EJMS
European Journal of Management Studies

THE INTERNET OF THINGS: THE PERSONAL AND SOCIAL DOMAIN

The European Journal of Management Studies is a publication of ISEG, Universidade de Lisboa. The mission of EJMS is to significantly influence the domain of management studies by publishing innovative research articles. EJMS aspires to provide a platform for thought leadership and outreach.

ISSN: 2183-4172
Volume 20 Issue 1

www.european-jms.com

Industry Report

Kane Smith, Sai Veena Ravulapati, Yogesh Daga, and Dheeraj Sai Naga

Virginia Commonwealth University, Richmond, USA

The Internet of Things, or IoT, is meant to refer to the vision of the Internet where one is not only connected anywhere and anytime, but to everything – from the tire of our car, to the toothbrush that we use. It acts as a nervous system, where anything is connected to everything in the world (Morgan, 2014). The Internet of Things, which is a new buzz word, is not a second type of Internet. It is a network of objects, which are connected through the Internet and which are able to share information amongst themselves though sensors embedded in them. Putting all of this in more simple words, the IoT is an interconnection of networks. This network might consist of anything, from cell phones to ear phones, lamps, wearable devices or all of the above (Denning, Kohno and Levy, 2013). It is going to be one giant network that includes people, and as said by Gartner, there will be more than 26 million devices connected to each other by 2020 (Morgan, 2014).

In the not so distant future, anything which can be connected will be connected, becoming the norm for daily life and there are number of examples which explain the potential value of doing so. Let us imagine that there is an important meeting that needs to be attended and that you are stuck in traffic. Your car then sends a message to the other party advising them that you will be late. Another example is that you are driving your car back home, and your home gets to know that you are near and then automatically opens the garage door and lights up your house. Also, your refrigerator knows that there is a shortage of supplies for eating, and thus places the order, etc. Soon it may come to

pass that a refrigerator knows more about a person's diet than a Doctor or dietician as it better tracks a person's food habits. Since in

this scenario it is possible we are talking about millions of devices, with some experts believing that this number might even go up to 100 billion or more, is it possible to provide IP addresses to all of them and connect them through the internet (Morgan, 2014)? All these interconnected things must have an IP address that allows them to share information over the internet. But how can this be done, especially if IPv4 addresses have already reached their limitation? With the use of IPv6, where the address is 128 bits and can then provide a vast number of IP addresses, more than the number of atoms in this world (Wigmore, 2009).

The IoT can be applied and used in various domains, such as healthcare, transportation and logistics, the smart environment and one's personal and social life (Atzori, Lera, and Morabito, 2010). The focus of this paper will be on the Social and Personal Domain of the Internet of Things. As the name suggest, Personal and Social Domain applications falling under this theme are related with the personal and social aspects of one's life. This allows an individual to stay connected with the world, via the use of social networks. With the IoT, it might come to pass that automatic messages are triggered to friends allowing them to learn what we are doing, where are we travelling to or whether we are moving from work to home (Atzori, et al, 2010). There are four major applications within this domain which are: Social Networking, Historical Queries, Losses, and Thefts (Atzori, et al, 2010). Each one of these will be explained in this paper, with examples given and their current and future states reviewed, and finally the risks associated with each application will be discussed.

The first application in the Personal and Social Domain is that of Social Networking (Atzori, et al, 2010). In this age, where one can have an account on LinkedIn or Facebook or Twitter, everyone is connected to their closest ones by just updating a post about where they are, or what they are doing (Ampofo, 2014). However, with the evolution of IoT, it is quite possible that connected devices, such as wearables, will update your status. In addition to this, even an individual will be able to maintain a friend list to whom their personal information will be disclosed (Atzori, et al, 2010). This hybrid interconnected network will act as a base foundation for creating unique online social experiences. As everything will be connected and communicating with each other in a useful manner, there will be a reflective and exponential change in the way organizations interact to serve their customers, and also regarding how devices will serve their users as well as fundamentally altering the concept of security and user privacy, something that will certainly require attention and redefinition due to the IOT (Rozenfeld, 2014). In the age of social IoT, users will have the ability to share every aspect of their life, regardless of how small or insignificant it may be (Ampofo, 2014). Many of the challenges faced by social IoT can be discussed with respect to both privacy, security as well as Interoperability (Denning, et al, 2013). Technology alone is not able to keep data secure with either new or old systems. It will be incredibly difficult to secure data with as much as innovation as the IoT will bring (Denning, et al, 2013). Information will be available quite easily and, with the devices that users are envisaged to have in the future, it will all be linked in one way or the other, and will provide an ample incentive to those with malevolent intentions (Denning, et al, 2013).

