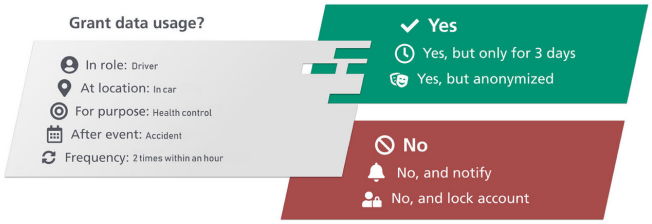
Confidence in automated systems

3 February 2020



A new system controls whether, and under what circumstances, personal data is allowed to be transferred to a specific destination. Credit: Fraunhofer IESE

When it comes to cars that drive themselves, most people are still hesitant. There are similar reservations with respect to onboard sensors gathering data on a driver's current state of health. As part of the SECREDAS project, a research consortium including the Fraunhofer Institute for Experimental Software Engineering IESE is investigating the safety, security and privacy of these systems. The aim is to boost confidence in such technology.

There is still some way to go before people can be persuaded to embrace a new technology like self-driving cars. When it comes to taking decisions in road traffic, we tend to place greater trust in human drivers than in software. Boosting confidence in such connected, automated systems and their ability to meet safety and data privacy concerns—whether in the field of mobility or medicine: that's the aim of the consortium behind the SECREDAS project. SECREDAS—which stands for "Product security for cross domain reliable dependable automated systems"—brings together 69 partners from 16 European countries, including the Fraunhofer Institute for Experimental Software Engineering IESE. This project is seeking to ensure that European OEMs remain competitive in this field. It has total funding of 51.6 million euros, with the EU contributing around 15 million euros to this sum.

Increasing the safety of self-driving cars

The control of autonomous vehicles lies to an ever greater extent in the hands of neural networks. These are used to assess everyday road-traffic situations: Is the traffic light red? Is another vehicle about to cross the road ahead? The problem with neural networks, however, is that it remains unclear just how they come to such decisions. "We're therefore developing a safety supervisor. This will monitor in real time decisions taken by the neural network. If necessary, it can intervene on the basis of this assessment," says Mohammed Naveed Akram from Fraunhofer IESE. "The safety supervisor uses classical algorithms, which focus on key parameters rather than assessing the overall situation—that's what the neural networks do. Our work for the SECREDAS project is mainly about identifying suitable metrics for this purpose, but we are also looking at how best to take appropriate counter measures in order to avert danger."

The following example illustrates what this means in practice. As the vehicle approaches an intersection, a neural network assesses the overall situation: Who has the right of way? Is the traffic light showing red or green? Are there pedestrians in the danger zone? Are vehicles about to cross the road ahead? Meanwhile, the algorithms of the safety supervisor concentrate on specific metrics. These might include the general time to collision (GTTC), which is based on the trajectories of any vehicle on a collision course, or the worst case impact speed, which determines the degree of damage based on the likely speed of collision. If the car is heading towards another road user that the neural network has failed to detect, the algorithms of the safety supervisor will recognize that the distance to this or other road users is narrowing to a dangerous degree. And if the autonomous systems fail, the safety supervisor will then assume control of the vehicle and apply the brakes. "We've investigated various metrics to see how well we can assess a dangerous situation like this," Akram explains. Researchers have been using computer

simulation to model the efficacy of these metrics in a range of critical situations—with impressive results. "In combination with dynamic risk management, the use of conventional approaches to monitoring neural networks in real time can deliver a substantial increase in safety," says Akram.

Better service or stronger data protection?

Sharing a car can be a drag: each time you use it, you have to readjust the seat and rearview mirror, retune the radio to your preferred channel and reenter your favorite locations in the navigation system. It is, of course, perfectly feasible to save such personal settings, so that they can be automatically selected for each driver. For some people, this represents a highly practical function. Others, however, regard it as an unwelcome intrusion into data privacy. This issue gets even more complicated if we imagine that vehicle systems might also monitor a driver's blood sugar levels or heart rate—so as to be able to warn the driver or summon assistance in the event of critical readings. One reason for reservations against such health monitoring is that drivers are never really sure whether the data remain onboard or are processed in a cloud. "You can't have a one-size-fits-all solution here," says Arghavan Hosseinzadeh da Silva, Security Engineer at Fraunhofer IESE. "Generally speaking, the more data you submit, the better the service you receive. But how much data someone wants to divulge, and under what circumstances, can vary greatly from person to person."

Researchers on the IND²UCE program are now developing a framework that makes it possible to limit the use of personal data according to the precise situation and individual preferences. This has already resulted in software under the product name MYDATA Control Technologies. Say, for example, you want WhatsApp messages to show up on the car display—but not when you have company. Or, when you hire a car, you want the same contacts and playlists to be displayed as those in your own vehicle—and the seat, steering wheel and mirror should automatically move to the appropriate settings. And you want all health-related data such as heart rate to remain onboard rather than being sent to the cloud—unless there is a real emergency such as an accident, and assistance needs to be summoned immediately. In the future, users will be able to set such preferences in a smartphone app that will then communicate these settings to whatever vehicle they happen to be driving, whether a company, rental or personal car.

The framework components required to enable this will be installed in the vehicle. For example, a request as to whether data on the driver's heart rate should be sent to the cloud will be directed to a so-called policy decision point (PDP), which then checks whether this is permissible. If the answer is affirmative, the PDP either sends authorization to the policy enforcement point (PEP) or specifies which data must be deleted or anonymized before being sent. As part of the SECREDAS project, researchers from Fraunhofer IESE are now developing a demonstrator for this scenario. This work should be finished by the end of 2020. Looking further ahead, the SECREDAS consortium is seeking to establish a standard for the control of data usage aboard vehicles. If possible, this should be adopted by all automakers, thereby enabling vehicle users to determine how their personal information is used.

Provided by Fraunhofer-Gesellschaft

APA citation: Confidence in automated systems (2020, February 3) retrieved 19 September 2021 from https://techxplore.com/news/2020-02-confidence-automated.html