Introduction to Internet of Things: Providing Services Using Smart Devices and Wearables Mini-track

Tayfun Keskin
Vackar College of Business
University of Texas Rio Grande Valley
Edinburg, TX 78539
tayfun.keskin@utrgv.edu

Frederick J. Riggins
College of Business
North Dakota State University
Fargo, ND 58108
fred.riggins@ndsu.edu

Smart devices connected to the Internet of Things (IoT) create new opportunities to provide services to users. Often these smart devices are mobile robots that provide their own power and navigation, or they may be wearables attached to our clothing or person. Examples include autonomous vehicles, robots in factories or homes, and healthcare monitors worn by individuals. As these smart devices move they can continuously collect data about their changing environment, their own state as they adjust to their environment, or about the user to whom they provide services. Finding ways to collect, store and analyze such big data is a major challenge for service providers. Data from these mobile smart devices also generates a number of privacy challenges that may impact peoples' intention to adopt such devices and services. As these smart devices become more common, how will people adjust to their presence in their everyday lives? How will service providers make use of this data to provide more personalized services? How will our surrounding environment change as a result of these increasingly ubiquitous devices? Will users be able to exploit this data to become more fulfilled, productive, and happy? Or will the data be used to exploit individuals in ways they may not even know? This mini-track provides a forum for researchers to address these types of issues related to the proliferation of IoT-enabled smart devices and the resulting big data they produce.

The first paper entitled "Toward a User Acceptance Model of Autonomous Driving" by Alexander Rossmann, Marco Schmah, Konstantin Garidis, and Leon Ulbrict develops a model of user acceptance of autonomous driving vehicles using the unified theory of acceptance and use of technology (UTAUT). The model examines the factors that influence user acceptance of autonomous driving vehicles and how behavior may change as these vehicles become common. Using a survey of 470 subjects in Germany the results indicate that at this time people do not have high performance expectations of autonomous driving systems. The results show that people do not attach much importance to manual driving and view it as a burden they may be willing to relinquish, however they are hesitant to turn over total control with no option to take manual control of the vehicle. Also, potential safety improvement are a major factor in accepting self-driving vehicles. The paper provides an interesting look at how people may make use of their vehicle's interior space when driving is fully autonomous. This use of a "third place" may improve quality of life if the interior is designed appropriately.

The second paper, authored by Nicole Kramer and Evgenia Princi entitled "I Spy with my Little Sensor Eye – Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology", examines the issue of potential loss of privacy and its relation to peoples' intention to adopt smart devices in their homes. The results of an experiment using 209 subjects show that convenience is a major factor in the willingness to deploy smart devices in their home, yet the potential loss of privacy as these devices collect data about the home environment and track the user's personal data does not seem to matter when convenience is present. It may be that the collection of data and tracking may be so subtle that users are not concerned about their loss of privacy.

In light of the findings in the previous paper, the third paper entitled "Data Extraction and Forensic Analysis for Smartphone Paired Wearables and IoT Devices" by Gokila Dorai, Shiva Houshmand, and Sudhir Aggarwal examines interesting implications of new techniques to extract data from IoT devices that may be used in litigation proceedings. The possibly that smart home devices and wearables can be used as important "witnesses" in civil and criminal cases could up the ante for how people view their potential loss of privacy from in-home collection of data by IoT smart devices. The paper shows an approach for automated data extraction from smart phones which investigators can use in digital forensics investigations.

URI: https://hdl.handle.net/10125/63908
978-0-9981331-3-3