

Handle System Integration as an Enabler in an Internet of Things Smart Environment

Dr. Louis Coetzee¹, Laurie Butgereit, Andrew Smith
Internet of Things Engineering Group (IoTeg)²
CSIR Meraka Institute
South Africa
20/06/2012



Handle System Integration as an Enabler in an Internet of Things Smart Environment by Louis Coetzee, Laurie Butgereit and Andrew Smith is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 2.5 South Africa License](https://creativecommons.org/licenses/by-nc-nd/2.5/za/).

1 louis.coetzee@csir.co.za; +27-12-841-3036

2 <http://ioteg.meraka.csir.co.za>

Abstract

In a future world where everything is connected to everything (the so-called Internet of Things), new possibilities of creating novel solutions are on the horizon. However, not all challenges of this completely connected world have been resolved or addressed. One such unresolved challenge is that of identity and associated information of connected things. This report presents research conducted to analyse the feasibility of using the Handle System as a mechanism to create globally unique identities with meta-information in a globally connected world. Experimental results indicate the function and utility of the Handle System in an Internet of Things world.

1 Introduction

In an Internet of Things (IoT)-envisioned future where everything is connected to everything else, the possibilities for the creation of innovative solutions linking the physical world to the digital world are endless.

One dimension where IoT is considered as a key enabler is in the creation of 'smart' environments (Vermesan & Friess, 2011). The promise of an ubiquitously connected environment, able to improve the quality and type of services provided to the citizen or occupant, has been at the forefront of research internationally (Seventh Framework Programme, 2010; "SmartSantander", 2012). IoT research is being conducted on how to create these smart environments to serve as technology test beds. Traditional IoT-related challenges of standardisation, interoperability, heterogeneity, scalability, trust, security, and appropriate architectures are being researched in these test bed environments.

In a connected world (such as a smart city) consisting of a large number of heterogeneous elements with different intrinsic capabilities, the challenge of a unique and persisted identity associated with an entity still remains unresolved. It is expected that in this ubiquitously connected world, connectivity will be ad-hoc and dynamic, varying from devices always being in the "on" state and connected, to sporadically connected and 'sleeping', thus requiring a different solution and means of identification and addressing than the traditional IP address or DNS entry. For smart cities to live up to its promise, 'Things' need to be reachable, their capabilities and location known every time, and all the time.

Utilisation of the Handle System is one possible approach to provide a unique and persisted identity to an element, act as complement to DNS and as an authentication mechanism ("Handle System", 2012). The Handle System is one component in the Corporation for National Research Initiatives' (CNRI) Digital Object Architecture (DOA) ("Research in Digital Libraries - Digital Object Architecture", 2012). The Handle System provides persistent names for Internet resources. It is created as a high performance, highly reliable distributed system. The other components in the DOA are the Digital Object Repository (which provides network-based storage and access to digital objects) and the Digital Object Registry (which provides secure registration and authentication of digital objects).

This report presents research conducted to investigate the feasibility of using the Handle System in a smart IoT environment. The research focused on registering Things in the Handle System with associated meta-information. Through this meta-information, the Thing's command-set was captured and stored from where other components in the smart environment could retrieve the command-set as and when required.

The report presents the formal objective of the research (Section 2), experimental set-up, and associated architectural approach (Section 3). Section 4 contains observations and comments regarding the approach and the suitability of using the Handle System. Section 5 concludes and presents the way forward.

2 Objective

The objective of the research conducted was to determine if and how unique, persisted identification in a smart IoT environment could be facilitated if the Handle System was used as a mechanism to persist identities and associated meta-information. To extract an

answer on the main objective, the following sub-objectives were pursued:

- Can the Handle System be used to complement DNS in an IoT environment?
- Can the Handle System be used as a repository through which meta-information associated with the Things can be retrieved by components in the IoT environment?

3 Architectural Approach

To research the stated objective, a smart environment demonstrator with relevant use-cases were created. The demonstrator utilises a combination of existing Meraka in-house IoT building blocks and newly created functionality. The existing main components of the demonstrator are:

- BeachComber: a bearer-agnostic event-driven platform able to receive and send messages via numerous channels (Butgereit & Coetzee, 2011).
- ThingMemory: an enterprise-scale application where a cyber model (and associated status) of the physical world is represented (Coetzee, 2011).

