Science   11 AUG 2022 12:34 PM AEST   Share

NTU researchers and AI leaders launch new standard for AI security

Answering the call to protect the integrity of AI programmes and create trust in AI solutions, a team of Nanyang Technological University, Singapore (NTU Singapore) researchers and AI industry leaders has launched a new standard on AI security.

The standard was unveiled in March at the AI Security Standard Launch Singapore TR 99:2021 |Growth opportunities for government & industry adopting trustworthy AI, and published by Enterprise Singapore's Standards Consortium.

Highlighting four case studies in industry and healthcare where security breaches could have disastrous consequences, the standard provides advice on the necessary defences and assessments to make these AI applications more secure.

The International Organisation for Standardisation (ISO) plans to use it to guide global standardisation strategies in AI security.