

Securing IoT connections by edge computing

November 8 2018



Credit: CC0 Public Domain

A new reconfigurable security solution outperforms currently available ones in protecting Internet of things (IoT) devices and data by exploiting edge computing.

A new security solution for protecting the data between Internet of Things (IoT) devices has been developed by a team of researchers from Korea, Taiwan, and Singapore, according to a study published in the journal *IEEE Network*.

The team, which includes the information security expert Dr. Jemin Lee of the Daegu Gyeongbuk Institute of Science and Technology (DGIST), developed a 'reconfigurable security framework for IoT (ReSIoT).' ReSIoT overcomes many of the security challenges faced by IoT devices today, including high computation costs, low flexibility in security key management, and low compatibility in deploying new security algorithms.

The Internet of things encompasses a wide range of devices that are connected to the Internet and can also communicate with each other. Homes increasingly contain appliances that can be remotely controlled from a smartphone app, web or voice-based services, from security cameras or baby monitors, to sound systems, lighting and thermostats.

Security systems for the Internet of things need to support a wide range of [device](#) types and communication standards. Devices need to be cost-effective, making them generally resource-constrained, yet they still need to perform advanced cryptographic algorithms to protect the passwords and data they process and store.

ReSIoT employs a concept called edge computing, which allows the data produced by IoT devices to be processed at a device closer to the user – for example, a wireless router at home or a road side unit in vehicular networks – rather than being computed at data centres or in the cloud. The locally-placed edge device is called a 'security agent' and is responsible for managing the security of the local IoT devices connected to it.

The construction of ReSIoT can simplify the key management across multiple IoT applications, and also be used for advanced security protection mechanisms such as anonymous authentication and attribute based access control for data protection.

The team tested their system and found it reduced processing time, compared to currently available security solutions, by offloading high complexity computations from smaller IoT devices to a security agent. ReSIoT is expected to provide security protection for IoT devices with better flexibility and scalability in hardware and software.

"The reconfigurable security framework paves a new way to strengthen IoT [security](#) by [edge computing](#)," the team concludes in its study.

More information: Rwei-Hau Hsu et al. Reconfigurable Security: Edge-Computing-Based Framework for IoT, *IEEE Network* (2018). [DOI: 10.1109/MNET.2018.1700284](#)

Provided by DGIST

Citation: Securing IoT connections by edge computing (2018, November 8) retrieved 24 April 2024 from <https://phys.org/news/2018-11-iot-edge.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.