Trust & Security RTD in the Internet of Things – Opportunities for International cooperation

James Clarke
Waterford Institute of Technology
TSSG Group
Carriganore, Co. Waterford, IRELAND
+353 719166628
jclarke@tssg.org

Abhishek Sharma
Beyond Evolution TechSolutions Pvt. Ltd.,
Gurgaon, New Delhi, INDIA
+91 98-10-412700
abhishek.sharma@beyondevolution.in

Neeraj Suri
Technische Universitaet Darmstadt
Karolinenplatz 5
Darmstadt, 64289, GERMANY
+49 160 90659435
suri@cs.tu-darmstadt.de

Rodrigo Roman Castro
Institute for Infocomm Research
1 Fusionopolis Way
#21-01 Connexis (South Tower)
Singapore 138632
+65 6408 2000
rroman@i2r.a-star.edu.sg

Javier Lopez
University of Malaga, NICS
Network, Information &Computer Security Lab
Malaga, SPAIN
+34 952 134185
jlm@lcc.uma.es

ABSTRACT

While there has been considerable progress in the research and technological development (RTD) of the Internet of Things (IoT), there is still considerable RTD required by international communities for the trust, privacy and security research challenges arising from the constitution of the IoT architectures, infrastructures, communications, devices, objects, applications and services. In this paper, we present an thorough analysis of the ongoing and future RTD work, specifically in Europe, regarding trust, privacy and security of the Internet of Things with a view towards enabling international cooperation efforts around the globe to solve these major research challenges.

Keywords

Trust, Privacy, Security, Internet of Things, International Cooperation (INCO), Research and Technological Development (RTD).

1. INTRODUCTION

There has been considerable research work undertaken in Europe on the Internet of Things and roadmapping activities looking at the future research needs for the concept known as the "Internet of Things". There are a number of widely used definitions for Internet of Things, including the following:

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts. Interconnected objects having an active role in what might be called the Future Internet." source: *Internet of Things in 2020 - Roadmap for the Future. May 2008 [1]*

"Objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment and/or use actuators to interact with it". source: *Internet of Things – An action plan for Europe. June 2009 [2]*

"A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols - Physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network." source: *Internet of Things – Strategic Research Roadmap. September 2009 [3]*

All IoT definitions revolve around the same central concept: "a world-wide network of interconnected objects" with the following attributes: existence, sense of 'self', connectivity, interactivity, dynamicity, and sense of environmental awareness.

A large number of research challenges have already been identified across the various domains when analyzing the road mapping for Internet of Things – Research Needs for the period 2015-2020. These include:

- ID Technology: Support various existing and future identifier schemes
- IoT Architecture: From the Intranet of Things to the IoT
- SOA: Composable process-oriented IoT services
- Comm. Technology: Self-configured, protocol seamless networks
- Network Technology: Internet of Everything
- SW and Algorithms: Evolving, Reusable, Autonomous, Aware SW
- HW: Smart sensors, nanotechnology, "insect-like" systems
- Data / Signal processing: Context aware data processing
- Search Engine: Cognitive/Autonomous search engines
- Power: Energy Harvesting, biodegradable batteries
- Standardization: Cross-Interoperability, Dynamic/Evolutionary
- Security: Universal Authentication, Standards, Context/Service aware, mobile security, trust, privacy, and many others

The SecurIT 2012 paper will specifically concentrate on the final bullet above and outline future research areas specifically in trust, privacy and security of the Internet of Things (IoT). The paper will also highlight the European Commission's Framework Programme 7 BIC project, which stands for **B**uilding **I**nternational **C**ooperation in Trustworthy ICT [4]; and the strategy and structure for BIC, which is perfectly positioned to enable future collaborations between the programme management (funding

agencies) and researchers from both academic and industry in a strategic and long term fashion.

2. RESEARCH CHALLENGES

The research challenges presented here have been primarily inspired on a number of events looking specifically at the security research challenges associated to the IoT. There were a workshop organized by the European Commission Trust and Security unit in September 2009 entitled Network and Information security: research ideas workshop [5] and two sessions during the bi-annual European Future Internet Assembly held in FIA Budapest (May 2010) [6] and FIA Aalborg (May 2012) [7]. In addition, as shown in figure 1, two documents were used to inspire this work, including Internet of Things: Strategic Research Roadmap" (published by IERC in 2011) [8] and "Towards a Trustworthy Information Society" (published by coordination action Think-Trust in 2010)) [9].

