# IoT Design Challenges and the Social IoT Solution

*Full Paper*

**David Goad**
Sydney University
david.goad@sydney.edu.au

**Uri Gal**
Sydney University
uri.gal@sydney.edu.au

## Abstract

The IoT (Internet of Things) promises to be the major phenomenon in information technology in the near term. By some forecasts more than half of all new IT system deployments by 2020 will incorporate some form of IoT technology. Currently, however, there is no dominant IoT platform and no universal IoT design standards currently in use. This contributes to Architectural Heterogeneity which in turn contributes to high integration costs and inhibits IoT benefits realisation. The use of universal design standards presents one solution to this problem. Social Internet of Things (SIoT) methods use the way that people manage social relationships as a reference architecture for the way to manage the interaction between the various Things in an IoT network. This paper discusses some of the current IoT design challenges and presents solutions couched in SIoT that can be used as standards for future IoT designs to reduce Architectural Heterogeneity.

**Keywords**

IoT, Internet of Things, Architecture, Social Internet of Things

## Introduction and Background

The term Internet of Things (IoT) was first coined in 1999 by Kevin Ashton, a British technology pioneer who cofounded the Auto-ID Centre at the Massachusetts Institute of Technology (Ashton 2009). Over the years the term IoT has had many definitions in the literature but it generally refers to the connection of everyday objects to the internet to generate highly useful real time data about us and the world around us. This data can be acted on in an automated or semi-automated fashion. In this way IoT devices become a medium for human to human and human to environment interaction.

IoT promises to be the major phenomenon in IT in the near to medium term. By 2020 it is forecast that more than half of all new IT system deployments will incorporate some form of Internet of Things (IoT) technology (Friedman et al. 2015). Currently, however, there is no dominant IoT platform, with 75% of business likely to deploy 3 or 4 IoT platforms by 2020 (Lheureux et al. 2015). A recent survey identified more than 16 internationally commercially available IoT platforms (Velosa et al. 2015). This list did not include the potentially hundreds regionally and locally based solutions.

This proliferation of solutions with no observable standards leads to significant *IoT Architectural Heterogeneity*. This in turn leads to significant integration costs and substantial overruns in deployment timelines for IoT projects and poor benefits realisation (Friedman et al. 2015). Integration costs are now reported to represent the bulk of IoT deployment costs (Lheureaux et al. 2016). As a consequence a number of researchers have identified reducing *IoT Architectural Heterogeneity* as a primary target area for future research (Ning et al. 2013; Xiaohui 2013; Zhang et al. 2014).

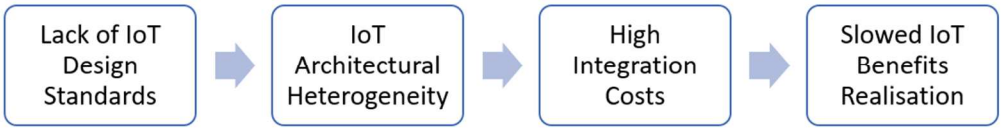


**Figure 1. Causality between lack of IoT Design Standards and IoT Benefits Realization**

One way of addressing this *Architectural Heterogeneity* is through universal design standards. Whilst significant work has already been done in the area of IoT Architectural Design standards (Alam et al. 2015; Atzori et al. 2012; Sarkar et al. 2014; Voutyras et al. 2014; Zhang et al. 2012), its incorporation as industry standards adopted by business has been slow and suggests the need for a different approach and even further research.

A potential strategy to solve this core problem of IoT design standards can be found in the concept of the Social Internet of Things (SIoT). The term SIoT was first defined by Atzori et al. (2011 as the process of building social relationships amongst IoT objects. The concept was further developed architecturally by Atzori et al. (2012) by providing a specific reference architecture, defined management processes and then demonstrating the solution through several illustrative example applications. At a conceptual level, SIoT uses the way that people manage social relationships as a reference architecture for the way to manage the interaction between the various nodes in an IoT network. These interactions include Thing to Thing, Person to Thing and Person to the Environment. It is possible to gain efficiencies in the way the various "things" work together by having them work and respond in similar ways. The architectural design concepts of SIoT represent a potential solution to the problem of IoT architectural heterogeneity by providing one blueprint for overall IoT architectural integration design.

