

FIA session S.II.3 – Internet of Things and the Future Internet

Organizers

Rapporteurs/Organisers: Jim Clarke, Waterford Institute of Technology; Alessandro Bassi, IOT-A.; Rodrigo Roman, University of Malaga; Trevor Peirce, AVANTA Global SPRL; Antonio J. Jara, University of Murcia; Antonio F. G. Skarmeta, University of Murcia; Francois Carrez, University of Surrey.

Other contributors: Stephan Haller, SAP, Dieter Uckelmann, LogDynamics Lab at the University of Bremen c/o BIBA; Oscar Garcia-Morchon, Philips Research Europe, Distributed Sensor Systems; Amardeo Sarma, NEC; Michel Riguidel, Telecom Paris-Tech; Sebastian Lange, VDI/VDE-IT; Ian Smith AIM UK; Laure.Quintin, VDI/VDE-IT; Nick Wainwright, HP Labs and Nick Papanikolaou, HP Labs.

1st Panel – IoT/FI architecture & integration panel

- Alessandro Bassi, IOT-A

The overall chair of the session, Mr. Alessandro Bassi of IOT-A, presented the main goals of the session: to highlight various aspects of IoT architecture and how it should map to the Future Internet in the first panel and then to delve deeper into analyzing the security, privacy and trust challenges for the integration of the IoT in the FI in the second panel followed by integration discussions. Mr. Bassi began presenting the first panel, introducing the challenges that we face in the Internet of Things (IoT) field. Mr. Bassi also encouraged the audience to join the Future Internet Assembly and help to solve these cross domain challenges.

- Stephan Haller, SAP

This talk began discussing the nature of the *things* in the IoT. Mr. Haller mentioned how *things* are not the computational devices, but the physical entities (e.g. human beings, cars, trees). Devices enable the physical entities to belong to / interact with the IoT. Still, there are challenges to consider such as connectivity, services enablement and interoperability.

Mr. Haller presented the Fundamental IoT architectural issues:

- connectivity
- service-enablement
- mobility
- heterogeneity
- deployability
- manageability
- scalability

On the subject of *connectivity*, we already have a protocol that provides IP connectivity in constrained environments (e.g., WSN) 6LowPAN. Still, there are some specific requirements (e.g. real-time processing/access constraints) that are not easy to meet. Mr. Haller introduced the need for gateways in some scenarios, but also mentioned that the IP protocol for Smart Objects (IPSO¹) proposes that the IoT should not depend on gateways. This was the predominant view at the IETF Interconnecting Smart Objects with the Internet Workshop² in Prague in March 2011 where it was suggested that we should ‘think twice’ before using gateways – first determine categorically the reasons why needed, otherwise, there will be end-end issues to deal with. Therefore the key message: where it is possible, a balance must be found here.

¹ Also sometimes referred to as IP protocol for Small Objects

² <http://www.iot-i.eu/public/events/interconnecting-smart-objects-with-the-internet-workshop>

Regarding *service enablements*, Mr. Haller points out that IoT services are different from enterprise services. Within the real-world where IoT services would be predominant, these would be comprised of any kinds of services interacting with the real world. The service layers exist to support interoperability – e.g. abstracting from underlying hardware and protocols. But this is fundamentally different from enterprise services – with different granularity and there are special factors that need to be considered, such as location, streaming data, geo-location, approximate values (eg. temperature) and QoS. Besides, Mr. Haller pointed out that while initial push on technical protocols for IoT was for SOAP –based protocols, there is a shift towards the use of REST, EXi and the SAP data protocols. There is satisfactory technical interoperability between the IPv6 (corresponding to OSI layer 3 – network) and REST (corresponding to OSI layers 6&7) protocols, but there is still the issue of semantic interoperability, namely, how the data presented at the level of REST is interpreted by different types of device. The applicability of REST for connecting IoT resources is backed up by the existence of future standards such as CoAP.