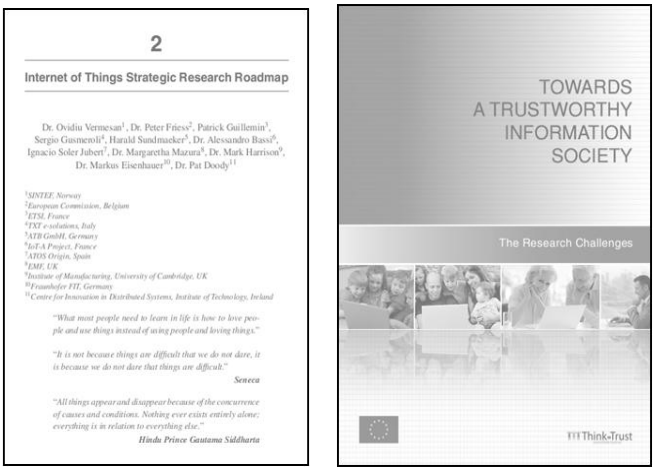

Figure 1. Documents used to carry out the analysis

As shown in Figure 2, there are a number of top level security research challenges. In summary, the challenges are the following:

Protocol and network security to deal with the large number of objects with significant heterogeneity. This would involve improved cryptography to make them operate in smaller environments requiring faster operation while keeping same levels of security so far. A Key management infrastructure is needed for the open configuration of IoT, in which the new systems need to be able to manage the keys in objects of small size where the current certificate based systems wouldn't work. The current Internet protocols are not usable in these environments.

Data and Privacy as carrying multitudes of objects can bring up a lot of privacy issues as they are not operating in an isolated way. This area can be addressed by using Privacy by Design (user should be able to decide which of his/her information and how it is being used); Privacy by Default (right to be forgotten); transparency (he should know when it is being used), and improved data and information management.

Identity management, which must be taken from a different perspective in IoT in which objects will have a core identity and yet a temporary identity must be possible. ID management systems should encompass Identification (how to define the identity of a "Thing"); Authentication (infrastructure that allows mutual authentication based on Centralized, Distributed, Local, Global, Attributes); and Authorization based on delegation (e.g. stethoscope) and granularity (e.g. classroom provides class schedule to everyone, syllabus only provided to students).

Trust and governance is required in order to obtain trust between the different objects (and from the user perspective). For the IoT, a trust management system is especially required inside in order to gain trust management from the user perspective. From the system perspective, governance is very important where policies should be contained and where the policies vs. control is dealt with;

Fault tolerance as the perimeters of the networks do not exist any more in IoT. Therefore, attackers will be all around and there is a need to provide solutions with the following attributes - Secure by default (Patch Tuesday?), Internal State and the ability to provide self - defence recovery.

Also shown in figure 2 are two special "foundational challenges", including those related that are **Properties / Application-specific**. These are basic properties that all challenges must consider (e.g. Interoperability, Scalability, Resilience) and to the high-level, application-specific security mechanisms that make use of all the challenges above (e.g. Secure discovery of services); and **Architecture.** Within a system, it is necessary to provide some architectural support to integrate the different security services.

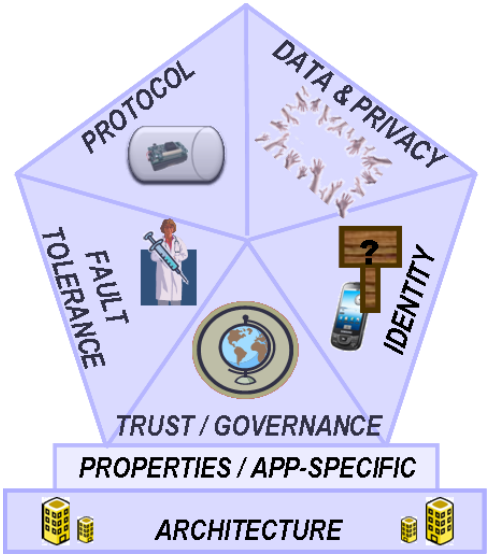

Figure 2. Security research challenges in IoT

Figure 3 depicts the current state of the art with respect to IoT trust, privacy and security highlighting where the challenges are actively being considered by the research communities already, based on findings in various research papers and the aforementioned documents.