The new components created to facilitate the demonstrator are:

- Mock Smart Environment: a newly-created building block consisting of an Arduino open-hardware platform linked to a number of different sensors and actuators.
- HandleProxy: a newly-created building block acting as proxy to the Handle System.
- Runtime configurable decision engine (embedded within ThingMemory) that, based on received information from BeachComber, calculates the appropriate control actions for BeachComber to execute within the smart environment.

The following figure presents the architectural approach.

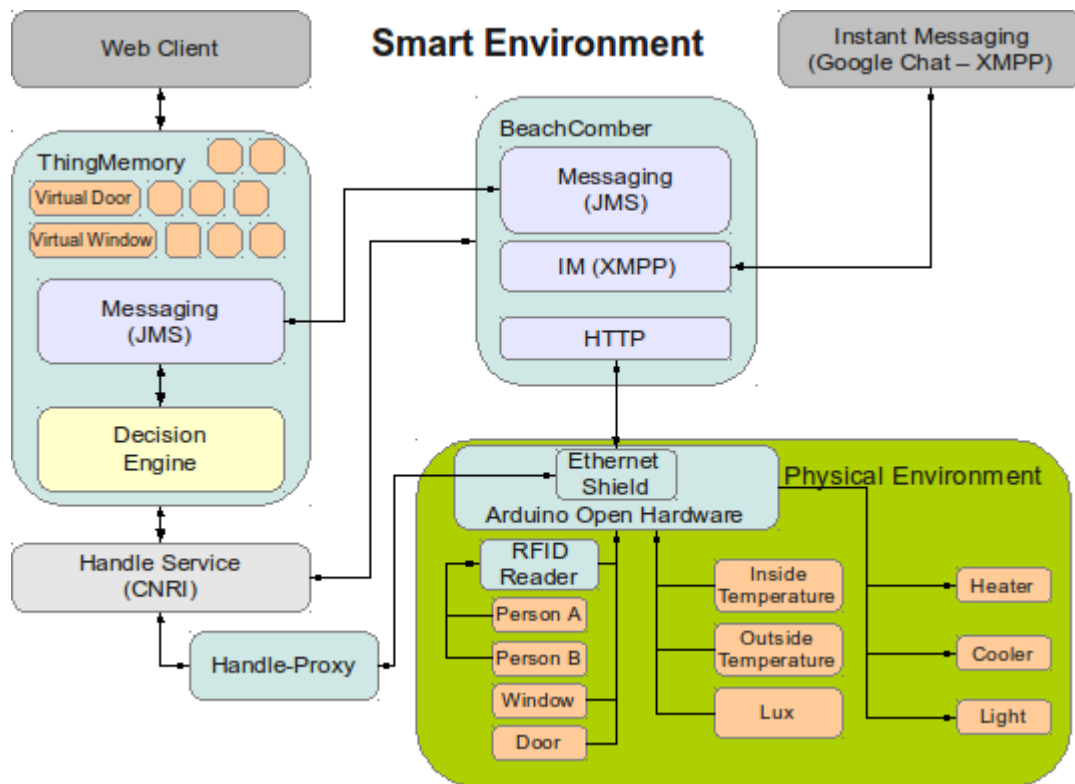


Figure 1: System Architecture

The experimental setup makes provision for two people (Person-A and Person-B) accessing a room, one person at a time. Both people have unique RFID tags. Person-A and B have different personal needs and abilities (with reference to the use-cases presented below).

The smart environment room is equipped with:

- an RFID sensor (to differentiate between the two people),
- a heater appliance (modelled by a red LED),
- a cooler appliance (modelled by a green LED),
- a table-top light appliance (modelled by a white LED),
- a light-level sensor,
- a door open/closed sensor,
- a window open/closed sensor, and
- a room thermometer.

To facilitate the experimentation a number of use-cases were implemented. They include:

1. Appliances are switched off when the door/window is open.
2. Appliances are switched off if no person is present.
3. If Person-A is present and both door and window are closed, the room temperature is driven to 22 degrees Celsius.

4. If person-B is present and both door and window are closed, the room temperature is driven to 25 degrees Celsius.
5. If lux level is low for Person-A, the light is switched on (but not for Person-B, he is visually impaired).
6. If any appliances are switched on remotely, they stay on for 30 minutes and override the current rules.

