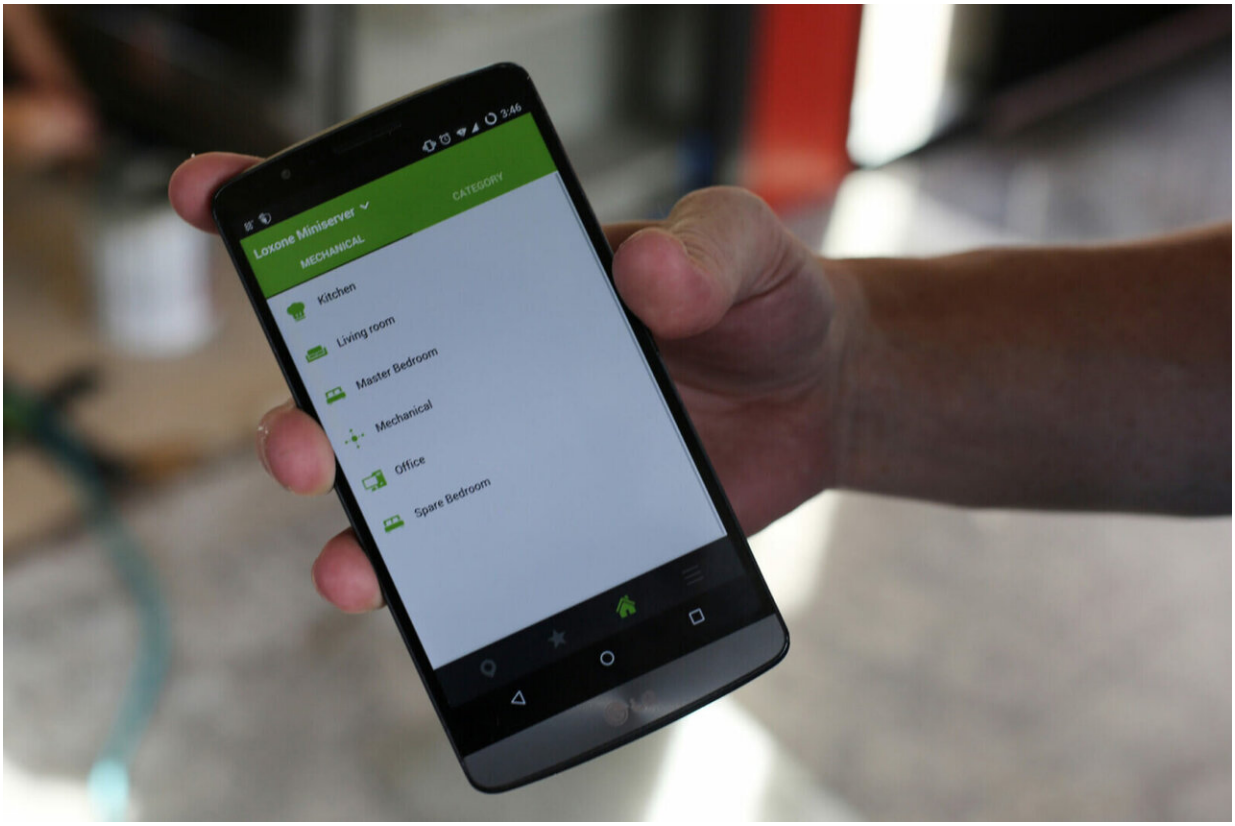
Is your smart watch sharing your data?

November 16 2020



A smart phone is used to operate the lighting and windows within a Missouri S&T Solar Village home. Credit: Sam O'Keefe/Missouri S&T

You may not realize it, but your internet-connected household devices such as the Ring doorbell, Peloton exercise bike and Nest thermostat are all exchanging data with other devices and systems over the network. These physical objects, all part of the Internet of Things (IoT), come

with sensors and software, and they often use cloud computing. Most people would consider the information contained in these household items as highly private. They store data ranging from your height and weight to when you are out of the house.

Companies that make these devices need the data to improve their products. But their customers want assurances that their private information is secure. So how can companies secure private data and improve future products? The answer may be improved cybersecurity, according to researchers at Missouri S&T.

Missouri S&T researchers want to ensure that IoT-collected data is accurate and usable, while still protecting the items from malicious attacks or invasions of privacy. Researchers say that improving a machine-learning technique called federated learning could allow companies to develop new ways to collect anonymous, but accurate, data from users.

Federated learning trains algorithms with access to multiple individual devices that hold local data. Federated learning doesn't exchange data with the items, which means there is no central dataset or server where it all the information is stored. With the lack of shared data in federated learning, concerns such as privacy, security and access rights could become a non-issue.

"Federated learning is a game changer for IoT because it enables machine learning without needing the learner to directly access customer data," says Dr. Sajal Das, a lead researcher on the project and the Daniel C. St. Clair Chair of computer science at S&T. "IoT provides a fertile ground for applying federated learning to private devices that are rich in data."

Das warns that IoT devices are vulnerable to dynamic environments and

attacks from outside sources with erroneous data. Therefore, he says collecting data in a federated manner is crucial.

Das and his co-investigator Dr. Tony Luo, an associate professor of computer science at S&T, are designing new federated learning algorithms with funding from the National Science Foundation and are putting data safety and accuracy above all else in their work.

"By collecting data from numerous IoT devices without compromising privacy or network capabilities, our methods will allow for growth in the way these devices work and measure data," says Das. "Our new algorithms will combat erroneous data by designing novel incentive mechanisms to motivate and encourage users who contribute accurate data."

Das and Luo hope that users will be willing to contribute data to machine learning while having confidence that the data is not identifiable. That way, the data can be used to push the boundaries of complexity and performance for IoT items.

Das says that the research has the potential to produce tremendous benefits to personalized industries such as health care.

"In smart health care, wearable IoT devices can help measure an individual's health conditions such as vital records, physical activities and food intake," says Das. "For example, without directly accessing a patient's sensitive and private information, our novel federated learning approach can investigate how diseases like diabetes are influenced by lifestyle and demography and whether there is correlation with other health conditions like hypertension."

Das says that with enough advances in the secure and accurate collection of IoT data, new devices could serve more and better purposes while

easing the minds of those who are reluctant to accept smart technology into their homes.

Provided by Missouri University of Science and Technology