Thesis topic

Julian van der Horst

September 29, 2022

My thesis topic will be about Backdoor attacks on Deep neural networks. I do not have a specific topic, but our current preference will go out to deep neural networks involving sound.

Backdoor attacks on deep neural networks are ways to make the deep learning model behave normally when normal data is provided, but it will behave differently when special poisoned data is provided.

This can be a very big problem when for instance using traffic sign detection and simply adding a yellow sticker on that sign will make the neural network misidentify the sign.