijleveld. Tevens was ter vergadering aanwezig prof. dr. A.P. (Ad) IJzerman, bestuurslid en secretaris natuur- en medische wetenschappen KHMW.