Resilience of the Internet of Things (IoT) from an Information Assurance (IA) Perspective

Rebecca Rogers
Cyber Security Unit (BUCSU)
Bournemouth University
Poole, UK
bucsu@bournemouth.ac.uk

Edward Apeh
Dept. of Computing and Informatics
Bournemouth University Poole, UK
eapeh@bournemouth.ac.uk

Christopher J. Richardson
Cyber Security Unit (BUCSU)
Bournemouth University
Poole, UK
cjrichardson@bournemouth.ac.uk

Abstract *- Internet infrastructure developments and the rise of the IoT Socio-Technical Systems (STS) have frequently generated more unsecure protocols to facilitate the rapid intercommunication between the plethoras of IoT devices. Whereas, current development of the IoT has been mainly focused on enabling and effectively meeting the functionality requirement of digital-enabled enterprises we have seen scant regard to their IA architecture, marginalizing system resilience with blatant afterthoughts to cyber defence. Whilst interconnected IoT devices do facilitate and expand information sharing; they further increase of risk exposure and potential loss of trust to their Socio-Technical Systems. A change in the IoT paradigm is needed to enable a security-first mind-set; if the trusted sharing of information built upon dependable resilient growth of IoT is to be established and maintained. We argue that Information Assurance is paramount to the success of IoT, specifically its resilience and dependability to continue its safe support for our digital economy.*

Keywords—Internet of Things, Information Assurance, Cyber Security, IA Architecture, Resilience, Socio-Technical Systems, Communities of Interest.

I. INTRODUCTION

Historically, Information Assurance (IA) was developed on risk management principles, placing various InfoSec defences against electronic attacks [1]. The principles behind information risk management and risk assessment is to identify areas of weakness in system defences that may impact harm and place information security controls (ISO/IEC 27002:2013) and protection mechanisms against them [2]. Although prevention must always be at the forefront of an enterprise's information security management system (ISMS), it is not always possible to militate against all attacks and therefore a more holistic approach is needed [3]. An Information Assurance perspective would provide insightful cyber situation awareness; help build a common operational picture to recent and future deployment of resilient IoT socio-technical systems (STS); improve enterprise decision making cycles and mitigate risk, thereby limiting the damage caused by malicious and erroneous attacks. From IA, we can learn to engender trust and resilient system-safety into IoT STS and their user communities of interest - human actors, IoT devices and their agents. Incorporating eight IA attributes, as illustrated in figure 1, in to STS it is possible to architect a more resilient, dependable system, capable of navigating and surviving the complex digital world and its cross-domain cyber threat landscape [4].

There is a plethora of regulatory compliance requirements in place to try to protect digital businesses and their customers. However, being merely compliant is no longer sufficient; cyber resilience posture must be adopted in order to ensure success when operating a hyperconnected enterprise [5]. In order to survive and ensure longevity, these businesses must be constantly evolving, being able to quickly adapt and/or react to the ever changing landscape and have the ability to recover rapidly from unforeseen events.

Figure 1: Dynamic Attributes of Information Assurance

The beginning of IoT can be traced back to the conception of the Internet itself. In 1989 the World Wide Web was proposed and in 1990, the first internet device was conceived: a toaster that could be turned on via the Internet [6]. Move forward to 2008, when more machines or objects were connected to the Internet than people, society started to

become reliant on these connections for the functioning of modern life. Now, the socio-technical system capacity of IoT is an integral part of our lives with everything from communication, to medicine, to travel being enjoyed, controlled and monitored via the Internet [7]. In a short space of time, society has gone from desktop computers to wearable devices that can relay real-time medical data and home appliance that can detect faults and relay them to manufacturers. Not only does information-driven society crave the use of these devices, it's starting to rely on them and with reliance, comes safety and trust issues. This key assurance attributes to IoT: its pervasiveness to every corner of the world, the demands to making its devices hyperconnective, giving effective capability to connect to the Internet and other networks of interest, accessible to anyone or machine regardless of its virtual or physical location requires more intelligent research and resilient architecture. Networked IoT socio-technical systems are extremely complex owing to their scalable size and distributed nature, with a multitude of subsystems and interconnections as well as its interactions with the human environment and their legal and regulatory constraints [8]. Accordingly, IA issues related to these factors are emerging at speed.

