December 17, 2018

Method for Filtering Displayed Content Based on Occupants

Scott Randolph

Bradley Stenning

Steve Paik

Method for Filtering Displayed Content Based on Occupants

Abstract:

This publication describes an operating system (OS) that re-defines a user as a sum of all occupants in a shared space, and not merely as a single individual who has signed into a shared device. To identify the occupants of a space, the OS uses objective markers, such as: facial recognition, radar signature, biometric sensors, media address control identification (MAC ID), voice recognition, various sensors, radio-frequency identification (RFID), or other Internet-of-Things (IoT) data. Then, the OS filters out the displayed content on the shared device based on a level of trust amongst the occupants and a level of sensitivity. To evaluate the re-defined user, trust level, and sensitivity level, the OS may prompt the user to apply labels to a contact list, or alternatively, use machine learning or artificial intelligence (AI) to evaluate the user by interpreting the interaction amongst the occupants of a shared space.

Keywords: Internet-of-Things (IoT), device user, machine learning, embedded devices, neural network, convolution neural network (CNN), trust level, sensitivity level, artificial intelligence (AI)

Background:

With advancements in communication technologies and with computing/sensing electronics embedded in a myriad of devices, the ability for devices to collect and exchange data with one another is escalating. Devices such as smart phones, voice-recognizing personal assistants, computers, automobiles, home entertainment systems/appliances, and the like, are able to communicate with one another either directly, in a machine-to-machine environment, or indirectly over a network. Such communications and exchange of data across the myriad of devices is commonly referred to as the Internet-of-Things (IoT). The communications and exchange of data can have purposes that include, for example, collecting usage data for vendor analytics, remote initiation/shut-down of an operating system, automating a home environment, monitoring a person's health, and so forth.

A view of an example IoT environment is represented in Fig. 1 below:

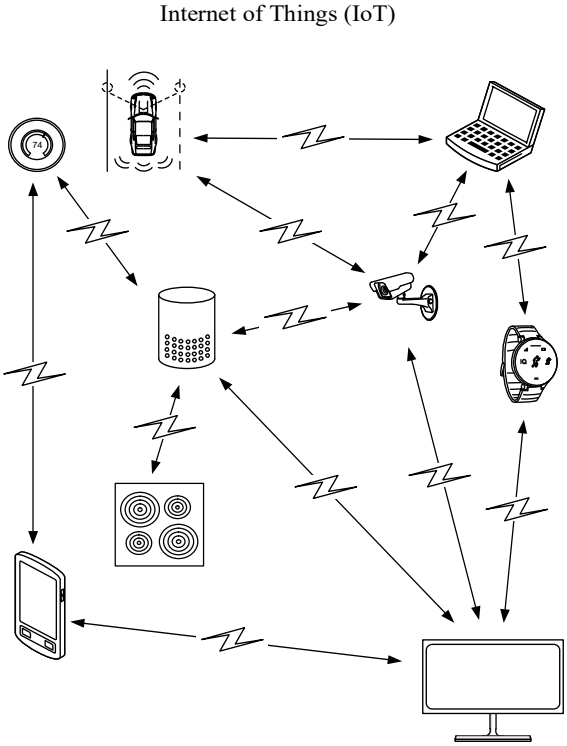

Fig. 1

In the IoT environment of Fig. 1, data may be collected by sensors of a device and shared with another device. Processing of data may be performed local to the device collecting the data or remote from the device collecting the data. Combinations of hardware (*e.g.*, sensors, microprocessors, memory), software (*e.g.,* algorithms, GUI's), and services (*e.g.*, communication networks) may be used to sense, collect, and exchange data. Large amounts of data are expected to be exchanged, as part of the IoT, across a horizon that is developing and changing frequently.

Detection mechanisms that may be built into IoT devices, such as light sensors, radar systems, proximity sensors, imaging sensors, cameras, or microphones, may measure conditions of an environment surrounding the IoT devices. Furthermore, and in some instances, computing algorithms may be applied to the conditions, as measured by the IoT devices, to assess aspects of the environment, examples of which include identifying a person who might be within the environment, quantifying movement of an object within the environment, or detecting a manufacturing anomaly within the environment.

