How the Internet of Things Will Change the User Experience Status Quo

Noel Portugal

Oracle Corporation, Applications User Experience, Austin, Texas, USA
noel.portugal@oracle.com

Abstract. The Internet of Things (IoT) will find its way into the way we work. As sensors and other connected devices invade our homes and places of work, we will expect an increase in new emergent ways to harness all this data to our advantage. Having intelligent context engines will be the glue that brings disparate data streams together. As we learn how we can use this data it will change the way we work and interact with our systems, effectively changing the User Experience (UX) status quo. This paper will explore the opportunities that IoT brings by collecting user data to help determine its context and offer a more compelling User Experience.

Keywords: IoT, UX, Location, Sensors, Context engines, Big data.

1 Introduction

We can define User Experience as the complete experience to accomplish a task. A successful User Experience will enable users to produce creative insights, make timely decisions, and complete their work in an accurate and efficient manner.

In the current state of the User Experience we tend to rely on the contextual information provided by the system. This information is limited by explicit data previously recorded into the system. Data such as profile, role, and access control lists (ACL) help the user access relevant information stored in the system. This information may not be enough to help the user accomplish all necessary tasks effectively.

We currently rely on manually captured data to make informed decisions in our day to day work. We also have had the need for personal or executive assistants to help us accomplish time consuming work. Work such as meeting scheduling, calendaring, meeting notes and material distribution. As the knowledge worker task-force increases and organization budget restrictions increase it might not be possible to have this kind of aid for all users.

In the past it has been widely discussed how smart connected devices can help the manufacturing industries and any industry in general using Enterprise Resource Planning (ERP) based systems. Tasks such as real-time inventory tracking, temperature monitors, and resource allocation have been previously discussed as prime candidates of the Internet of Things applications.

M. Matera and G. Rossi (Eds.): MobiWIS 2013 Workshops, CCIS 183, pp. 1–5, 2013.
© Springer International Publishing Switzerland 2013

A sensor or detector measures physical quantities and converts them into a signal that can typically be read by an electronic instrument. Internet connected sensors and devices are what has become known as the Internet of Things. The next frontier is the application of these connected devices in our day to day work. The Internet of Things expands a brand new way to enhance the applications User Experience. Sensors and other connected devices can collect invaluable information that can collectively help us work in a more efficient way. Location data will be one of the most important measures to deliver the right content at the right time and to the right person.

Physical presence is one of the most important metrics used to provide a better User Experience using the Internet of Things. Indoor activities and interactions with other users will prove to be of great insight when analyzed by smart systems. By tracking the user inside movements and interactions with other users, intelligent systems will be able to make better recommendations on how to accomplish tasks in a more efficient way.

Raw data coming directly from these interconnected devices will not be completely valuable unless it is first uploaded to a global repository and processed by a context engine. A context engine is needed to help make sense of all this information and should make smart decisions based on predefined rules. As context engines mature they will also learn patterns and make appropriate suggestions based on historical data and complex algorithms.

2 The Cloud and Big Data

As more devices are enabled with connected capabilities the need for capable repositories that can be easily accessed by any system and with the right access authorization is crucial. This global repository solution is the Cloud, which is a network of computer systems. The Cloud has become the de-facto home of Internet of Things repositories.

Current advances in location technology are making it easier to track an individual's physical presence. The key to these advances is not just better Global Positioning Systems (GPS), but a combination of data coming from different sensors and devices such as Wifi routers and smartphone sensors such as gyroscopes, compasses, and barometers (to detect altitude). The data provided by these sensors can yield a more precise location even if the user is indoors. Radio frequency technologies such as passive or active Radio-Frequency Identification (RFID) and Bluetooth sensors could also help provide accuracy. Near Field Communications (NFC) is another alternative to keep track of physical presence. In the case of NFC the user has to implicitly log its location [1].

As more Internet of Things devices are added to our ecosystem it is important to maintain a standard way of communicating with each other. A possible way to do so would be to follow Representational State Transfer (REST) style architectures applied to each device. Each device can potentially call any other device by using any of the REST-style methods such as GET, POST, PUT, and DELETE. Any connected

device could potentially be accessed inside the local network (Intranet) as well as from the Internet, with the assumption that security protocols have been set in place.

As sensors upload data at exponentially faster rates the remote Cloud repository becomes a Big Data source. Big Data is defined as a large collection of data sets that conventionally are not easily processed by traditional relational database tools. The data collected by Big Data repositories on the Cloud do not always necessarily have to adhere to ACID (Atomicity, Consistency, Isolation, Durability) database properties. Instead data stored in Big Data datasets can yield better results when properly analyzed for trends and patterns.