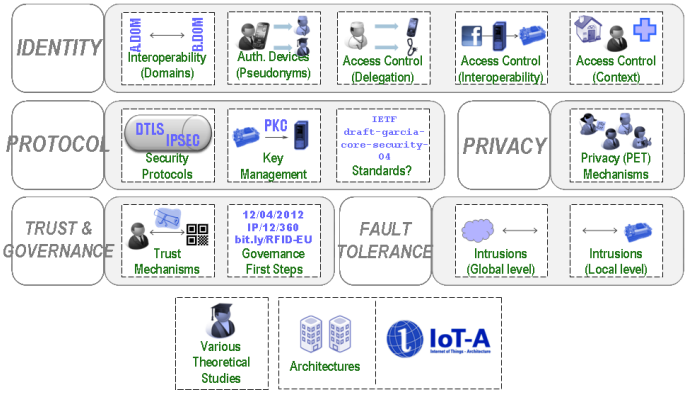

Figure 3. State of the Art research studies

Within figure 4, the challenges are configured into a timeline as introduced by Internet of Things: Strategic Research Roadmap [8]. As seen in the figure underneath the timeline, there are a number of research items (e.g. trust management, access control (delegation) and governance) that don't easily fit yet into the timeline and the research community needs to urgently work together closely to determine when and how these challenges should be addressed for IoT.

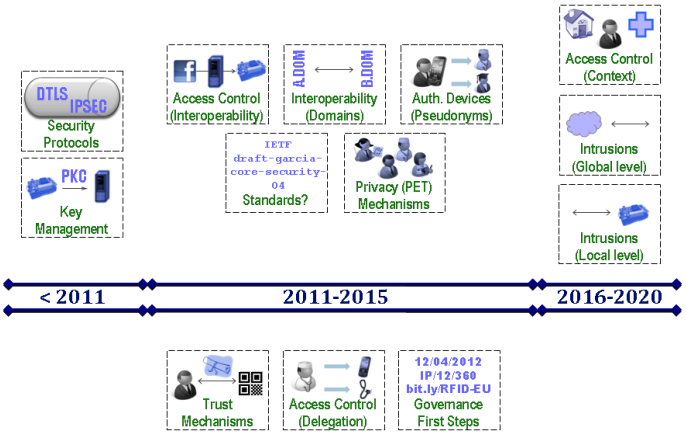

Figure 4. Research challenges in a timeline

Although a considerable amount of research has already been undertaken for IoT, there needs to be considerable more research carried out in particular with respect to trust, privacy and security elements. It should be noted that while the data here is as accurate as the authors could conclude from their research and interactions in the aforementioned events and documents, there could be existing studies already being carried out on these items not included here (e.g. in an European project, where public deliverables are sometimes limited), or there may be additional challenges not considered in detail within our analysis. Therefore, the paper and presentation are being used to draw feedbacks from the research communities on these topics in which readers and listeners could certainly clarify something and to share their knowledge with the authors and other attendees.

Figure 5 depicts research areas where we are lagging behind in the timeline formation. These include the following:

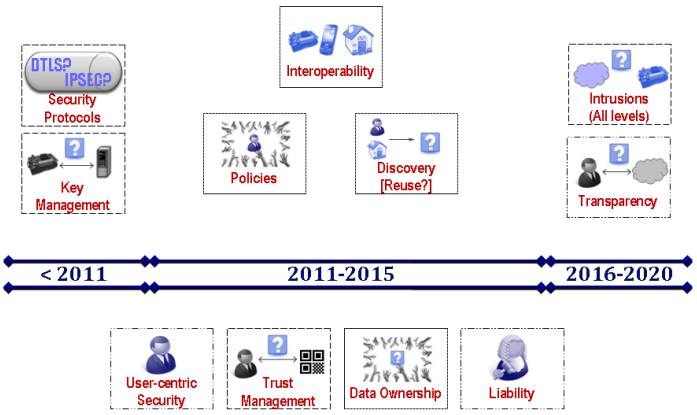

Figure 5. Future research challenges required in timeline

Security Protocols and Key Management as the work on these research challenges is far from finished. There are still some studies (e.g. better analysis on IPsec, Secure protocols for web services, new protocols, key management) that still require significant research.