A number of people still have their personal information open to everyone on social networking platforms and all their sensitive information can be accessed by a single click (Denning, et al,

2013). People do not really understand the importance of safeguarding their personal data on social platforms which is available there for everyone. With the evolution of IoT, where so many devices will be connected to each other, this information will become even more critical (Denning, et al, 2013). Social engineering has been the most common problem that businesses have faced up to today, and with so many devices where sensitive information of an individual is readily available, this might pose a huge threat to individuals, as well as to businesses. Within the context of social networks, information can be seen as flowing out in a manner that is not controlled by the user. Suppose for instance, someone is looking for new sunglasses on lenskart.com, in a span of few hours an advertisement related to lenskart.com will appear on their Facebook wall. This demonstrates that Facebook knows everything that a person is doing on their site and that it knows everything about you and what you are planning to do when you post information through Facebook (Siciliano, 2009). And if many devices get connected to each other and these social platforms, as we are suggesting, then it is not hard to imagine how data will flow between them, making them more vulnerable. No matter how innovative and capable the IoT seems to be, this phenomenon certainly increases a number of security risks that might be faced by businesses and individuals alike. The probability of devices being connected to the Internet and having an operating system which is vulnerable is high, and this may become a backdoor entry for attackers (Rozenfeld, 2014). All these devices will have an embedded OS in their firmware, and as an embedded OS is not designed to keep security in mind, vulnerabilities can be easily exploited. Looking at the number of malware attacks on smartphone devices for instance, it is not difficult to expect the same thing happening with IoT devices as they increase in popularity. This concern about privacy and data is not new to the Internet of Things, as similar issues were faced during RFID adoption (Rozenfeld, 2014).

The second application for discussion in the Personal and Social Domain is that of Historical Queries, where data about events and objects can be tracked over time and thus allows users to then study them (Atzori, et al, 2010). The idea of data being tracked for later study is not a new concept, and it has been in use for some time. There are a number of different companies and applications that utilize this concept to great effect. One particular company is Google, which has such a vast expanse of user data that it can use someone's search history to predict which results would most ideally suit that person. However, in this sense it is more about moving that capability to the user themselves to study or learn about their own behavior, in order to create some type of positive effect (Atzori, et al, 2010). One particular example is Google Calendar, as any type of calendar system that allows a user to record appointments, events or their activities should be capable of providing the necessary data for study (Atzori, et al, 2010). These bits of data, if set over a long enough period would allow the user to then study their past action to determine how they are spending or utilizing their time (Atzori, et al, 2010). A graphical analysis could provide a user the information necessary for deciding whether they are using their time effectively, or whether they are spending too much or too little time on a particular event or activity (Atzori, et al, 2010). One such example could be that a user notices that they spend 15 minutes every morning clearing out old emails which means that their day does not start right away. If, for instance, this activity had done been it while they were eating breakfast,

or during the 20 minute train ride to work, then their day could start as soon as they get to work, perhaps even allowing them to leave earlier at the end of the day.

The current state of historical queries exists more at a corporate level, and is used by companies such as Google to leverage advertisements and targeted search results for the consumer. Very little has been done to allow the user themselves to track or study their own behaviors through the accrued data. In the future, products such as calendars that allow users to record data entries could be expanded with statistical capabilities which users themselves could access and exploit to better manage their time. Corporate tools like Microsoft Project could even be leveraged to provide an even better analysis of group projects, which could save companies large amounts of money by analyzing how employees spend their time working on various assignments. While the advantage of using historical data seems very obvious, and would be greatly welcomed by many, there are inherent risks associated with storing and accessing this type of data about the application's user.

While discussing the subject of storing and utilizing personal data, even for simple historical analysis, it is important to note the single greatest concern can be considered that of user privacy due to the nature of the data being stored and its value to criminals (Denning, et al, 2013). Tracking every aspect of how a user spends their time in a given day is always open to abuse. One thing which is often overlooked is when employees use personal devices at work. Many times one's business calendar is synchronized with one's personal phone, and can thus be viewed by your company. The potential of using information gained about what someone does on a day off, or if they had called in sick can be very tempting. An employer may be very interested to know whether an employee is really sick, or whether they are just abusing the system to gain an extra day off work. Additional abusive behaviors can occur when private information is accessed without a user's permission with the purpose of exploiting it for profit. A current risk of companies like Google having such an immense wealth of historical data is that this data can be used to specifically target a user with the only goal being motivated by profit, while potentially adding no real benefit. For example, a user's past search trends may indicate they have a strong affinity for dogs, and a search company could then target that user with ads to solicit donations for a particular animal shelter, fund or product that may give companies a kickback for a referral. While this may seem like an extreme example, Google is currently involved in litigation all over the world about its search results being filtered to give its own partners a better position in search results, likely a result of receiving greater compensation for users selecting those links or products from a search over another. The idea then of taking the tracking of user behavior further to simply exploit that information for profit is not an unlikely scenario, especially as we move towards greater user-integration within the Personal and Social Domain.