The use-cases lead to the creation of the following rules:

Rule: "Direct command light on"

Rule: "Direct command light off"

Rule: "Direct command cooler on"

Rule: "Direct command cooler off"

Rule: "Direct command heater on"

Rule: "Direct command heater off"

Rule: "Person B present, window and door closed, too cold, switch on heater, switch off cooler"

Rule: "Person B present, window and door closed, too hot, switch on cooler, switch off heater"

Rule: "Person A present, and dark inside switch light on"

Rule: "Switch off appliances when either door or window is open"

Rule: "Switch off appliances when nobody is home"

The following figures depict the mock smart environment.



Figure 2: Front view

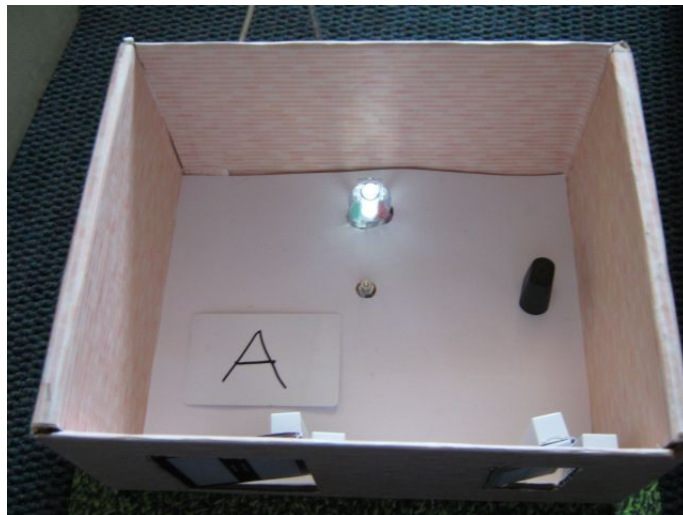


Figure 3: Inside view: Person-A present, light on

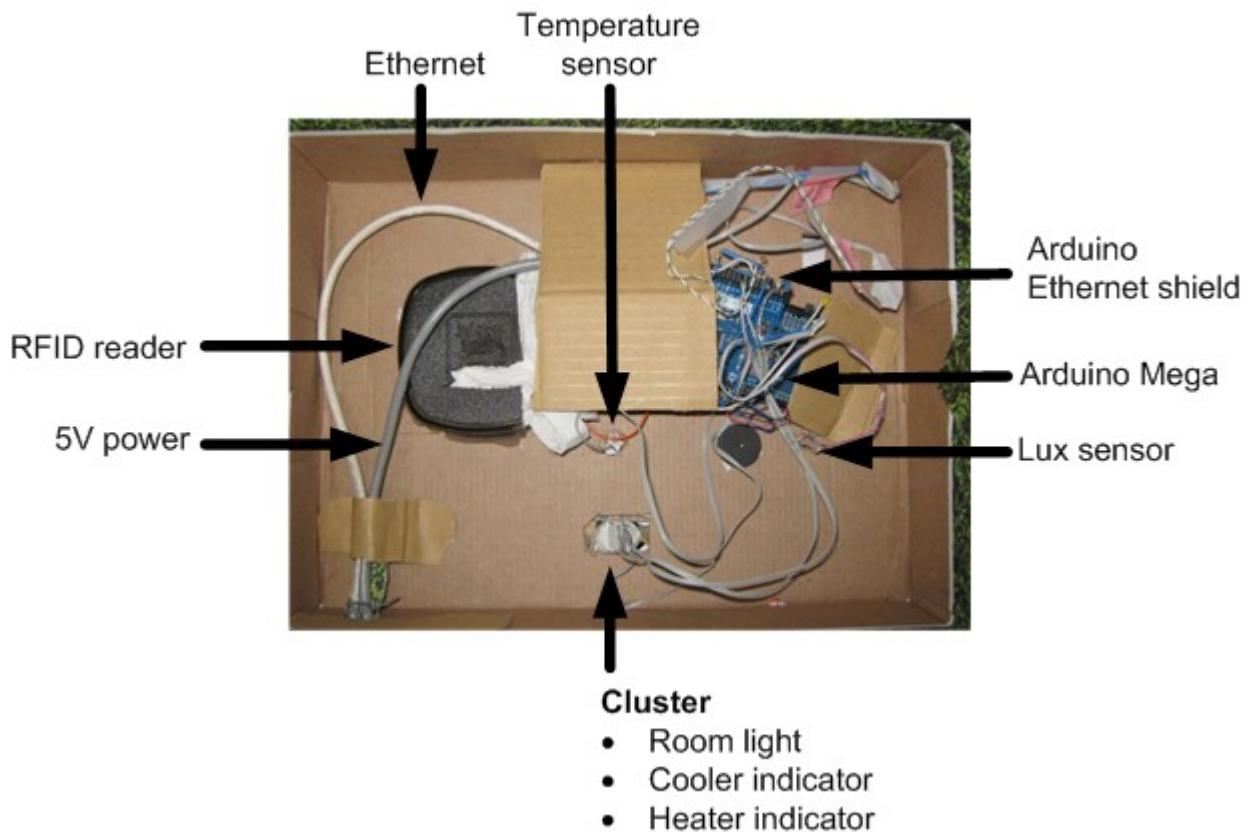


Figure 4: Annotated view of physical implementation

Interaction with the smart environment is possible through physically placing/removing RFID tags in the room whilst the door and window can be opened/closed. Similarly, the temperature and lux level in the room can be affected by heating or cooling the temperature sensor and by preventing/allowing light on the lux sensor. The smart environment can further be controlled through access from instant messaging (XMPP). Through this communication channel status of the environment can be obtained. In addition, direct user commands can be simulated (e.g. switch on the light, regardless of level of lux sensor, thus overriding the decision engine).

The stated objective could be researched through the creation of the IoT enabled smart environment. This environment incorporates the Handle System which complements DNS and functions as a meta-information repository. The following comments can be made:

- The use-cases associated with the smart environment could be executed effectively indicating the success of the approach and subsequently the success of the Handle System in such an environment.
- Based on the results obtained, it is clear that the Handle System can provide effective, unique and persisted identification of Things with their associated useful meta-information.
- Through the experimentation it is clear that the Handle System is an effective and low cost complement for DNS. It is able to function at a global scale.
- In addition, through the meta-information stored in the handle, it is clear that the Handle System is an effective repository for information which can enhance the communication and interoperability between Things and associated back-end

services.

4 Comments and Observations

The following broad comments and observations can be made:

- Creating unique and persisted identities for Things through the Handle System eases the addressability of those Things.
- Storing meta-information in the handle reduces the complexity of architectural solutions. All elements are configured with updated information from a central, one-place-holds-all repository at boot-time.