The smart environment of IoT offers many advantages, including the saving of time, energy and resources; things that are increasingly in short supply in today's age. As a society becomes dependent on IoT, our privacy, safety and security is reliant on the trustworthy operation of these systems by their operators and owners [9]. Digital economics drives price reduction of connected devices, increasing their access and availability, financing new capabilities and scaling-up digital capacity. The IoT market is expanding rapidly with forecasts estimating that within the next 5 years the industry will double from 25 billion connected devices to 50 billion, outnumbering people by approximately six to one [10].

II. Information Flow in IoT

IoT has dramatically changed the way in which organisations interact with users and customers. Long-term after-purchase relationships are now formed whereby information is passed between the customer and provider allowing insights into user behaviour and product performance. This virtual world of enterprise is known as the 5th domain. Where the cost of doing business in the first 4 domains: Land, Sea, Air and Space, is significantly rising, in contrast and with limited equipment, staff and a physical presence required in the 5th "Cyber" domain. Here digital economics ensures accessibility is cost efficient and more attractive as a primary business focus for all enterprises [4]. This value is not only important to the enterprise itself but also brings benefits to the customers and its communities of interest. Operating a business online in this way brings with it an increasing level of complexity and a wide range of new threats for businesses. These complex challenges require changes in the approaches taken to IT risk assessment, its assurance and a paradigm shift in appreciation towards security by design.

Assured architecture of IoT can be split into three parts: (1) the Internet of Things itself; (2) Big Data and (3) Intelligent use of the information [10]. These complex socio-technical systems where trustworthy interactions are required between technology and people in virtual and physical ways including: hardware, software, procedures, laws and regulations, data and data structures are more open to external factors now than ever before with further rapid changes occurring information technology and the use of AI towards Singularity [11].

These systems are so fundamental to modern organisation operational ability that any system failures can give rise to major financial and reputational damage. It is therefore imperative that organisations and the socio-technical systems they utilise are resilient. IoT underlines the importance of the security and trustworthiness of the interactions between the social and technical elements of a system and the behaviours that emerge from these interactions [12]. By understanding these interactions in more depth and the risks they pose, a fuller picture of the cyber-risk landscape can be built up by Information Assurance professionals.

The Cyber Domain is further complicated by the fact that perceptions of "locality" to the respective globally displaced communities of interest (COIs), each of which will often have different disruptive aims, goals and challenges; different network structures and interconnection of systems with fluctuating boundaries non-compliant to established architectures. Establishing the right balance with these often competing IoT STS will be challenging, but also a great opportunity for IA Architecture and resilience system designs.

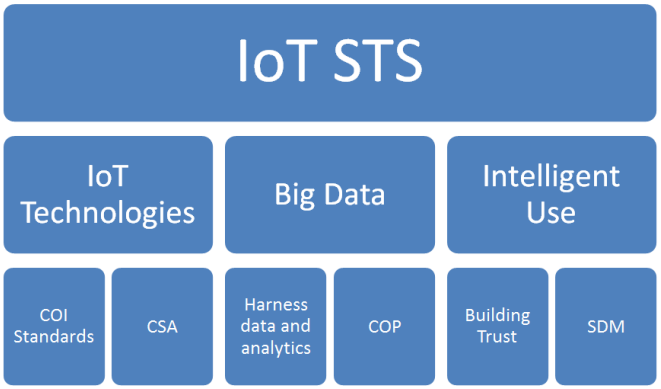

Figure 2: Assured Architecture of IoT STS

As illustrated in figure 2, by taking the following steps, IA can greatly improve IoT's three constituent parts by:

a) *Internet of Things Technologies:* Establishing acceptable standards for Service Provision: Working with IETF, ITU and the EU's Internet of Things Cluster (IERC) can formulate goals and standards that meet expectation of their COIs enabling better system of systems integration, information sharing and Cyber Situation Awareness (CSA).

b) *Big Data:* COIs can underpin the IA cycle of Cyber Situation Awareness, establishing and maintaining a Common Operational Picture (COP) with appropriate and robust protocols and improving Superior Decision Making (SDM) with hard evidence extracted from relevant IoT STS data. IA Architectures can provide a mechanism and capability for harvesting and collating the data for analytical analysis and potential service value.

c) *Intelligent Use:* COIs can utilise time to rebuild structures and relationships that work on the assurance of trust management between themselves and the communities they serve in order to accelerate joint working and data sharing on IoT STS

Business alignment and stewardship on the efficiency and sustainable data governance of the COIs and their deployment of IoT STS would also produce better financial returns.