Intrusions: This is a very important aspect that should be brought forward and studied as soon as possible, not in the 2015-2020 timeframe.

Trust Management: There are multiple dimensions of trust that must be considered (trust on the system, trust within the system), and these are significantly underdeveloped. To highlight this, in the consultation described in the Think Trust document, 64% of the respondents consider trust management as an important factor, but currently trust management is not even included in the timeline. This must be rectified.

There are also a number of underdeveloped research challenges highlighted in the Internet of Things: Strategic Research Roadmap [8]. These include:

Policies: As mentioned in the IERC document, we should be able to define "User-centric (context-aware) privacy and privacy policies". However, there isn't significant work yet on this particular aspect. In fact, the management of the whole lifetime of the policies must be considered (definition, development, enforcement, migration).

Discovery: The literature on service discovery in the IoT is vast. However, there seems to be few research results on secure service discovery. In fact, we need to look back and see if all the secure service discovery systems that have been developed in the past years (HYDRA, SENSEI, BRIDGE…) can provide a good foundation for creating IoT services.

Data ownership: This is a sensitive problem that must be urgently addressed. The user generates data, and data is immediately sent to the "cloud" (or whatever architecture). Then the user no longer controls his/her data. Who is the owner of the data? Who should be the owner of the data? Also, is it possible to store policies within the data, so non-authorized people cannot access it? All these issues need to be carefully considered and solutions reached.

Interoperability: While not a research challenge "per se", it is a foundational property that should be considered at all times. It

is highlighted here to remind people that the development of interoperable (security) systems is a must in the heterogeneous IoT. In fact, the existence of interoperable identities is truly a must, and is still an ongoing challenge with many ramifications.

A number of research challenges from the Towards a Trustworthy Information Society Think-Trust report [9] were highlighted also, including:

Transparency: Although transparency (i.e. monitoring, observability, logging) is relegated to the 2015-2020 timeframe if it is considered as an element of the self-* property, the Think-Trust consultation gave it an "importance" score of 80% (i.e. 80% of respondents thought it was important). Moreover, transparency is also essential to increase users' trust on the IoT.

User-centric security: User-centric mechanisms and user education/awareness received a score of 75% in the Think-Trust consultation, but there are very few (if any) advances in this area right now.

Privacy: Also scoring highly in the Think-Trust report, in order to ensuring societal acceptance of the IoT, users and consumer data and information privacy protection must be addressed and considerable further research on architectural and policy issues must be addressed. As presented at the FIA Aalborg session II.3 Internet of Things and the Future Internet [10], when looking at privacy and IoT aspects, the work going on with privacy impact assessment (PIA) 'Framework for RFID applications' [11] should be considered as a prototype for a broader risk assessment approach to IoT in order to ensure that privacy needs are catered for through architectural choices and technical policies. It is also required to work towards better governance for the IoT (e.g. using privacy by design and privacy by default principles as mentioned previously). With this in mind, there is an ongoing open consultation on governance for the IoT [12].

Last but not least, **Liability**: (66% of respondents considered as an important factor that spans over various challenges (governance, transparency, accountability,…), but it seems underdeveloped although there are some scholars including Rolf H. Weber that have studied the legal ramifications of the IoT [13].

3. Building International Cooperation in Trustworthy ICT – FP7 BIC project

3.1 Introduction

The purpose of the European Commission funded BIC coordination action project [14] is to foster cooperation between the EU and the international programme agencies and researchers in India, Brazil and South Africa within the focus areas of Trustworthy ICT, including trust, privacy and security, in order to:

(a) understand the activities and planning of the target countries; and

(b) carry out a mapping of the European Commission's planning to them, such that a common technical and policy alignment is viable.

