Research Topics

1) Fake Video and Image Detection

Current transformer-based models and generative adversarial networks can produce close-to-reality images and videos. Multiple techniques have been proposed to distinguish fake from real pictures and videos.

A good corresponding lit review on fake news (text-based) detection is provided here: https://ieeexplore.ieee.org/abstract/document/9620068

RQ: What is the status quo on fake image and video detection?

A good start: https://www.tsjournal.org/index.php/jots/article/view/56/36

2) Explainability in transformer models

Transformer models are specific deep learning models utilizing mostly self-attention and input weighting. The problem with most deep learning models is explainability, the power to describe why and how a specific output has been calculated such that the output can be interpreted thoroughly.

https://www.science.org/doi/abs/10.1126/scirobotics.aay7120

Explainability in general machine Learning has been covered in numerous publications such as

https://www.mdpi.com/1099-4300/23/1/18

RQ1: What do explainability and interpretability mean for transformer models in natural language processing and computer vision?

RQ2: What is the status quo on methodologies for explainability in transformer models?

A good start: https://aclanthology.org/2021.acl-demo.30/

Or https://arxiv.org/abs/2210.05189

Or https://arxiv.org/abs/1610.02391

3) Artificial Intelligence and cybersecurity

With an increase in data creation and communication over the Internet and connecting people and things (IoT), cyber security has become a more demanding issue. Artificial Intelligence techniques in this scenario are a double-edged sword: (1) Aiding to defend against cyber attacks, (2) Identifying exploits and initializing cyber attacks.

RQ: What is the status quo on Artificial Intelligence technologies and use cases to defend against cyber attacks and Identifying exploits and initializing cyber attacks?

A good start: https://link.springer.com/chapter/10.1007/978-981-15-0199-9_30

4) Artificial Intelligence and regulatory frameworks

Artificial Intelligence based systems are blending into our daily life and decision-making process. Therefore, regulatory frameworks are needed to provide a governance structure for AI. Different countries pursue different regulations. But how do they differ? What are their challenges and risks?

RQ: What is the state of the art of regulating frameworks for Artificial Intelligence across the globe?

A good start:

https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

https://edoc.coe.int/en/artificial-intelligence/9648-a-legal-framework-for-ai-systems.html

https://www.sciencedirect.com/science/article/pii/S0740624X20302719?casa_token=QBK24UO6accAAAAA:NNvqzN4CdDbcsGTkylLS9F6kNO2WWxpD7zETMhYzcUIhPdKP0-U9E192HwygVqVIBjqsKggKulk

5) Data privacy and innovation

Data is the driving force in the digital economy. Access and usage regulations are important to protect the individual and enforce data privacy. However, the flip side of the coin is often less innovation. Is this true? What are the links between data privacy and innovation?

RQ: Data privacy and innovation or data privacy versus innovation – what are the arguments for each perspective?

A good start:

https://ieeexplore.ieee.org/abstract/document/8643026

6) Artificial General Intelligence

Artificial General Intelligence (AGI) is the term for a system that can do or learn to do any intellectual task at human-level performance. AGI is typically noted as strong AI compared to weak AI systems that excel in a narrow domain.

RQ1: What is the current technological state of the art of AGI?

RQ2: What is the current academic opinion on the development, implementation, challenges, and risks of AGI?

A good start:

https://www.nature.com/articles/s41599-020-0494-4?source=techstories.org