This paper discusses some of the current IoT design challenges and presents solutions couched in SIoT that can be used as standards for future IoT designs. Recognised as only a subset of the design issues that result from *Architectural Heterogeneity,* this paper considers the application areas of *Security*, *Reliability* and *Control* in the design of IoT architecture. It discusses how *Architectural Heterogeneity* impacts each of these areas and then proposes *Trust*, *Problem Solving*, and *Device Hierarchy*, respectively as potential solutions to each of these application areas (see Table 1). The issue of IoT Design Standards in general is then discussed. Finally, areas for future research are identified.

| **IoT root problem** | **Derivative IoT design challenges** | **SIoT concepts to address these challenges** |
|---|---|---|
| **Heterogeneity** | Security | Trust |
| | Reliability | Problem-solving |
| | Control | Device hierarchy |

**Table 1. IoT Architectural Design Challenges**

## *SIoT as a model for addressing IoT Security*

Architectural heterogeneity has proven to have an adverse effect on IT security. As IoT devices begin to integrate with each other in more complex ways, a common problem is how to secure communication between devices. While many methods are used, these may be considered to be substandard and not up to the task given a number of recent serious IoT security breaches (Greene 2016; Zetter 2015; Zetter 2016). In the current online world, most security relies on personal authentication. But often this will not work in the IoT world where devices inter-connect with little to no human involvement.

In the social world, security validation is done through reference and experience. Two people unknown to each other with no experience of each other upon which to base their interactions can establish a working relationship based on the knowledge of a common third party. A foundational construct for most business interactions, whole social websites such has LinkedIn have been built on the concept of the referral. This social referral method practiced in society for ***Trust*** can be applied to IoT to improve security.

## *SIoT as a model for addressing IoT Reliability*

Another impact of architectural heterogeneity is on reliability. Heterogeneity, in combination with the sheer volume of IoT devices which by some estimates will be 25 Billion by 2020, makes the reliable integration of *Things* difficult (Moran 2016). One way to effectively address this volume of devices, and the resultant volume of data and transactions is through a distributed architecture where routine problems

can be resolved at a local level without human involvement. Voutyras et al. (2014 make the argument for a distributed architecture in their paper on Social IoT. Automated ***Problem Solving*** using distributed computing through devices working together will help to improve overall system reliability. Again *Social IoT* provides a construct for how this problem solving would work as we observe what makes a successful problem solving team in the human world.

### *SIoT as a model for addressing IoT Control*

Managing the vast range of *Things* present in the IoT ecosystem can be a challenge. Atzori et al. (2011 characterised several components of an SIoT model which could be used to facilitate device control. These components or services allowed IoT devices to interact in useful ways similar to the way people interact based on standard written and unwritten rules of engagement. One of the components of the proposed model is *Object Profiling*. This refers to the way objects maintain static and dynamic information about themselves that can be provided to other devices on demand. Another component or service is *Owner Control* which allows the owner the ability to limit how the device is used. Other components in the model include a *Relationship Management* service which allows governance on what other nodes in a network a device could be connected to and *Service Discovery* service which is the device providing response to standard inquires and which allows devices to seek useful connections with other devices. Building on these services, a standard SIoT Architectural ***Device Hierarchy*** of device or *Thing* roles and responsibilities would be beneficial in designing IoT networks.

## SIoT and IoT Security

### *The use of Trust Models in IoT Security*

The security of IoT applications has been an area of keen focus in the last number of years, highlighted most recently by the significant DDoS (Distributed Denial of Service) attack launched in the USA late in 2016 using IoT based botnets (Greene 2016; Smith 2016). That attack attracted significant global attention including in investigation by the US Department of Homeland Defense. The traditional authentication based security control method typically used in IT proved completely inadequate in this case. Traditional IT security relies on human intervention through user authentication as a prime method to establish a trusted relationship between devices for security purposes. But in IoT there is often no human interaction with connections often being spontaneous, which presents a problem (Hung et al. 2016). How does one device connect to another safely with no human interaction? It becomes clear that establishing a trust mechanism between objects much like the way that people establish trust with each other is a potential way to improve IoT security as this model does not rely on the traditional authentication base model nor human interaction. Several Trust Models have been built based on SIoT concepts in an effort to improve IoT security (Yan et al. 2014). Many authors have written about the challenges in IoT Security (Zhang et al. 2014). Aside from providing a critical evaluation of these works, this article presents another trust model based on SIoT concepts which has certain advantages over the models presented in the literature.