A. Information Assurance for the Internet of Things

H. Sato, et.al. [13] describes the IoT as four distinct layers; the cyber physical layer where the devices are placed, communicating with cyberspace via the internet; the device layer which is the physical devices themselves including smartphones, monitoring devices, smart cars; the data service and control service layer – the layer connecting the devices to the internet and the Big Data analysis cloud which collates and analyses the data in the service layer. Each of these layers has its own complex security issues and these issues overlap creating a tangled web of ever increasing complexities.

Securing IoT devices requires optimal cryptography algorithms and key management systems on top of efficient security protocols [3] and in order to mitigate against the vast array of threats it faces, it must have strong security foundations at all steps and layers. The main aim of information assurance should be to manage these risks and threats, and gain trust, ensuring that information can flow across systems which are both protected and resilient [4].

Governance adds to and strengthens the trust in IoT systems [3], due to their connectivity and the oversight by the system owners, feedback can be access quickly and as the basis for issuing patches for example. However this governance also has its drawbacks; although it offers stability it can also be excessive which results in an environment that is overly monitored and controlled which ultimately reduces the trust users have in the system, largely due to the perceived (or indeed real) lack of privacy and following that trust. Trust and more importantly, trustworthiness are an integral part of our everyday experiences and is a basic underpinning of cooperative environments [14]. When looking at IoT, trust is paramount for the wide adoption of these systems in the digital world [15].

Trustworthiness can be described as a combination of dependability, availability and integrity. That is, how much can you relay on a system to perform tasks, perform them correctly and at the time you want them to. Miclea and Sanislav [16] state that dependability usually has the following attributes: Availability, Reliability, Safety, Integrity and Maintainability. Not only is it imperative to establish trustworthiness, but the monitoring of the trust characteristics is paramount for a systems long term success.

B. Cyber Incidents damage Trust Management

Society is reliant on the storage, process and transmission of data therefore ensuring the integrity, security and privacy of this data is paramount. Inadequately protected data gives rise to fraud which leads to reputational and financial losses for organisations and in turn a loss of trust in the system for the user. The greatest threat to online businesses is damage to their reputation and customer trust in their organisation. An organisations reputation and brand is a valuable asset and the basis of its success and ultimately its income [17]. The digital economy's financial success can easily be brought down by data leakage, loss of customers as well as lawsuits from those customers, shareholders and the intervention of data protection authorities and fines.

Most enterprises take years to build up their trustworthy reputation of a reliable organisation but overnight that reputation can be irrecoverably damaged by a cyber-attack or massive data leak. This applies regardless of whether an incident was the result of data misuse or an unpredictable event. Humans base decisions to trust on historical evidence that suggests the future trustworthiness of a given interaction [18]. However when the prediction of future trustworthiness turns out to be false, trust is lost for all ongoing interactions and rebuilding that trust is difficult if indeed possible at all.

Clearly cyber-attacks are damaging and costly, however the true cost to an online enterprise is in the damage to the trust the users place in the system. Not only can cyber-attacks damage individual businesses, the knock on effect for the whole digital economy could be devastating. It is clear therefore that online enterprises must work with not only government and regulatory groups but also each other to ensure the long term success of doing business in this, the 5th domain.

Due to the multiple layers of information flow for IoT devices, enterprises are under constant pressure and have to deal with the threats in these environments and the complex conditions that are constantly changing and evolving. Faced with these turbulent conditions, in order to ensure long term survival of the business, they must embrace agility and resilience to the core of any information assurance strategy [19].

C. Culture change and Trust

A shift the IoT paradigm is needed to transform performance, deliver significant system trust and improve the data quality and security of IoT STS. Significantly, culture changes are essential components of establishing good resilience in IoT STS. Culture is often seen as an abstract idea by organisations, and intangible asset not easily transposed to business goals. The abstract perception often makes it difficult for company boards to address the reasons for employee resistance to change and the fundamental need to build human resilience in a socio-technical system.