- Retrieving data stored on the Handle System from devices with limited resources (low-end devices) remains a challenge. The architectural solution required to solve this involved the creation of a Handle System proxy. Using the proxy, handle information can now be retrieved directly via an HTTP 'GET' request. The information returned from the 'GET' request contains only the specific Thing command and does not require further parsing and extraction on the low-end device.
- The meta-information stored in a handle should be improved. This can be done by following REST principles in order to allow for better description of the command-set associated with a Thing. The approach implemented contains URLs at various index positions in the handle. The first index contains the URL to the digital representation of the Thing in ThingMemory. The second and third index positions contain the command to be executed based on the occurrence of a specific event (e.g. a door closing-event being communicated to BeachComber). This proved to be clumsy and difficult to parse and executed in the various building blocks. The following is an example entry of this implementation:
 - Index position 1:
URL= <http://things.meraka.csir.co.za/memory/thingView.seam?thingId=278>
 - Index position 2:
URL= http://146.64.28.16/beachcomberservlet/issac?door_event=closing
 - Index position 3:
URL= http://146.64.28.16/beachcomberservlet/issac?door_event=opening
- It is envisioned that the Handle System can also contain authentication information (e.g. public and private certificates) with which a trusted system can be created. In such a trusted system, devices and commands are authenticated with required authorisation.
- Currently, changes in status of the various elements (such as the temperature sensor) are communicated via the identified command-set. It will be an interesting expansion of the handle functionality if these status information sets can be stored by the device in its own handle (thus acting as a repository for run-time information, in addition to the meta-information).
- In this experimental configuration, digital objects were stored in ThingMemory. Future research can explore the utility of using the other DOA components (registry and repository) as a mechanism to store digital objects.

5 Conclusion and Way Forward

The use of the Handle System reduces complexity in terms of the overall smart environment IoT architecture. It ensures that common information used by various components are stored centrally. Thus, when changes are required, only one component needs to be updated.

The scheme discussed here stores a Thing's command-set in the Thing's own handle. This scheme allows for actions (e.g. the capability and status) to be communicated. Even though the scheme is unsophisticated, it proved to be valuable. This scheme can still be revisited and refined further.

It is clear that using handles for Things add value. It is recommended that this concept be further explored and researched. The experimental smart environment embodies a limited number of Things. Research relating to a massively scaled environment needs to be conducted.