### *Trust Models in the Literature*

Yan et al. (2014 divide IoT trust into two types of trust: data collection and process trust. The importance of having trust in the data collected by an IoT device is illustrated in Gartner's estimates that the black market in fake IoT sensor data will be a $5 Billion USD by 2020 (Friedman et al. 2015). Process trust is also important and has implications for the privacy and efficacy of the automated decisions taken on IoT data. It can also have an impact on public safety if one considers such applications as IoT in vehicles, Smart Cities traffic control or general industrial IoT applications. Therefore, any trust model needs to address process trust and data collection trust.

Key concepts in the development of trust models include *Transitivity*, which is the concept of a recommendation from someone that is not directly known, *Composability* which is calculating trust based on the recommendation of friends and *Personalisation* which is the concept that different people can trust the same person at different levels (Nitti et al. 2014). It is also important to note that Trust is Asymmetric and that two people may have different views of how much they trust each other.

Methods to establish trust can be divided into the categories of Subjective Trustworthiness and Objective Trustworthiness (Atzori et al. 2014). With Subjective Trustworthiness, each node in a network computes the trustworthiness of the nodes it interacts with based on its own experience and other nodes experiences. With Objective Trustworthiness, the trustworthiness information about each node is distributed and stored using Distributed Hash Tables. The information is visible to every node but is only managed by special nodes called Pre-Trusted Objects. Nitti et al. (2014 in their work demonstrated that methods based on Subjective Trustworthiness were generally more effective.

In establishing Trust in a network, social network theory needs to be considered. In characterising a social network of people or objects some people or network nodes can be more important or influential than others to the relationships formed. What it means to be important depends on the context but can include access to information and the frequency of transactions through node. One concept regularly used as descriptors for network management is Centrality. The concept of Centrality was first described by Freeman (1978 in his heavily cited paper. Centrality provides a way to quantify the different ways a node in a network (or a person in a social network) can be important. Within the concept of Centrality there is Degree Centrality which implies that the node with the most connections is the most important. Alternatively, there is Closeness Centrality which implies that the node in the middle is the most important. Also, there is Betweeness Centrality which implies that the nodes with the most transactions are important. Finally, there is Eigenvector Centrality which infers that the most important node is the node connected to the most number of important nodes. Overall, centralisation tells us how influence is spread across a network. The key takeaway is that the concept of Centrality needs to be considered when using SIoT methods to build IoT Architectures.

Finally, when developing an IoT architecture it is generally agreed that IoT can be broken down into the three conceptual layers of software/ hardware combinations which perform specific functions (Atzori et al. 2012; Gubbi et al. 2013; Yan et al. 2014). The layer that consists of components that interact with the environment such as sensors or actuators is often referred to as the *Perceptual Layer*. There is then a *Network Layer* which includes the technology to communicate data between devices. Finally there is an *Application or Presentation Layer* which presents and/or manages the data and provides the process management. Each device or node on the internet has an architecture then which must consist of these three layers in various forms. To establish trust between Things in an IoT network one cannot focus just on the network layer but also has to look at the application layer and the perception layer of the IoT Architecture in their design (Yan et al. 2014). There has to be agreement on the data being collected, the communication of that data between devices and the actions that result from the applications built into those devices.

## *SIoT as a Solution to Trust Models in IoT Security*

For a security solution to be practical in the current IoT environment it needs to be cost-effective and recognise the limitations of compute power and memory that many IoT devices have. In the consumer space, it needs to recognise the limited skill sets of the average user. For example, many recent attacks have taken advantage of the fact that users never changed their device passwords from those set in the factory. Ideally any solution presented will also ensure that incentives are built into it for participants to proactively support the system (Guo et al. (2012.