The building of international cooperation (INCO) is a collaborative effort that only works if it reflects the views and priorities of the target countries as well as buy-in from technical experts of the EU along with the target countries. Hence, this component of community building is a key role of the Working Groups (WGs) of BIC as shown highlighted in figure 6. The areas and scope of the three working groups are the following:

1. WG1. Human oriented /citizen trust, privacy and security, which will focus on topics related to a multi-disciplinary approach for international cooperation amongst all stakeholders;

2. WG2. Network Information security / Cybersecurity, which will focus on topics related to the need for international cooperation for enabling the protection of networks and systems;

3. WG3. Programme /funding focus/ identify community, which will focus on the requirements, processes, mechanisms and barriers to enable collaboration opportunities.

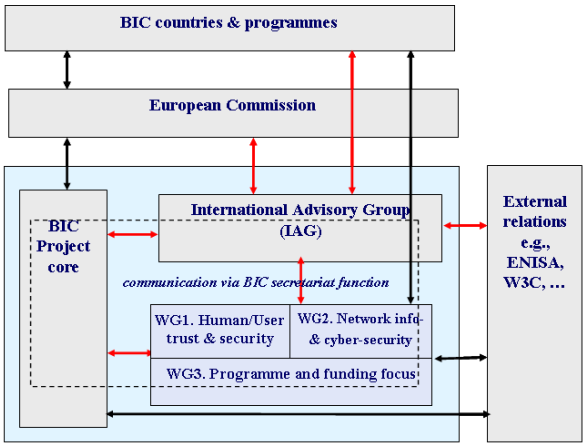

Figure 6. Overall structure of BIC

3.2 The need for international cooperation

From the European perspective, cooperation with third countries and international organisations has been and will be promoted with the following objectives:

- Strengthen EU's excellence and attractiveness in research and innovation
- Strengthen EU's economic and industrial competitiveness
- Jointly address global societal challenges
- Support EU's external policies.

3.3 Strategic approach for INCO

The current approaches towards INCO are based on a bi-lateral basis (tactical level) as shown in figure 7.

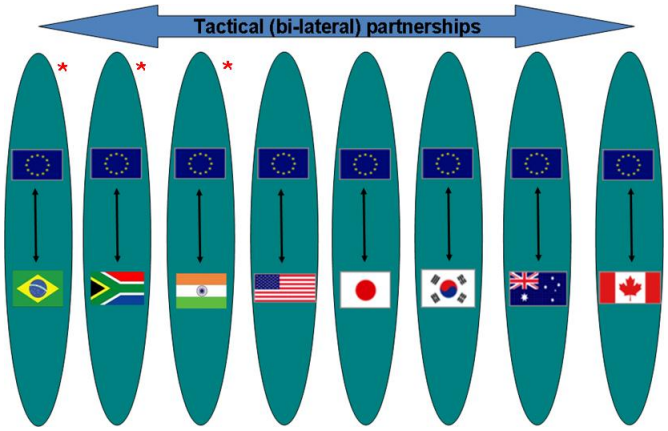

Figure 7. Bi-lateral (Tactical) approaches to INCO

The majority of the current mechanisms support regional bi-lateral activities. While this regional approach may work for higher level themes, the main difficulty arises when a particular research topic, for example, cyber security, needs to be addressed globally and multi-laterally amongst many regions and the bi-lateral approach is not suited for this type of longer term strategic activity.

Therefore, the BIC project is examining the feasibility of a more strategic approach based on multi-lateral partnerships as shown in figure 8.