Finally, Mr. Haller brought up the *interoperability* challenge. In fact, there are two major interoperability challenges that need to be solved: technical interoperability (for devices to connect via networks) and semantic interoperability, which is not addressed by the technical interoperability. The semantic interoperability seems especially challenging, as we need to deal with a huge amount of linked data in the IoT. There is good work in FIA already on Linked Data that could be a viable solution. However, we need to determine who is going to provide all of the annotation? What about finding resources, discovery. It raises the question do we need basic infrastructure services then for the IoT?

In conclusion, Mr. Haller re-iterated that while IPv6 is useful for IoT, it will still need to be used in conjunction with gateways; interoperability at the level of REST is satisfactory, but still more work is needed and significant work is especially needed at the semantic level, to achieve semantic interoperability in the Future Internet

- Dieter Uckelmann, LogDynamics Lab at the University of Bremen c/o BIBA.

Mr. Uckelmann's talk began discussing different aspects of the IoT that can be summarized using the following words: *envision* (how the IoT can be defined), *extend* (make use of what we have), *enable* (find solutions in order to bring the IoT to the real world), *excite* (bring users to the IoT) and *evaluate* (how to generate IoT business models).

Mr. Uckelmann presented a new definition of the Internet of Things from the new Springer publication "Architecting the Internet of Things". After that definition, he introduced the elements of the structure that should exist in order to fulfil such vision, with elements like business innovation, new services, a front end and back end architecture, administration of edge devices, resource management, and other elements.

After that, the description of an architecture for the IoT was introduced. This architecture considers the existence of a billing interface at its very core. This way, it can be possible to enable the creation of new business models thanks to direct revenue streams.

Mr. Uckelmann also mentioned the design of the edge component of this architecture, highlighting the issues associated to obtaining information from different devices (e.g. RFID, sensor networks, actuators, non-IP devices). Finally, it was mentioned that part of this architecture actually exists as a prototype, which focuses on billing information queries.

Mr. Uckelmann described an effort to build a business model on top of the IoT architecture, in particular a demonstrator of a *billing system for FI services*. The idea was to show how one could account for IoT usage and charge users and businesses accordingly. What is interesting is that there are different measures and aggregation of IoT 'usage' that can be considered in a business model.

- Questions & Answers

Question: “In the definition of the IoT: does the requirement that you want to be able to uniquely identify things something that is really needed because if you look at sensor networks often it may not make sense to address individual sensors. For example, for temperature – you don’t need to identify individual sensors but groups of sensors instead?”

Answer: You may not need to identify the individual sensors, but from a management perspective you may need to do so. We need to make a link to unique objects – only so that you can know what the data refers to (e.g. temp). The ‘thing’ is the item that is being monitored.

Question: “The definition is very restrictive in that it says that the *things* are available to everybody, and secondly assumes there will be one business model. For example, if we consider the ‘accessed by anybody’ (open Internet of Things vs. constrained Extranet of Things) part, we might limit the IoT to one single business model. Other companies might need something different”.

Answer: A common definition should exist to differentiate the IoT from other fields of research. There is a need to have a common definition and there are discussions about Intra-net of things and Extra-net of things. But the Internet should be more open – there’s a bigger concept behind it. Somehow it has to pay, and the only thing you can charge for is the data.

Question: “The business model does not convince me. We are not used to this kind of ‘pay for one off pieces of data’ by the item in the Internet. (e.g. pay per article). The Internet of things should provide means for application developers to get revenue, not necessarily just for the data from the thing, which might be a disincentive for the development of applications by developers.

Answer: We need a certain incentive for increasing the deployment of IoT technologies and development of new applications. Besides, the business model is based on the following question: ‘Are we willing to pay for information provided by the IoT?’ In fact, in the real world, we do pay, for example, through downloading apps, paying for the IT department by the slice, product sales and the selling of data.

Question: “You propose an architecture of the various Internet of Things. In proposing an architecture, it’s important that the architecture provides access to any objects in an interoperable way. Do you think that all systems should be built this way, so that they can all interoperate?”