3 Context Engine

An intelligent system is needed in order to effectively use the massive amount of data generated by sensors and other IoT devices. These devices are constantly uploading data to Big Data repositories. This system is what I call a Context Engine. A Context Engine has the job to provide relevant information to a user according to that user context. This context is created by a combination of data provided by the following:

- Explicit data from the system (profile, access control).
- Implicit data collected from the user local environment (cookies, local time).
- User based rules and workflows.
- Data collected by various sensors and devices (location, heat).

The Context Engine is responsible for providing meaningful connections and suggestions. As more data is added into the system, the engine will have better recommendations. The context engine also has the capability to reach into other

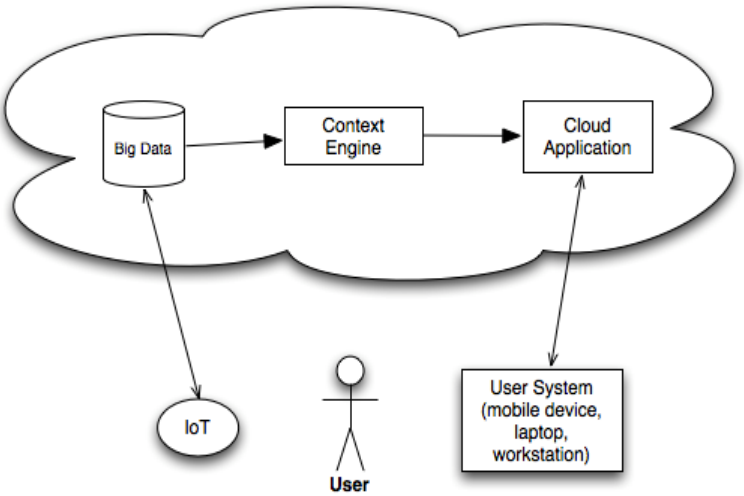

Fig. 1. Context Engine Diagram

systems to collect data to compliment its output suggestions. The architecture of the Context Engine is generally an independent system that can be queried by other systems. Communication is done by common internet protocols using a REST API architecture with proper authentication methods.

4 Use Case

The following example provides a scenario for the ability of IoT to track physical presence in the workplace: A user comes to the office in the morning. As he enters his office the lights come on and temperature is automatically adjusted to the user's predefined preference. Since the system knows who he is and his role it will present the user with the day's tasks to accomplish. As the day goes by a co-worker stops by his desk and ask a few questions. Since the system knows who the co-worker is it will display outstanding activities that involve that co-worker. Now the user has a reminder to inquire about these activities and set up a chance to follow up.

After lunch the user attends a meeting in a conference room. The conference room has sensors that can tell who is in the meeting. All meeting attendees are automatically added to a virtual conference where they can review the material in their own systems and make annotations that will be shared with the team in real time. The system can send meeting notes, recordings, and materials discussed to the people who could not attend the meeting.

Before the day is over, another user happens to walk by the user's desk. These two users do not know each other. The system recognizes the individual and prompts the user to inquire about a project which both have common interests but never had to physically meet and discuss. Anytime the user walks away from his office, his system and access to records are automatically locked. These are only available while he is in the geo-fenced area of his office.

5 Privacy and Security Considerations

It is very important to recognize that as we want more precise data, we will have to explicitly allow these sensors and systems to monitor us. The ability to receive a personalized experience comes with a price. One consideration will be who will be able to see this data. Collectively this data will be helpful, and it could be publicly available. Individually data should be more protected and only shared with authorized parties.

An opt-in mechanism is a must if we want the users to confidently trust the system. By giving the user the choice, I believe users will find the positive outcomes far greater than the negative outcomes. Some places of work might require a mandatory agreement to allow this monitoring, but it is up to the user to agree to work there or not.

There is generally a wide perception that IoT devices are inherently insecure. This notion comes from the fact that these new internet citizens lack the human factor to establish communications and can be completely autonomous. As a starting point to

resolve this the IoT need to adhere to existing security mechanism used on the web. Authentication methods such as OpenId, as well as authorization methods like oAuth should be used whenever required. Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL) protocols should also be used to provide secured communications on the internet.

Legal frameworks have been suggested to assure that IoT devices will comply with paradigms of IT governance, ensuring resilience to attacks, data authentication, access control and client privacy [2].

6 Conclusion

The Internet of Things is poised to change the way we currently work. It will not be just one single device or sensor that will give the necessary information. It will be a collection of explicit and implicit data collected by smart devices that will be able to provide better personal context to our systems. The current state of User Experience is limited by the system explicit constraints. As we feed the system with more relevant data, the user experiences will be more rewarding.

References

1. Teixeira, T., Dublon, G., Savvides, A.: A Survey of Human-Sensing: Methods for Detecting Presence, Count, Location, Track, and Identity. ACM Computing Surveys V(N) (20YY)
2. Weber, R.H.: Internet of Things – New security and privacy challenges