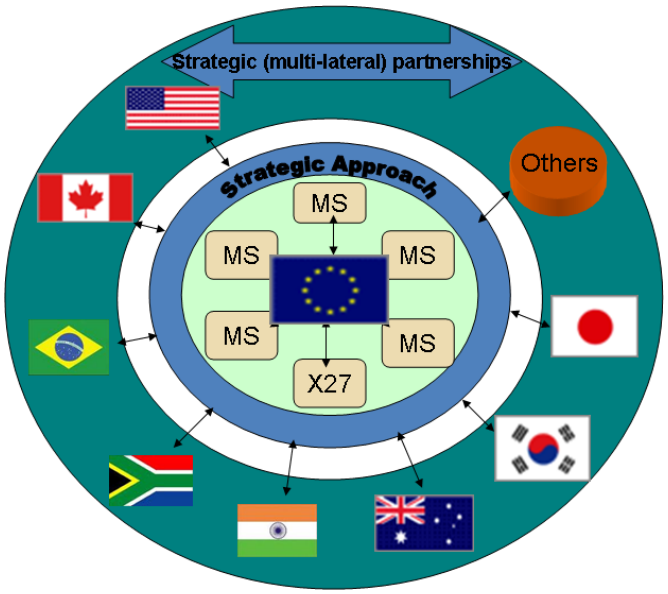

Figure 8. Multi-lateral (strategic) approaches to INCO

In order to examine the challenge of moving from a bi-lateral to a multi-lateral approach, the project held a recent workshop in June 2012 [15] bringing together a majority of the projects engaged in international cooperation to enable the following outcomes:

1. discuss their experiences and insights in order to brainstorm a strategy to move forward on international cooperation in future calls for collaborative research;

2. Forming the current bi-lateral (and potentially overlapping) country to country cooperation into a comprehensive and coordinated global cooperation.

In addition to BIC, a wealth of experience was represented from the following international cooperation projects: IST Africa, EuroAfrica-P8, FEED, AUS-ACCESS4EU, PACE-Net, EU – India Spirit, Synchroniser, Euro-IndiaGrid2, OpenChina-ICT, FIRST, FORESTA, PAERIP, SEACOOP, EuroAfrica-P8 and AMERICAS.

These projects gave their insights on their experiences and suggestions for improvement and the main point was agreement that it is a very good idea to move towards a more multi-lateral strategic position. However, in the discussions, it wasn't very clear how this strategy shift could occur within the current mechanisms that focus bi-laterally on seven (7) distinct regions.

In order to address this further, the BIC project are examining how the combination of their International Advisory Group and supporting working groups could assist in a move towards a more multi-lateral strategic approach.

3.4 BIC International Advisory Group

The BIC project has established an international advisory group (IAG) with the following terms of reference.

- The IAG will be the forum bringing together the countries representatives from the earlier INCO-Trust [16] countries (United States, Japan, Korea, Canada, Australia) and the BIC countries (India, Brazil and S. Africa) in a more strategic way;
- To facilitate collaborations between national ICT Trust and Security constituencies and related ICT trust and security related constituencies from other countries;
- To review the situation on International collaboration strategy in ICT trust and security on a regular basis providing advice on the priorities for international cooperation between the respective research communities, providing directions to the project and recommendations for improvement;
- Assist in the building of the working groups to enable BIC to structure relationships and linkages and facilitate contacts for theme based workshops or other networking events.

The IAG has representation from all the participant countries from both the researcher communities and programme management (funding agencies). The IAG is there to suggest and formulate the policies, processes and mechanisms to achieve international cooperation in the area of the ICT Trust and Security community. Three independent working groups, WG1, WG2 & WG3 with specific objectives as defined in the BIC WG Terms of Reference [17], have been formed comprising specialists from different countries and different specializations. Indeed, these WGs form the backbone of the Project; however, they alone would not be enough to take the entire project forward to its logical conclusion. They would, therefore, need to be supported by additional Groups and Sub-Groups in a structured manner as shown in figure 9, at the management and functional level with defined focus area, roles and responsibilities.

Since the nature of the project requires interactions amongst all participant countries to share the information, resources etc, the approach for the formal interactions, flow of information and smoothness of actions, it becomes natural that the groups and sub groups working for the project work closely with each other. Accordingly at international management level, it requires a change in approach from the existing bi-lateral approach i.e. EU-India, EU- Brazil, EU- SA, U.S, Japan, … to multi-lateral

approach where each participating country develops a formal system for direct multi-lateral communication and interacts with each other besides interacting centrally as well. Of course, the existence and role of a central body is essential for ensuring that the focus of the projects are not digressed and there is proper coordination amongst all adhering to the core principles and objectives of the project.