Much of the discussion so far has been around the concept of "Trust" with the view that IoT devices will develop and maintain connections with other devices based on some form of established trust. The challenge with the Trust models in the literature is that they do not fully address this problem. Highly effective models are proposed to calculate a trust score aggregating previous experiences (Capra and Musolesi 2006) or the experiences of others through the use of constructed mathematical models which filter and weight pre-determined trust assessments (Nitti et al. 2014). However these models do not provide a method for calculating each individual node's initial trust score and they may generate significant computational workloads given the mathematics used. In other words, how do you determine what is a nodes initial trust value when history isn't sufficiently established and there are an insufficient number of nodes that the new node has connected to in order to establish an initial pattern? Also how does a simple device with limited computation capabilities calculate a trust score? Possibly this is due to the presumption that a trust scoring mechanism needs to be specific to the use case. If it were possible to

have a trust scoring mechanism that was universal and independent of the type of thing being considered this will fill a gap in the current literature as well. Also a trust scoring system which was mathematically simpler will have computational and resource advantages.

The following is that proposed mechanism. Using one of the commonly used unique identifiers (such as MAC Address), devices would be able to request a simple trust score from other devices on the network. Trust scores from devices of similar architecture would have higher weighting as their experience would be perceived to be more relevant as would those devices identified as would devices with a *Parental*, *Co-work* or *Co-locational relationship*. New devices could inherit initial trust scores from devices identified as having a *Parental* relationship. The lowest available weighted trust score reported from those devices contacted would be the one used to evaluate whether the connection from the new device would be accepted. The preceding logic is illustrated in the following mathematical model:

$$T_n = \min\left\{T_{np}, min\{T_{n1}, \dots, T_{nj}\}, w * min\{T_{nj+1}, \dots, T_{nk}\}\right\}$$

$T_n$ = Trust value of node n; $T_{np}$ = Trust of the parent node for n; $T_{n1}$ = Trust score evaluation returned from adjacent node 1 for node n; W = weight assigned to adjacent nodes with the same device code

In this model *Trust Scores* would improve over time as a device or its parent establish more connections and thereby generate more reference nodes. The model proposed would be a subjective model in that each of the Things would be responsible for calculating its own trust scores. Centrality would be addressed by collecting as many scores as possible. Cost and simplicity are achieved in that each device is only responsible for storing the calculated trust scores for the networked devices it is connected with, storing its own unique identifier, and storing a universal identifier for the category of device it was. A simple protocol would be required for each device to request and receive the trust scores from other devices for a unique device identifier. No significant computational power is required for the calculation and so even simple devices could use this method. The term *Social Referral Method* is used as the methodology replicates human behaviour in terms of establishing trust between two new participants in a relationship. Below is a comparison of the various SIoT based Trust Methods including the proposed *Social Referral Method*:

| **Attribute** | **Capra and Musolesi (2006** | **Carminati et al. (2012** | **Nitti et al. (2014** | **Social Referral Model(2017)** |
|---|---|---|---|---|
| Provides a universal model for the initial Trust Value to be calculated | No | No | No | Yes |
| Incorporates Historical Trust Assessment | Yes | Yes | No | Yes |
| Incorporates a Peer Trust Assessment | No | No | Yes | Yes |
| Subjective vs. Objective Trust Model | Subjective | Subjective | Both | Subjective |
| Provides a Universal Model | No | No | Yes | Yes |
| Autonomic Model (Trust Calculation without User Intervention) | Yes | Yes | Yes | Yes |
| Light Weight (does not require significant local resource) | No | No | No | Yes |
| Domain Homophily (recognises the importance of similar devices) | Yes | No | No | Yes |
| Addresses the issue of Centrality | No | No | Yes | Yes |

**Table 2. Comparison of the various Trust Calculation Models**

# SIoT and IoT Reliability

## *Reliability and the need for Device Problem Solving*

A device is reliable when it performs its required function in its specified environment consistently over a period of time. Reliability in IoT is critical. In Agricultural IoT many of the Things will be located in remote locations where access is difficult. In Industrial IoT the Things will likely be subjected to adverse environmental conditions yet involved in the control of dangerous manufacturing processes. Medical IoT devices could potentially be critical for life support. It is clear then that an architecture that supports reliability is a necessary component of the IoT. Devices that are resilient and tolerant of faults in the network of other devices will support reliability. Device Problem Solving will be key to IoT Reliability.

