Taxonomy for Internet of Things
Tools for Monitoring Personal Effects

Leon Barker, Martin White, Mairead Curran, Zeeshan Patoli, Benji Huggins, Tudor Pascu and Natalia Beloff
University of Sussex, Department of Informatics, Chichester 1, Brighton, U.K.

Keywords: Internet of Things (IoT), User Experience Design, Ubiquitous Computing, Big Data, Peer-to-Peer Networks, Cloud Computing.

Abstract: Human capacities to track and identify peers, products and activities have benefited from the wide proliferation of networked electronic devices; developments in smart-materials, near-field communication and computer-vision technology further advance these capabilities. During this investigation into The Internet of Things (IoT) a new taxonomy was created together with a set of prototype applications and accompanying architecture. In addition to presenting these taxonomies the creation of a peer-to-peer network with a distributed database is discussed. The development of a system that enables users to track and exchange objects or services using a secure and robust data repository model is also proposed.

1 INTRODUCTION

The research presented in this paper initially focused on investigating the types of activities, applications and behaviours that may result from the emergence of ubiquitous smart devices and the establishment of the Internet of things (IoT) infrastructure. Prototype applications have been created as a result and user trials are being conducted. This research was undertaken as part of a UK interdisciplinary Technology Strategy Board (TSB) Collaborating Across Digital Industries 2 (CADI2) project 'Connecting virtual communities to the digital economy through micropayment technologies'.

The IoT concept is not new; though originally proposed in 1999 (Ashton, 2009) and often discussed within the fields of Human Computer Interaction (HCI) there is little consensus regarding the composition and application of this concept. The lack of clear consensus creates obstacles that prevent holistic perspectives on the impact and composition of IoT infrastructures from being gained. This lack of consensus serves only to further reduce the capacity for interdisciplinary fields of research and industry to collaborate in the development of products and the evaluation of IoT systems. The outcome of such consensus would aid the development of a robust IoT system architecture. The creation of such a framework would provide a useful template to support and inspire developers to create novel IoT applications that are of genuine benefit to users.

The wide distribution of smart-devices not only allows users access to information regarding current and historic global events they also facilitate users with the ability to communicate with their peers. Moreover, through advances in technology users will soon be able to monitor there own bio-signals through the use of smart-fabrics such as temperature-responsive polymers (Crespy and Rossi, 2007), shape-memory polymers (Nji and Li, 2010) and polyelectrolytes coated with carbon nanotubes (Shim et al., 2008).

The rapid development of smart objects that have the capacity to access and broadcast sensitive information make the establishment of a consensus regarding the direction of IoT both significant and important to address. The establishment of a coherent IoT architecture would provide positive benefits to end-users of smart technologies by enabling the creation of agreed protocols that will help provide consistent user experiences and a layer of data security.

Though there are many obvious benefits to establishing a robust IoT system architecture there is also significant potential for conflict to occur between competing forces within technology and social sectors. As IoT systems by their nature are dynamic they can be configured in multiple ways and can either be networked as a centralised data repository or a decen-

Barker L., White M., Curran M., Patoli Z., Huggins B., Pascu T. and Beloff N..
Taxonomy for Internet of Things - Tools for Monitoring Personal Effects.
DOI: 10.5220/0004809500670071
In *Proceedings of the 4th International Conference on Pervasive and Embedded Computing and Communication Systems* (PECCS-2014), pages 67-71
ISBN: 978-989-758-000-0

tralised peer-to-peer network. The potential ramifications of each system configuration is outlined in section 2.2 of this paper.

Through the course of investigating the current IoT landscape a wide range of interconnected elements and components were identified. In an effort to provide a coherent frame of reference a set of taxonomy for describing the active elements observed during this investigation have been defined. This taxonomy is described in section 2.1 .

2 TAXONOMY OF THINGS

It is common for discussions regarding IoT to focus upon only one category of object; it is generally assumed that an IoT eco system is made up of networked electronic devices. Advances in near-field communication and computer-vision equip modern day smart phones with the ability to track and identify a wide variety of objects. This capability means a wide array of different object types can be contain within the IoT ecosystem.

2.1 IOT COMPONENTS

The categories of objects constituted within an IoT ecosystem have been observed as follows:

- Smart Devices;
- Persistent Nodes;
- Collectables;
- Actor/Sentient Agent;
- Semi Autonomous Agent;
- Loose Perishables;
- Gateways.

2.1.1 Smart Devices

The smart device in our IoT ecosystem describes a device or mechanism that is able to communicate its own presence or existence to servers and other listening devices over either a wired or wireless communication network. Typically a smart device also is equipped with sensors and is able to broadcast information about its local environment. Smart devices are generally assigned a unique ID, which they are able to both store and communicate.

2.1.2 Persistent Nodes

The Persistent node can exist in the mid to long term. It is part of a network and typically provides a service or storage function. These nodes have unique IDs, buildings and sensors can fall into this category. A warehouse can be a persistent node in a supply chain just as a weather vane can be a persistent node in a meteorological survey. Persistent nodes tend to operate in closed networks that access the outer world through gateways.