The experimental smart environment does not implement any form of trust and security. This is an important aspect to research and implement. The use of the handle to also host Private Key Infrastructure (PKI)-elements in order to provide authentication and authorisation is a worthwhile future research topic.

Through the creation of an experimental smart IoT environment the use of handles hosted in the Handle System was researched. From the results obtained, there are clear motivation and support for formally expanding the research of applying handles in IoT.

6 Acknowledgement

The IoTEG research team gratefully acknowledges the role Sorene Assefa (Technology Analyst, SG office/Corporate Strategy Division, ITU) played in facilitating the interaction with Corporation for National Research Initiatives (CNRI) as well as facilitating access to the CNRI researchers.

The IoTEG research team thanks Dr. Larry Lannom, the Director of Information Management Technology, and Vice-president of CNRI. He has provided valuable information and insight and played a significant role in establishing communication channels to other CNRI researchers.

References

- Butgereit, L., & Coetzee, L. (2011). Beachcomber: Linking the “Internet of Things” to the “Internet of People.” In P. Cunningham & M. Cunningham (Eds.), *IST-Africa 2011 Conference Proceedings*. Gaborone, Botswana.
- Coetzee, L. (2011). ThingMemory. Retrieved April 6, 2011, from <http://ioteg.meraka.csir.co.za/ioteg/contentView.seam?contentId=64>
- Handle System. (2012). Retrieved May 15, 2012, from <http://www.handle.net/>
- Research in Digital Libraries - Digital Object Architecture. (2012). Retrieved May 15, 2012, from <http://www.cnri.reston.va.us/doa.html>
- Seventh Framework Programme. (2010). European Research Cluster on the Internet of Things. Retrieved November 29, 2010, from <http://www.internet-of-things-research.eu/>
- SmartSantander. (2012). Retrieved July 20, 2011, from <http://www.smartsantander.eu/>
- Vermesan, O., & Friess, P. (Eds.). (2011). *Internet of Things: Global Technological and Societal Trends*. Aalborg, Denmark: River Publishers.

Appendix A: Handles and associated meta-information

Handle Meta-information scheme:

Index 1: URL to digital representation in ThingMemory

Index 2: URL for Command to be executed

Index 3: URL for Command to be executed

10913/SE_COOLER :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=284>

<http://se-room1-controller.meraka.csir.co.za/?cooler=on>

<http://se-room1-controller.meraka.csir.co.za/?cooler=off>

10913/SE_DOOR :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=278>

http://146.64.28.16/beachcomberservlet/issac?door_event=closing

http://146.64.28.16/beachcomberservlet/issac?door_event=opening

10913/SE_HEATER :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=282>

<http://se-room1-controller.meraka.csir.co.za/?heater=on>

<http://se-room1-controller.meraka.csir.co.za/?heater=off>

10913/SE_LIGHT :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=286>

<http://se-room1-controller.meraka.csir.co.za/?light=on>

<http://se-room1-controller.meraka.csir.co.za/?light=off>

10913/SE_LUX_METER :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=292>

http://146.64.28.16/beachcomberservlet/issac?room_lux_event_d=

http://146.64.28.16/beachcomberservlet/issac?room_lux_event_i=

10913/SE_OUTSIDE_THERMOMETER :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=290>

http://146.64.28.16/beachcomberservlet/issac?outside_temperature_event_d=

http://146.64.28.16/beachcomberservlet/issac?outside_temperature_event_i=

10913/SE_PERSON_A :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=294>

http://146.64.28.16/beachcomberservlet/issac?person_present_event=SE_person_A

http://146.64.28.16/beachcomberservlet/issac?person_not_present_event=SE_person_A

10913/SE_PERSON_B :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=296>

http://146.64.28.16/beachcomberservlet/issac?person_present_event=SE_person_B

http://146.64.28.16/beachcomberservlet/issac?person_not_present_event=SE_person_B

10913/SE_ROOM_THERMOMETER :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=288>

http://146.64.28.16/beachcomberservlet/issac?room_temperature_event_d=

http://146.64.28.16/beachcomberservlet/issac?room_temperature_event_i=

10913/SE_WINDOW :

<http://things.meraka.csir.co.za/memory/thingView.seam?thingId=280>

http://146.64.28.16/beachcomberservlet/issac?window_event=closing

http://146.64.28.16/beachcomberservlet/issac?window_event=opening