## *Problem Solving in the Social Realm*

Studies show that problem solving in groups of two or more people can provide a better solution to a problem (Bahrami et al. 2010). The participants in a group decision need the ability to effectively share information with each other and to be able to test that information for its reliability or consistency across multiple data sources. Detailed and timely feedback about the accuracy of the decisions subsequently taken and the accuracy of the other participant's decision making is also important. But most important is the ability for one party to communicate their confidence in the proposed decision to the other party. Successful collaboration relies on the participant's ability to accurately estimate and report their own ability to solve a problem accurately (Bahrami et al. 2010). People's tendency to overestimate their own abilities is referred to as the Dunning-Kruger effect (Kruger and Dunning 1999). These concepts around group problem solving can be taken into effect when developing problem solving models involving multiple "Things" of an IoT network.

## *Device Self-management and Intelligent Problem Solving within SIoT*

As previously noted, problem solving can be enhanced when more than one person are working together to solve a problem. However there are a number of pre-requisites to how communication occurs between those people for them to work together effectively. The parties need to have a clear view of both the information accuracy and the historical decision accuracy of the other party. It is therefore reasonable to assume that devices working together meeting those same prerequisites should be able to achieve a more optimal solution faster, thereby improving overall network reliability.

As an illustration, some examples of intelligent problem solving cited by Atzori et al. (2012) in their constructed vision of SIoT problem solving, included one PC communicating with other PCs that have similar user profiles to identify best practices in terms of configuration, one house with controllers and sensors establishing an energy usage profile that then seeks out houses in the local area with similar profiles to identify suitable energy providers, and finally one car experiencing poor fuel performance developing a sensor profile then seeking out other cars with similar profiles to establish what the problem might be.

Some applied work has been done already around the development of problem solving within the IoT paradigm. Foteinos et al. (2013 achieve a level of reliability and device self-healing by creating an abstraction layer in an IoT control system with virtual objects and composite virtual objects. Testing demonstrated an optimal level of abstraction in terms of how the virtual objects and composite virtual objects were constructed. But as a platform as a service the solution was not universal.

The proposal here is to build a universal logic into IoT devices such that simple information about issues experienced, the impact, the resolution to the issue (if realised) and the quality of the resolution are tracked. This information would then be made available on a simple request/ response process through some form of web service type call such that other devices/ things in the network could make use of it. Devices with more computing power capabilities that could make use of the information could then use it to identify and communicate potential solutions to other similar devices in the network.

To achieve this model requires two things. First, that all IoT devices maintain a limited storage capability which allows the device to be tagged with information relating to its history of issues, fixes, impact and so forth. Second, that some common Mark-up Language is established which will facilitate the request/response protocol required between devices. Precedents for this type of mark-up language exist with HTML (for websites), XML (for integration) and XBRL (for reporting). There could be an IoTML for IoT devices. If these common architectural components were applied to all the "Things" in IoT then this would facilitate the future development of distributed computing and problem solving which is a necessary requirement for the IoT to achieve scale.