2.1.3 Collectables

Collectables can represent a wide array of objects such as books, teacups cornflake packets and any object that have been assigned a UPC barcode. These objects do not have unique IDs because it is impractical, as it would only succeed in creating a bloated database and no real performance benefits. It is only through association with other IoT object types that collectables can become unique.

2.1.4 Actors/Sentient Agent

Actors and Sentient Agents describe things that are by nature unique and are capable of acquiring collectable things. Sentient things exhibit free will and thus are able to make unprompted decisions about their actions. People obviously fall into this category and perhaps in the future some machines will also be considered sentient.

2.1.5 Semi Autonomous Agent

A semi autonomous agent is only capable of initiating actions once a super-user or systems admin has set specific permissions for a particular action. Once an action has been authorised a semi autonomous agent is capable of acquiring collectables and conducting tasks in a similar way to sentient agents.

2.1.6 Loose Perishable

Loose perishables consist of objects such as fruit and unpackaged foods stuff; it also describes objects with a limited lifecycle that would be impractical to assign an individual unique ID. Asides from their limited lifecycle loose perishables have the same characteristics as collectables.

2.1.7 Gateways

Gateways are essential parts of any IoT ecosystem as they are the link between interconnected networks. A router is the gateway that allows computers to access the Internet, just as the point-of-sale device (POS) is the gateway that allows banks and individuals to transfer funds to retailers and other such organisations. Gateways are the links between nodes and are

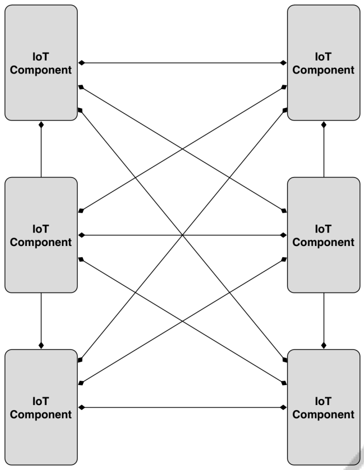

Figure 1: Category-One decentralised peer-to-peer network.

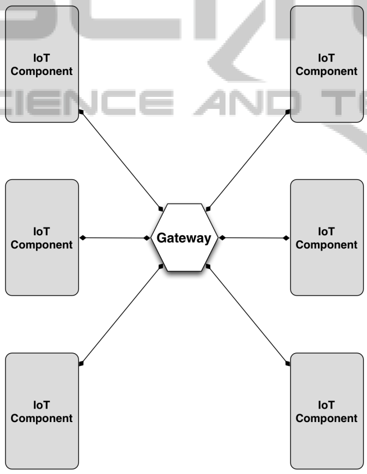

Figure 2: Category-Two centralised gateway repository.

therefore the key elements to consider during the development of security and privacy protocols.

It is possible for particular objects to fit more than one of the categories described, for example a loose perishable object could also be collectable for the duration of its lifespan. However once a thing is categorised it becomes easier to see how objects function within an IoT ecosystem.

2.2 Central and Decentralised Networks

Different network configurations are possible within an IoT ecosystem; for example as an IoT ecosystem is composed from many components it is dynamic and can be configured as either a centralised data repository or a decentralised peer-to-peer network. Currently, companies seeking to profit from IoT are attracted towards centralised cloud based architecture where data is stored in a central repository. This approach offers great potential and opportunity for companies to capture large amounts of data regarding the activities and habits of consumers. The emergence of big-data analytic tools currently demonstrates that messy data can be analysed to facilitate insight regarding the habits of network users. This type of architecture reflects a category-two (see figure: 2) infrastructure (Karimi and Atkinson, 2013), where all end nodes send data to centralised repositories. This type of network can draw upon pre-existing IT infrastructure where servers are centrally located in dedicated server farms throughout the world. This type of approach seems to ignore some of the novel attribute offered by an IoT ecosystem. One of the main attributes of IoT is the notion of the hyper-connectivity of devices. We are currently seeing the wide distribution of devices capable of communicating with other systems both globally and locally. The centrally located cloud based server that is seemingly being advocated by meanly companies ignores the potential of a local peer-to-peer IoT infrastructure. This type of architecture reflects a category-one infrastructure (see figure: 1) (Karimi and Atkinson, 2013), which encompasses a heterogeneous architectural model consisting of millions of peers.

By insisting that a device report back to a server that is often hundreds if not thousands of miles away we have ladened our personal devices with energy hungry telecommunications chips, which require these devices to be continually recharged. A lot of energy could be saved if our devices only had to interact with local networks. Through a single search query it is claimed that on average Google reads one hundred megabytes of data, which consumes tens of billions of CPU cycles (Barroso et al., 2003). Added to these processing requirements is the need to send the data via satellite and wired connections as well as server cooling issues; these factors illustrate the impact that a centralised repository has on power consumption.

To address the need for the creation of a peer-to-peer network that allows for the secure, accurate and robust transfer of sensitive and private information a modular data storage infrastructure needs to be created. A prototype infrastructure was instigated during the course of this research investigation. The proposed infrastructure will enable the transfer of information in local or global peer-to-peer exchange networks through widely distributed repositories.