Corporations need to identify a Board Champion and also establish a board belief/trust to the importance of culture changes required in assuring STS. It may be too much to expect engage all to changes, but taking the majority through a disruptive change will make a difference. In this respect, the company boards need to realize tangible goals for change.

a) *Vision: Provision of the COIs to understand and exploit IoT STS digital technology to improve the quality of services they provide and enhance working in the digital environment.*
b) *Cyber Psychological: To create the human elements that interface computational trust and behavioural trust [20].*
c) *Human Factors: Endeavour to humanise the process and encourage an emotional buy-in.*
d) *Collaborate: Develop a COI view towards the deployment and maintenance of an IoT system interconnected and interacting with local/global societies.*
e) *Invest in People: COIs must encourage corporate*

buy-in with continued investment in to people skills.

f) *Manage Trust: Give staff an input into the decision making process to encourage ownership and break down change resistance.*

Embedding culture change in to an organisation also requires intellectual capital to manage emerging ethical issues when IoT becomes part of the solution. Deploying IoT STS is often viewed as a technological enhancement that inevitably results in changes and people's perception on modernisation. Again, this is about constructing value, through innovation, both within the IoT systems and the business opportunities that are envisaged. This disruptive capability influences how IoT in its turn changes people's values. This is an excellent research area for scientists to learn with technologists and should deepen and provide better understanding of the PESTLE influences on the Socio-technical systems that evolves from IoT deployments [21].

III. IA TRUST MANAGEMENT AS A RESILIENCE ENHANCER IN IOT

The concept of resilience is relatively new and the interpretation of the meaning of this is still widely debated however in general it is taken to mean the ability to respond to disturbance without regressing [22]. Although the prospects of unforeseen events are at the forefront of those dealing with information assurance, organisations are over over-whelmed when they occur and struggle to react and adapt appropriately [23]. Resilient systems strive to cope with severe instabilities and disruptions and return swiftly to their desired state of operations [19]. Resilience is two-fold; a system must be robust against attacks (that is be able to prevent most attacks in the first instance) and it must be able to return to a safe state if an attack has been successful [24]. The main reason to have a resilient system in the Cyber Domain is to maintain trust and privacy by mitigating security risks. Ultimately resilient enterprises are in a better position to protect their customers, provide better and secure services and therefore earn and maintain this trust.

In order to develop and retain a resilient system, enterprises must implement a variety of measures; adopt security by design; ensure systems can operate when parts have been compromised and reduce time needed to fix issues identified [8]. However it is not the number of technologies that make an enterprise resilient, the key is using those technologies effectively as part of a security strategy [25]. For example, situational awareness is also necessary to identify treats, prevent them and recover from successful attacks [24]. This involves collecting information from a wide range of sources which in itself involves trust in order to permit information exchange between disparate parties and systems. Due to the nature of IoT devices, that is their connectivity, it is possible to use this for the advantage of system security by effectively monitoring the real-time faults and security breaches and continually updating and applying appropriate security measures as and when needed, where they are needed.

The concept of trust management was not developed for the dynamic environment that is the IoT but for more basic and static systems and it does not lend itself easily to this new 5th domain [26]. An effective trust management system for IoT needs to take into consideration the largely distributed nature of this domain as well as the complexity of many of the applications used by it. Although trust issues have been widely researched in both real and virtual scenarios, it is not clear how appropriate these models are for use in an IoT context and there has been limited research into how existing trust models should be transformed for use in this arena [27].

Once trust parameters and values are identified, the task of trust management is required to monitor these values. The key to effective trust management is to continuously monitor and analyse system behaviours, identifying threats and recommending and executing potential actions that will militate against issues identified [15]. One aspect of trust management is trust negotiation between interested parties; this negotiation is ongoing and requires active sharing of data and information [28]. Enterprises must learn to communicate and share data regarding breaches. By sharing this intelligence, it will engender a more visible threat landscape and allow information assurance professionals to see attack patterns allowing them to constantly develop their security processes and policies. This constant and proactive adaptation is paramount to the long-term resilience of these complex socio-technical systems.

Due to the very nature of IoT and the everyday items that utilise it, the first hurdle in establishing trust is to get the users to trust the objects themselves which often are making decisions for their users [26]. Leister and Schulz [29] states that trust in IoT is not transparent enough for users, therefore clear trust indicators must be developed for humans to feel comfortable in using and trusting such connected devices.

Humans are an integral part to any Socio-Technical System, and the human factor is an integral part of cyber-security. In the past, much information assurance architecture has worked on developing the security domains of Confidentiality, Integrity and Availability (CIA) and it is only in the last few years that more focus has been placed on the human factor which largely influences these complex socio-technical systems [21]. Even though security policies are used to convey secure practices to employees and other stakeholders, people often do not comply with these policies and these results in exposing the organisation to various risks [24].