Answer: to a certain extent (e.g. at the discovery service level) we should follow the same approach. Of course, we will have heterogeneity, but we need some common standards enabling interlinking of the different approaches such as common discovery services, semantic approaches, using information from different sources.

Question: There was mention in the presentation about the use of linked data, and whether the source of such data could be deemed trustworthy and reliable. “What do you mean with the problem of ‘who provides the data?’”.

Answer: It is a challenge about data provenance and we need to know if the source of the data can be trusted.

Question: You argued for a layer of sensors and a layer of applications including billing – the world is indeed a complex place. There will be sensors everywhere and a multitude of sources of IoT transactions (multiple initiators, etc.) and the notion of sensors we can always access is very good. But: do we really require customer billing for this or make this a main driver as discussed in the presentation on business models? At least, we should consider

the existence of an accounting and management component, which might be just everything we need instead of individual billing systems that could frighten off users who aren't accustomed to this type system". It raises questions: Whom are you billing? What about charging ISPs?"

Answer: It is true that accounting and management is important. However, existing accounting solutions may not be able to deal with the huge amount of possible 'billable' interactions in an Internet of Things. The ensuing discussion showed that this is still a contentious point, which requires further research.

2nd Panel – privacy, security & trust

- Trevor Peirce, IERC

After introducing the speakers, the panel moderator, Trevor Peirce, AVANTA Global SPRL presented '4' days of recent media and policy events influencing public trust in ICT, the IERC cluster, IERC identified principle IoT technologies, and introduced the current European policies and approaches to IoT. Furthermore, Mr. Peirce showed the results of a questionnaire made by the IERC cluster, where the main question was "What are the technologies of the Internet of Things?" The most voted were sensor networks, RFID, M2M, virtual worlds, and the Internet. Later, Mr. Peirce asserted that security and trust is critical for the success of the IoT: For this purpose, we need to study aspects such as control, ownership, capacity, privacy, and security.

- Oscar Garcia-Morchon, Philips Research Europe, Distributed Sensor Systems

Mr. Garcia-Morchon began his talk by explaining possible use cases and technologies for the IoTs and gave some examples showing that the IoT is already here amongst us – at least a first version of it. Later, he introduced the concept of the 'lifecycle' for objects in the IoT, and explained that there are security challenges to consider in each of the stages of the life of a "thing".

Mr. Garcia pointed out that for security goals of IoT to be met, the following elements are needed:

- a set of secure applications
- a set of guidelines and standards (e.g. for good practice)
- a security architecture

The above triad constitutes the basis of secure IoT. In this context, it is key to answer the following questions:

- 'What we exactly need?' (related to the application needs [on security](#));
- 'What we should/shall/may use?' (related to [security](#) standards);
- 'How everything works together?' (related to the overall security architecture).

In the context of the security architecture, Mr. Garcia-Morchon pointed out that there are many security issues that must be considered: application security, [security](#) bootstrapping, network security, and the 'thing's' security model. Mr. Garcia-Morchon explained how [some](#) of these issues are being explored in the IETF draft "Security Considerations in the IP-based Internet of Things"³, of which Mr. Garcia-Morchon is co-author. Of the open problems identified by Mr. Garcia-Morchon, there was an emphasis on the issues of end-to-end security, secure multicast and (cryptographic) key management. The last one is central to the success of a secure IoT, since the multitude of devices will require a multitude of keys to be issued, managed, and revoked.

³ <http://tools.ietf.org/html/draft-garcia-core-security-01>.

- Antonio Skarmeta, Univ. of Murcia

The main focus of Mr. Skarmeta's talk was on the security requirements of the IoT and the necessary steps to provide a secure, trusted and private IoT. While introducing his talk, Mr. Skarmeta pointed out that human beings are one important element of the IoT due to the novel way a human can interact with its environment. This particular fact might influence on how security is achieved in certain IoT interactions.

