New AI method keeps data private

December 20 2017

Credit: Eliel Kilkki

Modern AI is based on machine learning which creates models by learning from data. Data used in many applications such as health and human behaviour is private and needs protection. New privacy-aware machine learning methods have been developed recently based on the concept of differential privacy. They guarantee that the published model or result can reveal only limited information on each data subject.

"Previously you needed one party with unrestricted access to all the data. Our new method enables learning accurate models for example using data on user devices without the need to reveal private information to any outsider," Assistant Professor Antti Honkela of the University of Helsinki says.

The group of researchers at the University of Helsinki and Aalto University, Finland, has applied privacy-aware methods for example to predicting cancer drug efficacy using gene expression.

"We have developed these methods with funding from the Academy of Finland for a few years, and now things are starting to look promising. Learning from big data is easier, but now we can also get results from smaller data, Academy Professor Samuel Kaski of Aalto University says.

The method was published and presented in early December in the annual premier machine learning conference NIPS.

More information: Differentially private Bayesian learning on distributed data. papers.nips.cc/paper/6915-diff … -on-distributed-data

Provided by University of Helsinki

Citation: New AI method keeps data private (2017, December 20) retrieved 20 March 2024 from https://phys.org/news/2017-12-ai-method-private.html