Understanding and changing how people operate online is one of the major challenges of cyber-security. The users themselves can also contribute to the resilience of IoT systems, due to the adaptability of humans and the accessibility of some technologies, often they bridge the gaps between elements of the technology manually that they perceive not to work efficiently [12]. These adaptations themselves can result in pitfalls which the users can instigate but blame the owning enterprise when issues occur. In order to ensure that these risks are mitigate enterprises need to either remove the potential for these kind of adaptations or incorporate a way to monitor the adaptations, measure the risks and potential benefits of them and potentially roll them out to other parts of their systems.

Conceptualising trust values within IoT STS and the importance individuals place on these trust values is dependent on the perceived quality and assurance of the systems, services and devices engaged. Within information assurance, trust, trustworthiness and trust management have become crucial components of digital interactions, HCI issues and more recently with the inter-activities of IoT STS. This convergence of human morals with machine intelligence will establish numerous models of trustworthiness and confidence that might have many shades of interpretation, collective meaning and differing shared situational awareness. Furthermore, it has been attested that trust could be defined for

the IoT environment as a level of confidence where the system domain can ensure another domain or entities/devices within for specific services in a given context [30].

IV. Conclusion

Building trust in an organisation is one element of ensuring a resilient enterprise will move forward in the digital economy. However there are other elements, not least security, which must all work holistically with business processes to ensure that maximum resilience, is achieved. Enterprises can employ a wide range of tools to try and ensure resilience and trustworthiness however it is not how many tools the enterprises has but how well they are implemented and employed that is the crux of the issue. It is not how the enterprise behaves once an adverse event has occurred that is an important sign of their trustworthiness but rather how that enterprise behaves before the event, how prepared they are to weather the storm and come out the other side with limited reputational and financial damage. Assured Enterprises need to be both flexible and robust at the same time in order to maintain a secure and trustworthy system. The very notion that an online enterprise can be completely protected is not only unrealistic but can breed a false sense of security which in itself is a huge risk and should occupy the interests of all company boards and C-Suites. Therefore to compensate for the inability to be completely protected against attack, online enterprises must ensure they are resilient [31]. Simply implementing security best practice is not adequate in the current cyber threat landscape, enterprises must assume that attacks will happen and constantly adapt more resilient systems to mitigate the risks and resulting damage.

Although trust is often considered to be a human attribute, it can be coupled with IoT devices, machine intelligence and/or digital media systems and this requires (S) better analysis of our digital society that (M) measures trust integrity which is (R) realistic and (T) timely to the environment as well as (A) attainable both in its design and exploitation. This SMART approach will help distinguish elements of trust (attraction, belief, expertness, etc.) and assurance (management, risk, resilience, etc.) within the Cyber domain. IoT STS cross domain solution as a vehicle for valued and respected relationships would include the interlacing and connectivity of (i) users to devices, (ii) between devices and (iii) from devices to users. Within our COIs, the intelligent use of Big Data and the IoT STS will generate an ethos to the new paradigm where knowledge exchange between man and machine will contribute to trusted digital interactions.

Ultimately, cyber-resilience, and trustworthiness improves user confidence in the system as well as scaling businesses potential. Although the IoT offers vast potential for society, the management of risks as identified in this paper will be ever present requiring better research into ways to maintain the trustworthiness of the devices and the development of systems that ensure the public can continue to make use of them in a safe and secure manner is paramount.

V. References

[1] Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2010.

[2] ENISA, "European Union Agency for Network and Information Security," European Union Agency for Network and Information Security, 2005. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management. [Accessed 27 August 2016].

[3] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," IEEE Computer, vol. 44, pp. 51-58, 2011.

[4] C. J. Richardson, "Bridging the air gap: an information assurance perspective," University of Southampton, Southampton, UK, 2012.

[5] World Economic Forum, "Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats," World Economic Forum, Geneva, 2015.

[6] P. Suresh, R. H. Aswathy, V. J. Daniel and V. Parthasarathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," Science Engineering and Management Research (ICSEMR), pp. 1-8, 2014.

[7] D. Shin , "A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things," Telematics and Informatics, vol. 31, no. 4, p. 519–531, 14 November 2014.