Mr. Skarmeta expressed the need to have *things* as an element in the Future Internet, so should go further from the scenario to the idea that we should take care that new ways of interaction are happening because people will use these objects to provide information to a third party. i.e. a 'thing' will be integrated into the personal 'space' of a user to provide information to third party. Therefore, we need to extend this concept of identity (rights, access, delegation) to the *things* so that this can be extended to the 'thing' itself.

Mr. Skarmeta presented a list of *challenges* that must be tackled in order to protect the IoT, such as security, privacy, trust, architecture, lifecycle, integration, and mobility. He also introduced some of the *requirements* that must be taken into account when developing security solutions, such as: interoperability, applicability, and optimality (against constraints). Moreover, he also showed the blueprint of a security architecture, whose purpose was to locate components from the point of view of security. It is clear that more devices will be connected with which we can interact. Trust needs to be considered here, and this has a certain 'dynamicity' as these networks are created dynamically and will need to relate *things* to *things* also on the fly. Mr. Skarmeta claims that this raises a fundamental question on bootstrapping for security in IoT – how does this scale to IoT? In other words, how do we issue the many cryptographic keys that are required to make the IoT work.

Finally, Mr. Skarmeta explained some of the key points that were discussed on security, privacy and trust at the recent IETF Interconnecting Smart Objects with the Internet Workshop⁴ in Prague in March 2011. In summary, the areas of most importance from the security and trust considerations for IoT/FI architecture research are:

- handling of time/delays/lags in the network
- applicability (of IoT to different problems/scenarios?)
- interoperability
- integration
- and bootstrapping.

The speaker clearly explained that, since we are still at the beginning of IoT research, there are many basic questions to be resolved; no more fundamental is the answer to the question: "what do we mean by the term *things* in IoT?"

3rd Panel – Closing panel

In this particular panel, as explained by Mr. Jim Clarke, Waterford Institute of Technology, the task of the closing panellists was to summarize the contents of the previous panels from their perspective and to ask questions to the previous speakers and the audience.

Amardeo Sarma, NEC. As we are in the phase of developing concepts and ideas for the IoT, the presentations raised quite a lot of views on the nature of things raising the question: "What are the *things* in the Internet of Things?". In the talks, we have heard *things* referred to as many possibilities from the IERC survey (sensor networks, RFID, M2M, etc.), real world objects (even trees and cows!) and identifiable end points. There are other issues related to the hierarchical nature of *things*, how to record access (and who can have access to such records), and how information created by different things could interact. This raises a

⁴ <http://www.iot-i.eu/public/events/interconnecting-smart-objects-with-the-internet-workshop>

need to identify things to different levels for example in the room that we are in and then the loudspeaker in the room. Based on this, a number of questions were put to the panellists:

1. Where we have identifiable *things*, e.g. hotel, then *things* within *things*, like the room, loudspeaker, do we need a recursive composition of *thing* and should it be part of the architecture?
2. From the discussions on billing and the nature of how people use and pay for *things* nowadays almost for free, shouldn't we urgently address the business models from the very start?
3. regarding naming and addressing for IoT, this raises issues such as how to get bootstrapping, deployment and discovery?

Responses from the panelists:

Yes, for the IoT, it is definitely necessary to have recursions - eg. pallets with objects on them, that's recursive - and this has already been accomplished to a certain degree. There needs to be hierarchal identifiers with descriptions that are more complex (rather than single hierarchy) when dealing with devices in IoT. A mechanism is needed to define the scope of recursion to allow different layers of aggregation for the IoT and FI with multiple models to fit the hierarchy of devices. It was pointed out that we need to make sure not to mix the address and identifiers. There is room for intelligent clustering – an example of a truck carrying special loads was given.

Regarding the previous point on the definition of IoT, the speakers all agreed it is the usual situation where the definition is a hard one to find and there is a tendency to over dwell on this issue - but this should be less important with the primary focus being on the IoT Architecture (IoT-A) instead and defining the concepts within and below that. IoT-A results should be a step forward in this regard.