A possible multi-lateral structure is outlined here.

a. Core Working Group (CWG); based on the current BIC IAG and supporting WGs as shown in Figure 6.
b. Extended Working Groups (EWGs) – specific for each participating country as shown in Figure 9.
c. Special Function Groups – operating under EWGs as specialists at functional level.

Note: This is only an initial proposed structure and will be discussed in more details as part of the Working Group 3 and the International Advisory Group.

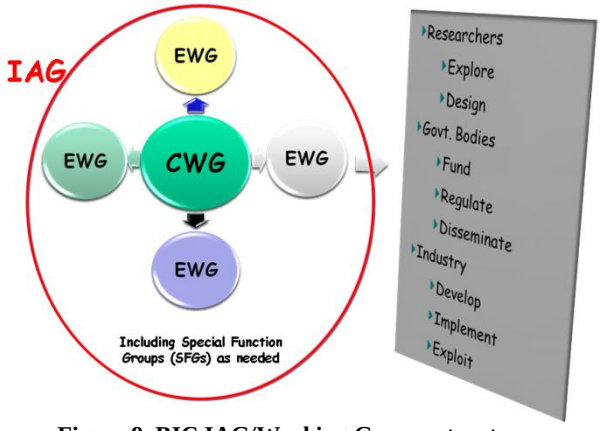

Figure 9. BIC IAG/Working Groups structure

4. CONCLUSIONS

There are significant research challenges related to the trust, privacy and security aspects of IoT, especially when looked at in either a centralised and/or distributed environments. Most research challenges (and papers, and business, and…) are focused on a centralized (i.e. cloud-based) models of the IoT, which makes a lot of sense for a number of reasons (business model, immediate usability and benefits, etc). However, the existence of a distributed IoT – where the intelligence and the provisioning of services is located at the edge of the network, and also various application platforms can collaborate with each other dynamically – is usually downplayed. In fact, this approach has been mentioned in various EU official documents and is being partially studied by some researchers (e.g. the IoT-A consortium, ...), but no relevant studies exist yet that we could find. Still, it can provide interesting scenarios. For example, "the IoT of a hospital can interact with the IoT located in the household of a patient, or even with the PANs of the personnel located inside the premises. Moreover, this interaction can be extended to higher-level cloud-based services, where the hospital can not only send certain information (e.g. bed occupancy) when queried but also acquires additional high-level information (e.g. overall bed occupancy) to improve its own services". In fact, the distributed model should exist because there must be some kind of collaborations between cloud-based IoT services and companies in order not to create opaque silos of information. Therefore, it would be interesting to discuss what are (some) advantages and disadvantages of this distributed approach in terms of security (Beyond the business model, of course). The research community should avoid a jump to advocate the use of distributed architectures over centralized architectures or vice versa but instead to study their existence in order to spark some discussions and focus on the relevance of the advantages, in particular, regarding the user-centric security. This approach can also spark some interesting discussions on managing rights of individuals (i.e. privacy) and their interaction with IoT objects.

One particular advantage of a distributed approach for IoT would be towards the development of user-centric security. The core idea is that every entity has more control over the data it generates and processes. There are several consequences of this approach. Firstly, entities can control the granularity of the data they produce. Secondly, entities can define their own access policies. Thirdly, entities do not need to provide all the data they produce, only the data that is needed by the external entities for a particular service. Note that in a centralized IoT, an entity can also decide whether to share or not a particular information stream. Still, as the intelligence is located on the central system, the type of services it provides will be limited to the amount of information it receives. Another advantage of a distributed system includes enhanced fault tolerance (although it is recognised there will be some inherent problems), If the intelligence is located at the very edge of the network, partial services can be provisioned locally even if the Internet fails. Also, survivability and availability improves: there are more service providers that can dynamically access various data providers, and if there is a failure within the system, it can be able to rearrange itself to provide a 'best-effort' service. But there is a catch here: these additional service and data providers become potential objectives for malicious entities. And when subverted, they can be used to target the services of the whole network. Note, however, that this problem also affects the centralized approach: data providers can be controlled by an adversary, pouring bogus information and hindering the reliability of the services.