3 IOT APPLICATION PROTOTYPE

There currently is no decentralised mechanism that enables mobile phone users to securely acknowledge the receipt and exchange of items. There are also few applications to facilitate the seamless transfer of lists between devices. Should a user wish to compile a lists of items such as ingredients for a recipe or electronic components to build a circuit, the user has to laboriously search for each individual item via third-party websites and inventories. The application developed during this project provides a mechanism for pushing lists to peers and merchants, whilst also providing a secure and seamless peer-to-peer record of exchange.

The emergence of hyper-connected objects with their own digital identities within IoT landscapes presents new opportunities for users to track and access information regarding their own possessions. The mobile application and supporting infrastructure presented has been designed to allow users to easily compile and access lists of owned objects, retail products and other things. Users are able to capture items via their smart phones using NFC, QR codes, barcodes, image-recognition or by manually entering the items description. Once a list has been compiled the user is able to push the list through desired channels. Using the application users can generate lists of recipe items and then purchase the item through an in-app shopping channel, by using the API of participating partners (see figure: 3). Alternatively a user might compile a list of items they plan to sell and use the app to list their items in auction or recycling channels such as Ebay or Freecycle. Using the framework developed users can even use the application to share books, music playlist, games and DVDs amongst friends, family and the wider community. In future scenarios users might store preferences for how their smart-fabrics and smart-vehicles should respond under specific social or climate conditions.

During the development of this demo application a peer-to-peer object archive framework was developed. The resulting application enabled users to seamlessly monitor possessions through their entire lifecycle (from purchase to disposal). Though initial development activity focussed on the redesign of a physical shopping basket it later became clear that the creation of a receipt repository for tracking general peer-to-peer transaction and interaction could offer wider benefits. Though an ever-increasing number of monetary transactions are conducted electronically there are few applications to facilitate seamless peer-to-peer transactions. The applications that do exist do not provide users with a method of recording the type of exchange both parties enter. The prototype application created through this research enables users to keep a record of past transactions through a distributed data store.

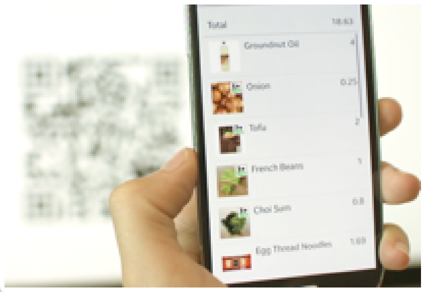

Figure 3: Category-Two centralised gateway repository.

4 CONCLUSIONS

The creation of the demo application is a trivial software development task, however the creation of a secure and robust decentralised repository that is distributed among a large peer-to-peer network is a significant challenge. We are beginning to see the emergence of exchange systems that exhibit the necessary characteristics to support decentralised peer-to-peer exchange. For example Bitmessage (Warren, 2012), Bitcoin (Nakamoto, 2008), Litecoin (Sprankel, 2013) and Namecoin represent cryptographic currencies and communication tools that offer decentralised peer-to-peer transactions. However these mechanisms do not include information regarding the item that has been exchanged and are designed to offer anonymity to both seller and buyers. The model we are developing would record the type of agreement each party has entered into as well as providing both parties with a formalised proof of exchange.

ACKNOWLEDGEMENTS

This research was undertaken as part of a UK interdisciplinary Technology Strategy Board (TSB) Collaborating Across Digital Industries 2 (CADI2) project 'Connecting virtual communities to the digital economy through micropayment technologies'.

REFERENCES

Ashton, K. (2009). That internet of things thing in the real world, things matter more than ideas. *RFID Journal. Retrieved from http://www. rfidjournal. com/article/articleview/4986/1/82.*

Barroso, L. A., Dean, J., and Holzle, U. (2003). Web search for a planet: The google cluster architecture. *Micro, Ieee*, 23(2):22–28.

Crespy, D. and Rossi, R. M. (2007). Temperature-responsive polymers with lcst in the physiological range and their applications in textiles. *Polymer International*, 56(12):1461–1468.

Karimi, K. and Atkinson, G. (2013). What the Internet of Things (IoT) Needs to Become a Reality. . Technical report, Freescale.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1:2012.

Nji, J. and Li, G. (2010). A self-healing 3d woven fabric reinforced shape memory polymer composite for impact mitigation. *Smart Materials and Structures*, 19(3):035007.

Shim, B. S., Chen, W., Doty, C., Xu, C., and Kotov, N. A. (2008). Smart electronic yarns and wearable fabrics for human biomonitoring made by carbon nanotube coating with polyelectrolytes. *Nano letters*, 8(12):4151–4157.

Sprankel, S. (2013). Technical basis of digital currencies. *Retrieved from http://www.coderblog.de/wp-content/uploads/technical-basis-of-digital-currencies.pdf*.

Warren, J. (2012). Bitmessage: A peer to peer message authentication and delivery system. *Retrieved from https://bitmessage.org/bitmessage.pdf*.