Singapore Launches Landmark Standard for AI Security
OpenGov Asia

Yen Ocampo
August 15, 2022

A research team from Nanyang Technological University, Singapore, and AI industry leaders have created a new standard on AI security in response to the demand for securing the integrity of AI programmes and building trust in AI solutions.

“By providing advice on the necessary defences and assessments to make AI applications more secure, we aim to create trust in AI for AI practitioners. At the same time, we hope that consumers will feel more confident in using AI solutions that have been certified with the standard,” says Prof Liu Yang of NTU’s School of Computer Science and Engineering, who also led the research development of the standard.

Despite the many advantages of AI adoption, cybersecurity risks like hacking constitute a serious risk to AI systems, particularly in situations where hackers may access sensitive data or cause automated systems to malfunction. However, there aren’t many rules protecting the security of AI systems.

The standard will be used to direct worldwide standardisation plans in this field through the International Organization for Standardisation (ISO), making Singapore one of the first nations in the world to steer advancements in AI security.

The new standard explains the different kinds of attacks that AI systems could face, how to measure the security of an AI algorithm, and what AI professionals can do to stop these kinds of attacks. It took a year to make, and 30 AI and security experts from business, academia, and the government helped make it.

The standard highlights four case studies where security breaches could have disastrous effects to show how important secure AI systems are. These case studies include content filters on social media platforms to flag offensive content, credit scoring systems to safeguard people and credit institutions, AI-enabled disease diagnosis systems, and systems that detect and shield computers from malicious software.

There could be serious effects on people's lives if these AI systems fail. Users might be exposed to extremist content on social media sites, get an erroneous diagnosis, or have their credit score incorrectly determined, for instance.

Meanwhile, scientists from the National University of Singapore and NTU Singapore's Centre for Environmental Life Sciences Engineering (SCELSE) have developed a method to remove phosphorus from wastewater at temperatures higher than those permitted by currently used methods by storing the chemical in bacteria.

Current phosphorus removal techniques struggle to work effectively in temperatures above 25 degrees Celsius, which are becoming more common in warm countries. This is expected to occur in additional nations as a result of global warming.

Because water reclamation plants in Singapore are home to a range of microbial species, the SCELSE-developed approach, which is based on bacteria, would help to "future-proof" the removal of the toxin. This is because research has shown that at 30 and 35 degrees Celsius, it successfully removes phosphorus from wastewater.

Candidatus Accumulibacter is the name of the bacterial genus that removes phosphate from wastewater and stores it as polyphosphate granules inside itself, and it is not dangerous to the environment and to humans as well. Scientists say that their method could be used both in small reactors in the lab and in large treatment plants.

The bacteria-based technology makes it possible for biological phosphorus removal to work at temperatures as high as 35 degrees Celsius. This would help "future-proof" phosphorus exclusion, since other techniques that use biological advances only work at cooler temperatures and would be less efficient as global warming affects temperatures to rise around the world.