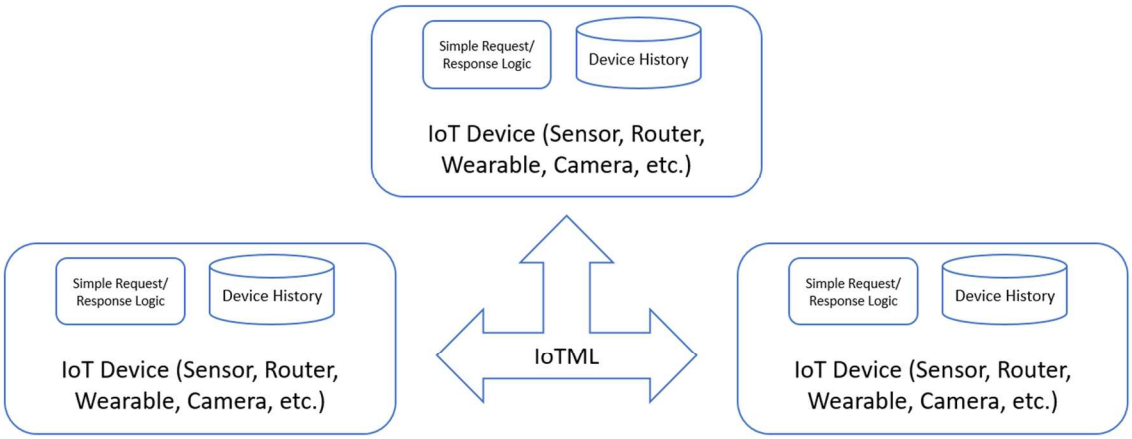


**Figure 2. IoT Problem Solving *Conceptual Diagram***

# SIoT and IoT Control

## *Social Behaviour Concepts and their Potential Application to IoT Control*

Conceptually social networks compare closely to IoT networks. Highly heterogeneous, often complex and with many constituents, social networks function based on a set of universal standards that, at their core, are based on the self-interest of the people involved with incentives to act in specific ways. It is argued that to operate effectively, IoT architecture should operate similarly. In this section the aspects of social behaviour that can be applied to IoT architectural design to form a basis for command and control are considered.

Fiske (1992 presented an approach for modelling people's social behaviour and how they work together by dividing social behaviour into four categories: authority ranking; equality matching; communal sharing; and market pricing. According to Friske, people act in one of only four distinct ways, sometimes concurrently. Fiske's model has been used by other authors on developing SIoT Architectures (Atzori et al. 2011; Atzori et al. 2012; Nitti et al. 2014).

The previous two architectural issues, Security and Reliability, follow a market pricing model and a communal sharing model respectively. For the area of IoT control the most appropriate social model is authority ranking. In Fiske's model, *Authority Ranking* is where those with higher ranking take most of the benefits but in return are responsible for the safety and security for those of lower rank.

The way devices or nodes consider one another in terms of a social relationship has been classified in one of 5 ways (Atzori et al. 2014; Atzori et al. 2012): First, *Parental* where the devices come from the same manufacture from the same period; second, *Co-locational* where the devices establish a relationship based on location; third, *Co-work* where the devices are components of one common solution; fourth, *Ownership* whereby devices establish a relationship based on a common human owner, and; fifth, *Social* where devices come into contact opportunistically due to proximity.

Finally as previously noted, Atzori et al. (2011) in his initial work on SIoT characterised several components of an SIoT sematic model which could be used to facilitate device control.

### *Control using a Standardised SIoT Architectural Device Hierarchy*

Previous works provide a method for communication regarding control in an IoT network and establish the types of relationships that can be expected in a social style IoT network (Atzori et al. 2014; Atzori et al. 2012). We extend these previous works by providing guidelines for how the various IoT devices would act in these roles and how they would respond to the various interactions. The context and the device relationship will determine how it will react.

Much like Fiske's model for Authority Ranking (Fiske 1992), those devices with a higher authority will be required to take responsibility for those devices with a lower authority both in terms of management but also in terms of providing capabilities for the successful functioning of the network as a whole. In this way this model recognises one critical aspect of most IoT networks. This is that many of the devices in the network do not have the capability or capacity to undertake all of the functions required to support the network.

Table 3 illustrates one possible set of guidelines as to the various roles within an IoT network based on SIoT principals. Part of this process will be for the newly installed device to establish the relationship type with all the devices it interacts with to determine what type of interaction is possible and how it will respond. If it cannot the relationship type will be deemed undefined.

| | **Co-locational, Co-Work, or Social Relationship** | | | | **Ownership Relationship** | **Undefined Relationship** |
|---|---|---|---|---|---|---|
| | **Response to Object Profiling Service Inquiry** | **Response to Owner Control Service Inquiry** | **Response to Relationship Management Service Inquiry** | **Response to Service Discovery Service Inquiry** | **All Service Inquiries** | **All Service Inquiries** |
| **Parental (Managing Device)** | Provides a response for itself and the supporting devices. | Provides a response for itself and the supporting devices. | Only between itself, supporting devices or devices deemed as having an ownership relationship | Provides a response for itself and the supporting devices. | Provides a full response | Provides a full response |
| **Parental (Supporting Device)** | Provides a full response | Responds by providing information of the managing device | Only between itself, supporting devices or devices deemed as having an ownership relationship | Provides a full response | No response | No response |