Rodrigo Roman, University of Malaga pointed out the importance of security and trust for the IoT to be successful and it necessitates a holistic point of view from the cradle to the grave and to see the different instances of the Internet of Things that are different. Mr. Roman introduced the idea of fault tolerance in the IoT ("If hackers control part of the actual Internet, what will happen when the IoT arrives?"), and questioned the panellists about the creation of the security mechanisms ("do we need to integrate, adapt, or create security mechanisms in the IoT?").

Response from the panellists:

All previous speakers agreed that all three approaches are necessary and this was also discussed at the IETF workshop⁵ in Prague. However, the risks associated with 'adapting' were pointed out that could cause unexpected knock on effects elsewhere. A solution proposed would be to leave the interfaces open. The notion of **trust** in IoT is currently not clear and is a major challenge for the community. The observation was made that *things* have a lifetime, and they evolve over time (they are not static!) and there is a definitely a need for **fault tolerance** in IoT, and that it will be resilient to attacks.

Finally, **Michel Riguidel, Telecom Paris-Tech** brought some welcomed controversy to the session by declaring that the existence of a one single providential Internet of Things with billions of elements raises some major issues for him on trust, security and especially governability. In essence, Prof. Riguidel doesn't agree with the concept that the IoT should be centrally governed/managed/administered since there are fundamental issues of personal freedom, online 'liberties' that we need to ensure are maintained, and he feels this cannot be accomplished by having a centralised IoT/FI governance model. Today, it is a closed world of hosts of billions of computers and the idea of having trillions of virtual, physical, static,

⁵ <http://www.iot-i.eu/public/events/interconnecting-smart-objects-with-the-internet-workshop>

nomadic objects raises thorny questions for Prof. Riguidel such as: Who will govern this? Where is the directory of this world? Who is going to manage the secrets?

Professor Riguidel raised the following questions:

- This leads to a double edged sword – do you want an Internet of Things that is connected all the time to everyone or one where things are only connected from time to time?
- What about personal freedoms? – especially not leading to a situation that is centrally controlled, monitored, watched?
- the tracking services of parcel providers are not questioned today, although they could have potential security and privacy implications for individuals. Will people keep these attitudes or become more conscious of their privacy in future?
- will devices really be uniquely identifiable? Prof. Riguidel asserts that maybe this is not realistic.
- there is a need to be more precise when talking about the IoT terminology. For example, what do we mean when we speak of IPv6 in FI? Do we refer to the *format* or the *protocol*? Prof. Riguidel argues that discussions in the IoT/FI community so far seem to be more about *format* than *protocol*, which can lead to a dangerous situation. This is a subtle point that deserves more attention especially at the edge of networks.

Response from the panellists:

The panellists agreed that the IoT will generate new problems (which must be discovered and analyzed), and the benefits must outweigh those problems. We must clearly differentiate between the Internet of People and Internet of Things and there is also a differential between dumb things and intelligent things that must be made. Yes, today we are on one Internet and there are billions of devices and from the outside it looks like one Internet of Things, but on the inside there needs to be differentiated, federated sets of services and devices.

Regarding governance, all panellists also agreed that it is an important problem that must be tackled following the conceptual and definitions phases to ensure security and trust in the IoT. In fact, in the current Internet, this is only partially solved.

Announcement of the IOT International Forum

Francois Carrez, University of Surrey presented the IoT international Forum, a place to debate, organize ideas, provide a global platform, and share common visions on the evolution of the IoT. The first meeting of this forum will be held on 22-23rd November 2011 in Berlin, Germany. Information for the forum will soon be available on <http://www.iot-i.eu/>.

Other relevant events:

6th June 2011: IoT week <http://iot-week.eu>.

17th October 2011: IoTech - IEEE Workshop on Internet of Things Technology and Architectures <http://iotech-ws.com/>

19th October 2011: SecIoT 2011 - 2nd Workshop on the Security of the Internet of Things <http://www.isac.uma.es/seciot11/>