This integration of devices has many user benefits, but it can also have its drawbacks, as demonstrated in Fig. 2.

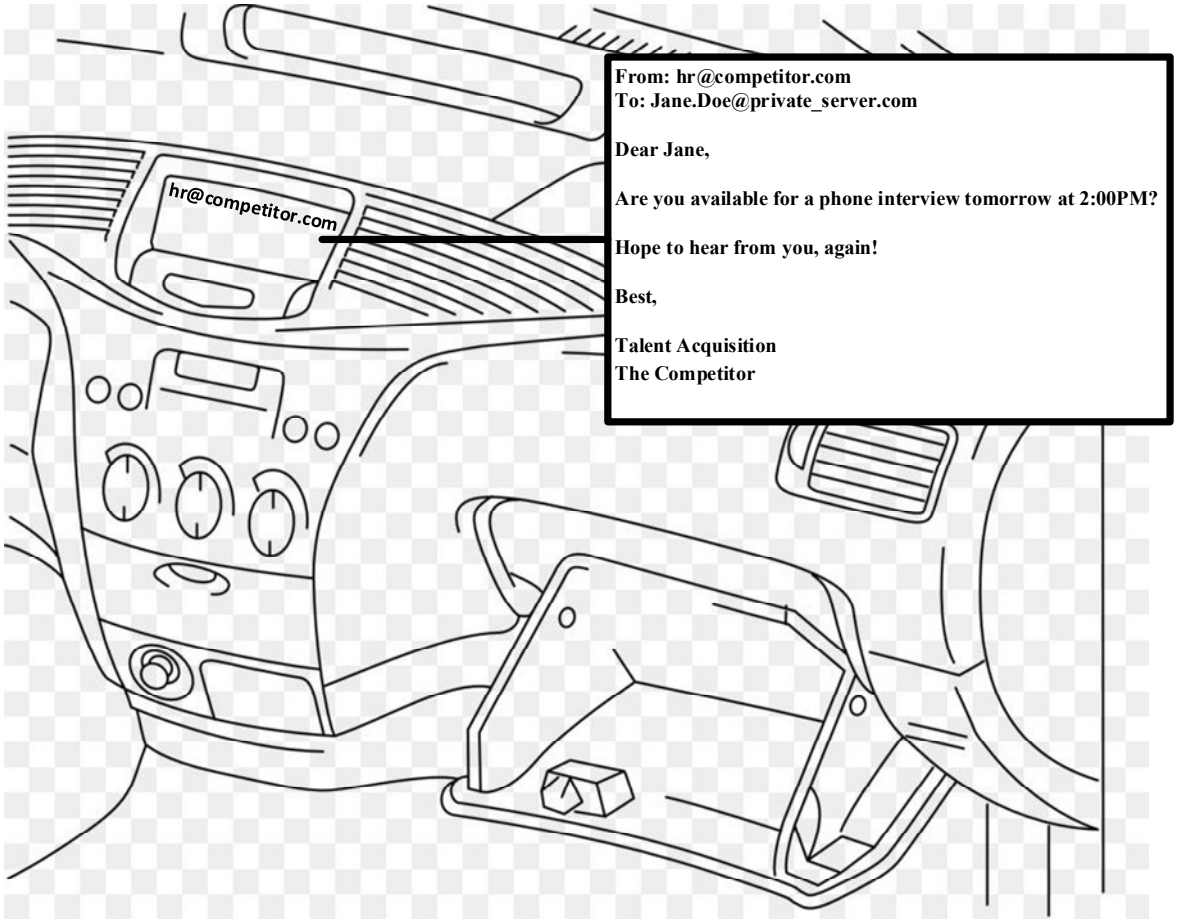

Fig. 2

In Fig. 2, consider Jane is driving her car, and she is conscientious about the risks of distracted driving. To this end, she wants any phone calls, messages, and emails to be displayed on her car's dashboard and read out loud on her car's speaker system; this way she can have both her hands on the wheel. Now, consider Jane and her coworkers are driving from a weekly team-lunch, and Jane receives an email from a prospective employer; the email is displayed on her dashboard and read out loud. A person can imagine how awkward, embarrassing, and, potentially,

detrimental this may be for Jane. The smartphone and the car indiscriminately display content whether one is alone, with coworkers, strangers, clients, friends, or family.