The third application within the Personal and Social Domain is that of Losses (Atzori, et al, 2010). There are few things, which are very important in our day to day routine, which we cannot afford to lose. Car and house keys, our cell phone, wallet, laptop, or even the parking lot number where we park our car are some examples. If just one of our personal items goes missing, we then panic and try our best to recollect the place or location where we saw them last. We are

often not capable of finding them ourselves all the time and can end up wasting a lot of time and energy, in these seemingly frequent situations. For this purpose, many tracking applications are available today which have been developed to help us find lost objects, pets, or even people.

The following are examples of tracking applications which are very effective in locating lost objects:

Tile Tracker: A Tile tracker is a device that helps us to find any object that it is attached to. It is a small device, which can be attached to a cell phone or keys or any desired object. The lost object can then be located using the Tile application on our phone where a map is used to guide us towards it, along with a beep pointing out the object's exact location (Armstrong, 2014).

Tagg Pet Tracker: When a pet goes missing, we can locate it using this application. This tracker has got a GPS system, which can be attached to the collar of the pet. The location of a pet with this tracker can be monitored using a computer or a cell phone (Armstrong, 2014).

GPS Tracking Freedom Wallet: Locating a wallet is a hideous task and the fear of losing one's credit/debit cards or money makes this process even more difficult. However this task can be accomplished with the help of GPS Tracking Freedom Wallet by Royce Leather. This tracker is small in size and can thus be placed into any of the slots of the wallet, which can then be tracked using a smart phone via GPS (Armstrong, 2014).

Find My iPhone or Android Device Manager: We have learnt about the tracking applications that can be used with the help of cell phones. What if we lose the phone itself? To help us find lost iPhones or Android phones, a tracking application is available which is called Find My iPhone or Android Device Manager. This application can be used to track down a lost smart phone using a computer or another cell phone, via GPS. The phone can be found with the help of a beep, and if that does not work, then one can even send a message to the phone itself saying, "this belongs to x, who should be contacted at…" which will be displayed on the phone's screen (Armstrong, 2014).

Click-N-Dig: This is another tracking application which can be used to track a TV remote. But to do this, one does not need a smart phone or a computer, as this tracker comes with a transmitter and the remote can be tracked with the help of the receiver attached to it, which flashes when we press the transmitter (Armstrong, 2014).

Technology can be amazing and do wonders that are often beyond our imagination. However very rarely do we realize that all the personal devices such as cell phones, laptops, tablets etc. that keep us connected through the IoT, do so at a cost to our privacy (Denning, et al, 2013). This means that the Social and Personal Internet of Things are always interconnected. For example, most of the time we keep ourselves logged in on Google accounts such as Gmail or Google+ on various personal devices, such as a cell phone, laptop or even a tablet. Yet this is where we fail to remember the fact that the information is being shared on a greater number of devices, increasing our risk of being hacked and of exposing personal information, or in the particular uses described above, where our most valuable possessions are being kept (Denning, et al, 2013). The risks associated with tracking a person or object can always related back to

privacy and the use of any data acquired through that tracking (Denning, et al, 2013). If users are storing data about where they keep their most personal and valued possessions, then if that data is misused in any way, the user has, in effect, told a potential criminal exactly where they need to go to find the best and most worthwhile items to steal. Government agencies could easily exploit these types of systems to track people without their consent or knowledge as well, perhaps even without a court order. Deciding who has access to this data as well as where and how it should be stored will be of great importance when debating the extent to which this aspect of the Personal and Social domain should be expanded.

The fourth and final application within the Personal and Social Domain is that of Thefts (Atzori, et al, 2010). The Internet of Things has made it possible to connect the virtual world of bits, 1's and 0's, to the world of physical objects and people. It enables normal objects in life to become integrated in daily life, and with the advent of a fully-evolved internet and analytics, it will be possible to create a seamless world, in which people and technology and indistinguishable from one another. There are many types of tools which are being designed and some of pilot studies are already underway in the social and personal domain with the goal of preventing theft. Securing personal gadgets, equipment, and, in fact, homes, is becoming more easily possible with the Internet of Things (Denning, et al, 2013). Indeed, smart homes are already popular, whereby a single application on a smart phone or a smart watch can control anything, from anywhere (Denning, et al, 2013). This type of application can allow users to not only track an object, but it can also be used to notify them if the object has been moved without permission (Atzori, et al, 2010). An object can have a defined set of parameters that restrict its allowed locations and if it is moved outside of them, an automatic notification is then sent to the user, or even the authorities. This type of device is not restricted to just smart homes, as it has potential for both personal as well as commercial use.