[8] Royal Society, "Progress and research in cybersecurity: Supporting a resilient and trustworthy system for the UK," The Royal Society, London, 2016.

[9] H. A. Boyes, "Trustworthy Cyber-Physical Systems - A Review," Cardiff, 2013.

[10] J. Baho, "Internet of Things," GE, 2015.

[11] A. Sandberg, "An overview of models of technological singularity," Oxford University, Oxford, UK, 2010.

[12] M. Werfs and G. Baxter, "Towards resilient adaptive socio-technical systems," ECCE, 2013.

[13] H. Sato, A. Kanai, s. Tanimoto and T. Kobayashi, "Establishing Trust in the Emerging Era of IoT," IEEE, pp. 398 - 406, 2016.

[14] W. J. Adams and N. J. Davis, "Toward a Decentralized Trust-based Access Control System for Dynamic Collaboration," New York, 2005.

[15] N. G. Mohammadi, T. Bandyszak, M. Moffie, X. Chen, T. Weyer, C. Kalofiros, B. Nasser and M. Surridge, "Maintaining Trustworthiness of Socio-Technical Systems at Run-TIme," in Trust, Privacy, and Security in Digital Business, C. Eckert, S. K. Katsikas and G. Pernul, Eds., Switzerland, Springer International Publishing, 2011, pp. 1-12.

[16] L. Miclea and T. Sanislav, "About Dependibility in Cyber-Physical Systems," 2011.

[17] W. Coghlan, "The Economist Perspectives," 2016. [Online]. Available: https://www.eiuperspectives.economist.com/technology-innovation/cyber-chasm-how-disconnect-between-c- suite-and-security-endangers-enterprise-0/article/protecting-brand%E2%80%94cyber-attacks-and-reputation-enterprise. [Accessed 20th July 2016].

[18] K. Aberer and Z. Despotovic, "Managing Trust in a peer-2-peer information system," Atlanta, 2001.

[19] L. M. Camarinha-Matos, "Collaborative networks: A mechanism for enterprise agility and resilience," in Enterprise Interoperability VI - Interoperability for Agility, Resilience and Plasticity of Collaborations, K. Mertins, F. Benaben, R. Poler and J. P. Bourrieres, Eds., Springer, 2014, pp. 3-11.

[20] V. Gilgor and J. M. Wing, "Towards a theory of trust in networks of humans and computers," in International workshop

on Security Protocols, Cambridge, UK, 2011.
[21] European Research Cluster on the Internet of Things, "Internet of Things: IoT Governance, Privacy and Security Issues," European Commission Services, Brussels, 2015.
[22] R. Martin , "Regional Economic resilience, hysteresis and recessionary shocks," Journal of Economic Geography, vol. 12, no. 1, pp. 1-32, 2012.
[23] M. Morisse and C. Ingram, "A mixed Blessing: Resilience in the Entrepreneurial scoio-technical system of bitcoin," Journal of information systems and technology management, vol. 13, no. 1, pp. 3-26, 2016.
[24] J. Rajamaki, "Towards a Design Theory for Resilient (Sociotechnical, Cyber Physical, Software-Intensive and Systems of) Systems," in Recent Advances in Information Science, X. Zhuang, Ed., Barcelona, WSEAS, 2016, pp. 29-34.
[25] Symantec, "The Cyber-Resilient Enterprise: Harnessing Your Security Intelligence," Symantec, Mountain View, California, 2014.
[26] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, "Internet of Things: Vision, applications and research challanges," Ad Hoc Networks, vol. 10, pp. 1497-1516, 2012.
[27] J. Schrammel, J. Hochleitner and M. Tscheligi, "Privacy, Trust and Interaction in the Internet of Things," in Ambient Intellegence, Berlin, Springer-Verlag, 2011, pp. 378-379.
[28] H. R. Rao and S. Upadhyaya, Information assurance, security and privacy services, Bingley: Emerald, 2009.
[29] W. Leister and T. Schulz, "Ideas for a Trust Indicator in the Internet of Things," in The First International Conference on Smart Systems, Devices and Technologies, 2012.
[30] I. Mihaela, A. Danzi, H. Koshutanski and L. Telesca, "A peer-to-peer multidimensional trust model for digital ecosystems," in Digital Ecosystems and Technologies 2008 2nd IEEE International Conference , 2008.
[31] H. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance," MITRE, 2010