But, even if an operating system (OS) of a smartphone, computer, or any other IoT device was capable to distinguish a work setting from a personal setting, the indiscriminate display of content still has its drawbacks, as demonstrated in Fig. 3.

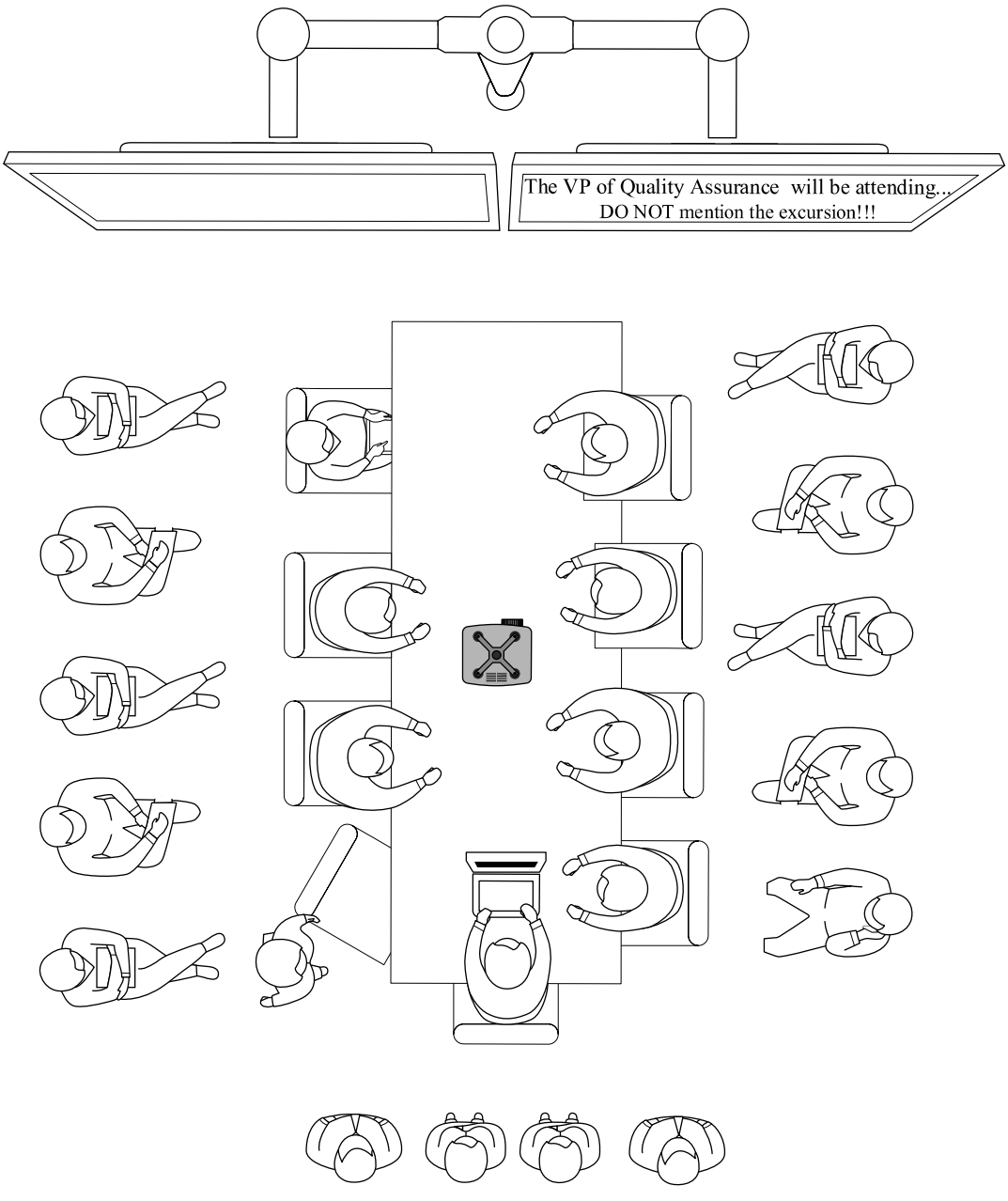

Fig. 3

In the scenario in Fig. 3, Jane is using her work laptop to go over the manufacturing data of the past 24 hours. She has logged in using her employee credentials. She thinks she knows her audience; process engineers usually attend the morning meeting. Now, consider that over the past 24 hours, there has been an excursion (e.g., an unplanned process deviation) in the manufacturing plant. The engineers have not had the chance to look at the data—let alone understand the problem or its root-cause. Jane's director hears that the Vice President of Quality Assurance has decided to attend the meeting, and messages Jane to not share the excursion event in this meeting. Such message being displayed during this meeting may have detrimental effects for the team and the company, because it is in the company's best-interest for the right message to be shared with the appropriate audience and at the appropriate time.

Furthermore, Internet-of-Things is becoming increasingly user-centric, and this may also have its disadvantages. Even in a family setting where the trust level is high, the privacy still needs to be protected. When Jane logs in her personal account and consumes media with her family, certain targeted advertisements can be inappropriate for some members of the family (e.g., an advertisement on a medical condition, adult content, or a surprise vacation that Jane may have been planning with her family).

Therefore, Internet-of-Things, with its increased individuality and device-interconnectivity, poses a question: what is the definition of a user?

Description:

A smartphone and other IoT devices contain sensitive information, such as: text messages, voicemails, emails, location history, contacts, search history, and other device usage history. When a person is alone, displaying this information on any display is appropriate. Nevertheless, when a user is occupying a space with others, it may not be appropriate to display private content. Furthermore, the level of trust and sensitivity (e.g., appropriateness) changes based on the occupants of that space.