Currently, we already have 14 billion sensors in the world, and by 2020 there will be at least 26 billion sensors, with some research firms even predicting upwards of 75 billion devices by this time, connecting everything with everything else (Basenese, 2014). Basic alarm systems have been in use for decades with sensors inside of homes, but within the last few years, new systems from companies such as Comcast, have allowed homeowners to take full control of their home. Users can now monitor and control everything from locking the doors, changing the temperature, seeing how many times someone goes in or out of the home, or who is inside, and where they are located. Companies involved in shipping also use a technology that lets them track packages in real-time, so that they always know where the package is, and they can provide customers with constant location updates (Schoenberger, 2002). The ability to take this concept further simply blends those two ideas together and moves this beyond the basic tracking packages to that of tracking every item within the home through the use of RFID tags (Schoenberger, 2002). The blending of these two ideas provides the capability to track items owned by an individual or company, as it can allow users to protect their personal things which are connected through the IoT, and also permit businesses to ensure, for example, that the company's equipment is not taken off site or away from restricted areas.

The risks inherent to this aspect of the Personal and Social Domain are similar to that of Losses. When data is held about where a person or object is located, it then becomes very valuable to someone who might be able to profit from this information (Denning, et al, 2013). An employer would likely want to know where their equipment is at all times, but may also be interested in knowing where their employee is at all times, even when they are not working or they could use RFID scanners to pick up information about customer's who have devices that are RFID enabled (Schoenberger, 2002). This would be a clear violation of one's personal rights and privacy, but it is just a simplified example of what is possible, when this aspect is not fully thought through and is not subject to proper rules and regulations regarding the handling and access to this type of data. Users will need to demand clear protections of their rights through the regulation of this issue, in order to protect their privacy (Denning, et al, 2013).

The Internet of Things is a vast network with interconnected objects that interact through the internet (Atzori, et al, 2010). The Personal and Social domain is quickly growing to become one of the largest users of the IoT, as people plug in to social media everywhere they go, upgrade their homes and businesses with new "smart" systems, and begin to track and study their daily habits. This domain is growing and advancing every day, and is marching inevitably towards a world were massive amounts of very personal data will be potentially vulnerable to all means of abuse. It will be up to users to demand protections for their data when using and connecting through these devices within the IoT (Rozenfeld, 2014). Users will need to be educated about the dangers, as well as the benefits of these devices, in order that they can make informed decisions not only about their use, but also about their continued development (Rozenfeld, 2014). The Internet of Things can bring a great deal of innovation, ease and wonder to the world around us, by allowing interactions with even the most innocuous of objects. The ability to envelop ourselves in an endless digital world will be a strong urge that is hard to resist in a society that is fascinated with technology, however it is necessary at least to look at the risks, as well as the benefits, and to assess for ourselves how far we want to take the Personal and Social Domain within the Internet of Things.

References

Ampofo, L. (2014, October 24). 5 Ways the Internet of Things Will Change Social Media. *Business 2 Community*. Retrieved January 21, 2015, from http://www.business2community.com/social-media/5-ways-internet-things-will-change-social-media-01047822.

Armstrong, M. (2014, June 30). Where's the remote? 5 best tracking devices to find lost items. Retrieved January 21, 2015, from http://www.today.com/money/lost-found-5-best-tracking-devices-find-misplaced-items-1D79862951.

Atzori, L., Lera, A., and Morabito, G. (2010). The Internet of Things: A Survey. *Computer Networks*.

Denning, T., Kohno, T., and Levy, H. (2013). Computer Security and the Modern Home. *Communications of the ACM*, Vol. 56 No. 1, Pages 94-103

Basenese, L. (2014, August 28). Internet of Things Creates New Security Risks. Retrieved January 21, 2015, from http://www.wallstreetdaily.com/2014/08/28/internet-of-things-security/

Morgan, J. (2014, May 13). A Simple Explanation of 'The Internet of Things'. *Forbes*. Retrieved January 21, 2015, from http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand.

Rozenfeld, M. (2014, March 7). The Value of Privacy. *The Institute*. Retrieved January 21, 2015, from http://theinstitute.ieee.org/technology- focus/technology-topic/the-value-of-privacy.

Schoenberger, C. (2002, March 18). The Internet of Things. Retrieved January 21, 2015, from http://www.forbes.com/global/2002/0318/092.html.

Siciliano, R. (2009, August 28). Social Media Privacy and Personal Security Issues. Retrieved January 21, 2015, from http://www.huffingtonpost. com/robert-siciliano/social-media-privacy-and_b_245857.html

Wigmore, I. (2009, January 14). IPv6 addresses - how many is that in numbers? Retrieved January 21, 2015, from http://itknowledgeexchange.techtarget.com/whatis/ipv6-addresses-how-many-is-that-in-numbers/