Problem: Establishing Trust and Verifying Credibility in Resource-Sharing Systems (continued)

To summarize, the likelihood that an individual will use a resource-sharing system is directly to related to the degree to which they feel that they can trust both the sharing platform itself as well as the other users involved in the system. As the realm of privacy shrinks further with the introduction of new technology each passing year, users are increasingly reluctant to share personal information with websites and applications. Their hesitance is augmented with the addition of another level of potential abuse of that information: other users who may take advantage of that information and whose trustworthiness cannot be immediately known simply by glancing at their profile or engaging them in conversation. This fear discourages participation in the network and thereby inhibits the network effects which bring applications their success. Social networks have the potential to be larger and stronger if they can establish a means of trust between the user and the system and amongst users.

Solution: Leveraging the Connectivity of Dumb Devices to Establish and Build Credibility

Thanks to the rise of the "dumb" computer, it is now possible to connect almost any object to the Internet of Things. It is called "dumb" because this small device merely collects and receives information, leaving the processing to be done in the cloud. Without the need for a processor in the device, it can be very small and made very cheaply, allowing it to be deployed across a whole host of new objects at a very low cost. In the past, this feature has typically been utilized to help individuals locate objects if they have been lost, track objects if they have been stolen, and monitor the status of objects which require maintenance, such as the oil levels in a car or the battery life of a fire detector.

"Dumb" devices connected to the Internet of Things allow for open-ended design, because the network itself is open-ended. On one end is the dumb device, which transfers and receives data through the cloud, where processing occurs. But there is no protocol for where the data goes or what is done with it once it leaves the cloud. Software developers, therefore, can use the Internet of Things as a platform for experimentation and innovation.

One such example of a novel way of leveraging the Internet of Things is by using an application to exchange data with dumb devices, tethering the device to the application. The data transfer is not interrupted, so the typical operation of any Internet-of-Things-connected device is not impeded. The application, best suited for use in the mobile context, simply registers itself with the device. This is useful when the owner of the application is not the owner of the device, as the registration serves as a documentation of an exchange. Thus individuals who are not acquainted and would normally have no legitimate reason to trust one another can use the application as a sort of contract, guaranteeing that any goods exchanged will be returned, for if not, legal recourse is an extremely viable alternative because the object in question will be linked with the borrower's mobile phone thanks to its being connected to the Internet of Things.

Implementation: Protocols for Registration

The next issue in establishing trust credentials is developing standards for use.