Traditionally, in any OS, a user is a single person who is signed into a device. Furthermore, multiple users may share a device, but only one user is signed in at a time. An augmented OS changes the user's experience by incorporating the following parts:

1) The OS defines the user as the sum of all individuals in a shared space.
2) The OS filters the displayed content on a shared device based on trust level.
3) The OS filters the displayed content on a shared device based on a sensitivity level of the content relative to the trust level.

To define the user, the OS evaluates each occupant of a given space by employing facial recognition, radar signature, biometric sensors, media address control identification (MAC ID), voice recognition, other sensors (e.g., in car seats), radio-frequency identification (RFID (e.g., an employee's badge)), or other IoT data.

After the OS evaluates the user, it evaluates the trust level amongst the occupants. As one example, if an individual works as a driver for a ride-sharing or a taxi company, the trust level amongst the occupants is none; the phone does not display any personal data on the shared display (e.g., the car's dashboard). As another example, if an individual is driving with coworkers, the trust level amongst the occupants is low; the phone filters out personal information but may allow

some companywide announcements to be displayed. And, as yet another example, if a person is driving with a spouse, the trust level amongst the occupants is high, but the OS still evaluates the sensitivity level; the phone may filter out information when the spouse is mentioned in an email or a text message (e.g., a sibling may share an opinion regarding the spouse).

Furthermore, to realize the newly-defined user as the sum of all individuals in a shared space, the OS may merge several individual account information (e.g., contact lists, play lists, email accounts, software applications, etc.). In this fashion, when a trusted group (e.g., a couple or a family) occupies the same space, the displayed content is the same regardless of the logged-in user. Still, the OS may filter the displayed content based on the sensitivity level.