Some of the disadvantages of a distributed environment for IoT include those related to the Heterogeneity of IoT (e.g. especially with regard to identity). In a centralized architecture, some of the challenges are inherently more simple. The reason is straightforward as the application logic is mainly located in one system (e.g. a cloud-based IoT application platform) that provides a limited set of well-known entry points (e.g. APIs). Protocols, Access Control are also at a disadvantage because in the distributed approach, extra challenges arise: any entity can connect with any other entity at any time, these entities might not know each other in advance, and also limited devices can exchange information with other limited devices.

The building of international cooperation is difficult when using a bi-lateral approach as it takes significant time for all of the parties to come together to try to align their activities and priorities. Therefore, it is even more difficult for a multi-lateral approach when building a longer term strategy as proposed within this paper. The BIC project has proposed a strategy and will follow up in the near future with interested countries as exemplars.

Although intensive undertakings were researched for the building of this paper, the authors wanted to make it clear that there might already be ongoing work that was missed in the presentation. For example, in newly starting research projects and/or current running projects, where public deliverables are

potentially limited. Nevertheless, in order to prepare this presentation the state of the art on IoT trust, privacy and security was thoroughly checked and highlighted. After all, the purpose of the paper is to invite and enable all of the readers to further clarify, share their knowledge and to enrich the materials within the paper and presented at SecurIT 2012.

5. ACKNOWLEDGMENTS

The BIC project [4] is funded by the European Commission's DG-CONNECT Unit H.4: Trust and Security [18].

6. REFERENCES

[1] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/enet/internet-of-things-in-2020-ec-eposs-workshop-report-2008-v3_en.pdf

[2] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf

[3] http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

[4] BIC Project, http://www.bic-trust.eu/ project within the portfolio of the European Commmission's DG-CONNECT Unit H.4: Trust and Security research.

[5] Clarke, J., 2011. Report of the European Commission DG INFSO Trust and Security unit workshop on Network and Information security: research ideas, Brussels, Belgium. http://cordis.europa.eu/fp7/ict/security/workshop22092011.pdf

[6] Clarke, J. 2010. Report of Session II.2 Internet of Things and the Future Internet, Future Internet Assembly, Budapest. http://www.future-internet.eu/home/future-internet-assembly/budapest-may-2011/session-ii3-internet-of-things-and-the-future-internet.html

[7] Skarmeta, A., Clarke, J., et al. 2012. Report of Sessions II.3 Internet of Things and the Future Internet, Future Internet Assembly, Aalborg. http://www.fi-aalborg.eu/index.php/program/session-2-2-internet-of-things-iot-and-future-internet-fi-architectures

[8] Vermesan, O., et al. 2011, Internet of Things Strategic Research Roadmap, published by The IoT European Research Cluster — European Research Cluster on the Internet of Things (IERC). http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf

[9] Foley, B., Sullivan, K., et al., 2010. Towards a Trustworthy Information Society - Report of the RISEPTIS Advisory Group, published by the FP7 Think-Trust project. http://www.think-trust.eu/riseptis.html

[10] Barani, B. 2012. Presentation at FIA Aalborg session II.3 Internet of Things and the Future Internet, Future Internet Assembly, Aalborg. http://www.fi-aalborg.eu/downloads/Session_2.2_Barani.pdf

[11] PIA framework for RFID http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

[12] Open consultation on IoT governance: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance

[13] Weber, Rolf H., Weber, Romana, 2010. Internet of Things: Legal Perspectives. ISBN-10: 3642117090 | ISBN-13: 978-3642117091 | Edition: 1st Edition.

[14] BIC Web site http://www.bic-trust.eu/

[15] BIC Workshop June 2012 site http://www.bic-trust.eu/events/bic-workshop-on-the-cross-domain-coordination-of-international-cooperation-day-1-and-technical-themes-in-trustworthy-ict-and-inco-day-2/

[16] INCO-Trust web site http://www.inco-trust.eu/

[17] BIC Deliverable D2.3 - Interim report of the Working groups activities (restricted).

[18] DG CNECT Unit H.4 http://cordis.europa.eu/fp7/ict/security/

SecurIT 2012, August , 2012, Kollam, India.