**Table 3. Social IoT Role Hierarchy and Responsibility**

## SIoT and IoT Design Standards

This paper began with the premise that there was a need to reduce *Architectural Heterogeneity* to improve IoT Benefits Realisation. The way to reduce *Architectural Heterogeneity* was through the adoption of standards. The methods of the Social Internet of Things were presented as the best way of establishing IoT design standards under the premise that there are a lot of similarities between human networks and IoT networks and that there are benefits in designing the one to reflect the other. In this paper, contributions have been made to IoT Architectural Design in terms of security, reliability and control. A *Social Referral Trust Model* has been constructed which improves on some of the *Trust* models previously presented in the literature and can be used to improve security. A sematic framework based on the concepts of Mark-up Languages to facilitate *Problem Solving* and thereby *Reliability* has been presented. Finally the work of a number of authors around the issue of device *Control* is extended to produce a Hierarchy defining device roles and responsibilities.

| IoT root problem | Derivative IoT design challenges | SIoT concepts to address challenges | Methods to apply SIoT concepts |
|---|---|---|---|
| **Heterogeneity** | Security | Trust | Social Referral Trust Method |
| | Reliability | Problem-solving | IoTML Semantic Framework |
| | Control | Device hierarchy | Device Roles |

**Table 4. Extension of the current SIoT Model**

## Conclusions, Next Steps and Future Research

Architectural Heterogeneity represents a significant barrier to the uptake of the Internet of Things. SIoT as a concept represents one solution to this issue of Architectural Heterogeneity. This was demonstrated by the three examples illustrated in this paper. But there are other methods that can be used. Regardless of the specific path taken, the adoption and enforcement of standards remains the surest way to reduce Architectural Heterogeneity and to improve IoT benefits realisation.

All of this makes the case for government/ regulatory intervention into the IoT space. For those that argue that natural market mechanisms should be left to address these issues, it is important to point out that these mechanisms only work when there is an educated buyer. Currently, the average buyer is ill-equipped to make these heavily technical decisions. Even for large corporations with a multitude of experts at their disposal the technology is so new and moving so quickly it would still prove challenging. An analogy can be drawn between IoT and the health care industry where one person's negligence can harm a number of people and therefore necessitates standards and regulation. The analogy is even more salient when one considers that health care is one of the faster industries to adopt IoT due to patient benefits. According to Soroush et al. (2016) the current IoT standards are simply not sufficient to meet the needs of the health care industry.

Taken in this context, future research into the issues that prevent the uptake of design standards within the IoT arena and that would facilitate standards enforcement needs to be completed. There is the opportunity to consolidate all the academic IoT architectural works into one unified model which would facilitate adoption. The practical application of those IoT architectural models to industry should also be considered. Finally, the potential for incentives that use market forces to drive standardisation in addition to market regulation also deserves further analysis.

## References

Alam, K. M., Saini, M., and El Saddik, A. 2015. "Toward Social Internet of Vehicles: Concept, Architecture, and Applications," *IEEE Access* (3), pp. 343-357.

Ashton, K. 2009. "That 'Internet of Things' Thing," *RFiD Journal* (22:7), pp. 97-114.

Atzori, L., Carboni, D., and Iera, A. 2014. "Smart Things in the Social Loop: Paradigms, Technologies, and Potentials," *Ad Hoc Networks* (18), pp. 121-132.

Atzori, L., Iera, A., and Morabito, G. 2011. "Siot: Giving a Social Structure to the Internet of Things," *IEEE communications letters* (15:11), pp. 1193-1195.

Atzori, L., Iera, A., Morabito, G., and Nitti, M. 2012. "The Social Internet of Things (Siot)–When Social Networks Meet the Internet of Things: Concept, Architecture and Network Characterization," *Computer Networks* (56:16), pp. 3594-3608.

Bahrami, B., Olsen, K., Latham, P. E., Roepstorff, A., Rees, G., and Frith, C. D. 2010. "Optimally Interacting Minds," *Science* (329:5995), pp. 1081-1085.

Capra, L., and Musolesi, M. 2006. "Autonomic Trust Prediction for Pervasive Systems," *20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06)*: IEEE, p. 5 pp.

Carminati, B., Ferrari, E., and Viviani, M. 2012. "A Multi-Dimensional and Event-Based Model for Trust Computation in the Social Web," in *Social Informatics: 4th International Conference, Socinfo 2012, Lausanne, Switzerland, December 5-7, 2012. Proceedings,* K. Aberer, A. Flache, W. Jager, L. Liu, J. Tang and C. Guéret (eds.). Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 323-336.

Fiske, A. P. 1992. "The Four Elementary Forms of Sociality: Framework for a Unified Theory of Social Relations," *Psychological review* (99:4), p. 689.