To filter the displayed content based on the sensitivity level, the OS may prompt the user to apply labels to a contact list (e.g., family, friend, coworker, client, etc.) and assign a trust and a sensitivity level to each contact. Alternatively, the OS may use machine learning or artificial intelligence (AI) to evaluate the user by interpreting the interaction amongst the occupants of a shared space.

Fig. 4 helps demonstrate how machine learning, via a neural network, may be used in determining the newly-defined user.

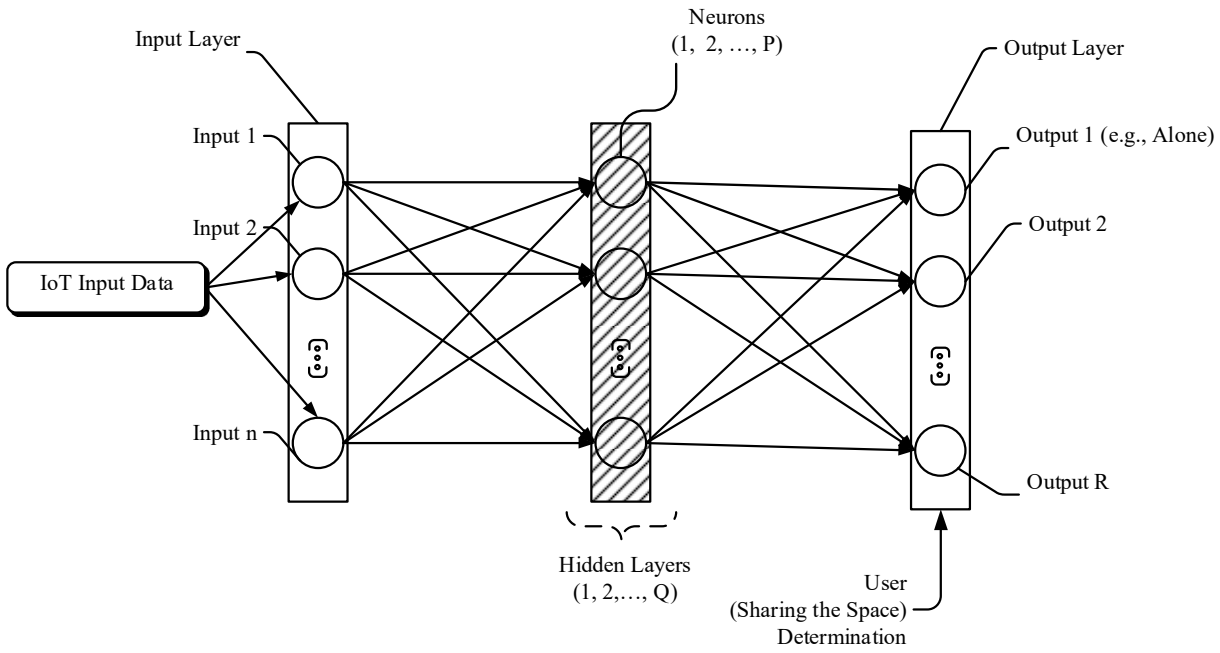

Fig. 4

The neural network in Fig. 4 may evaluate IoT input data (e.g., RFID, MAC ID, facial recognition ID, car seat sensor, voice recognition, motion sensor, etc.) from the occupants of a space. The output layer may consist of several bins, which may represent different occupancies (e.g., alone, alone with the spouse, the whole family, the whole family plus one yet-to-be-determined person, etc.). In the case when the neural network is unable to make an exact determination of who is occupying the space, the OS may train the model with future device usage patterns or may follow up with some questions. For example, the OS may have sniffed an unknown MAC ID and, in a more opportune time, may prompt the logged-in user to identify who was in the shared space at a given time, and assign a trust and sensitivity level.

This technology may also be incorporated to various access control lists (ACLs) used to control the traffic entering a network. It can enable a family, business, or organization, to control and filter the displayed content in a shared space.

The Internet-of-Things, with its individuality and device-interconnectivity, benefits by the OS re-defining the user as the sum of all individuals in a shared space and filtering out displayed content based on levels of trust and sensitivity for that summed user.