Foteinos, V., Kelaidonis, D., Poulios, G., Vlacheas, P., Stavroulaki, V., and Demestichas, P. 2013. "Cognitive Management for the Internet of Things: A Framework for Enabling Autonomous Applications," *IEEE Vehicular Technology Magazine* (8:4), pp. 90-99.

Freeman, L. C. 1978. "Centrality in Social Networks Conceptual Clarification," *Social networks* (1:3), pp. 215-239.

Friedman, T., Perkins, E., Velosa, A., Schulte, W. R., and Steenstrup, K. 2015. "Gartner Predicts 2016: Unexpected Implications Arising from the Internet of Things," *Gartner Research*).

Greene, T. 2016. "Largest Ddos Attack Ever Delivered by Botnet of Hijacked Iot Devices." *Network World*, from http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. 2013. "Internet of Things (Iot): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems* (29:7), pp. 1645-1660.

Guo, B., Yu, Z., Zhou, X., and Zhang, D. 2012. "Opportunistic Iot: Exploring the Social Side of the Internet of Things," *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on*: IEEE, pp. 925-929.

Hung, M., Singh, A., and Mahdi, D. 2016. "Hardware Security and Its Impact on Iot" *Gartner Research*.

Kruger, J., and Dunning, D. 1999. "Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments," *Journal of personality and social psychology* (77:6), p. 1121.

Lheureaux, B., Pezzini, M., and Velosa, A. 2016. "Market Guide for Iot Integration," *Gartner Research*.

Lheureux, B. J., Reeves, D., Perkins, E., Natis, Y., Steenstrup, K., and Kutnick, D. 2015. "Gartner Predicts 2016: Rising to the Challenge of Building Iot Solutions," *Gartner Research*.

Moran, M. P. 2016. "Why the Internet of Things Will Dwarf Social," *Gartner Research*.

Ning, H., Liu, H., and Yang, L. T. 2013. "Cyberentity Security in the Internet of Things," *Computer*:4), p. 46.

Nitti, M., Girau, R., and Atzori, L. 2014. "Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on knowledge and data engineering* (26:5), pp. 1253-1266.

Sarkar, C., Nambi, S. A. U., Prasad, R. V., and Rahim, A. 2014. "A Scalable Distributed Architecture Towards Unifying Iot Applications," *Internet of Things, 2014 IEEE World Forum on*: IEEE, pp. 508-513.

Smith. 2016. "Iot Botnets Used in Unprecedented Ddos against Dyn Dns; Fbi, Dhs Investigating." Retrieved 30 Oct 2016, 2016, from http://www.networkworld.com/article/3134093/security/iot-botnets-used-in-unprecedented-ddos-against-dyn-dns-fbi-dhs-investigating.html

Soroush, H., Arney, D., and Goldman, J. 2016. "Toward a Safe and Secure Medical Internet of Things,").

Velosa, A., Natis, Y. V., Pezzini, M., Lheureux, B. J., and Goodness, E. 2015. "Market Guide for Iot Platforms," *Gartner Research*).

Voutyras, O., Bourelos, P., Kyriazis, D., and Varvarigou, T. 2014. "An Architecture Supporting Knowledge Flow in Social Internet of Things Systems," *2014 IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 100-105.

Xiaohui, X. 2013. "Study on Security Problems and Key Technologies of the Internet of Things," *Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on*: IEEE, pp. 407-410.

Yan, Z., Zhang, P., and Vasilakos, A. V. 2014. "A Survey on Trust Management for Internet of Things," *Journal of Network and Computer Applications* (42), pp. 120-134.

Zetter, K. 2015. "A Cyberattack Has Caused Physical Damage for the Second Time Ever," *Wired*).

Zetter, K. 2016. "Inside the Cunning, Unprecedented Attack of the Ukraine's Power Grid," in: *Wired*

Zhang, C., Cheng, C., and Ji, Y. 2012. "Architecture Design for Social Web of Things," in: *Proceedings of the 1st International Workshop on Context Discovery and Data Mining*. Beijing, China: ACM, pp. 1-7.

Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., and Shieh, S. 2014. "Iot Security: Ongoing Challenges and Research Opportunities," *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*: IEEE, pp. 230-234.