# Towards a Context-aware and Adaptable Room System for Intelligent "Trusted" Office-spaces in Smart Cities

Tim French[1] and Nik Bessis[2,1]

[1]Department of Computer Science and Technology, University of Bedfordshire, United Kingdom
[2]School of Computing & Mathematics, University of Derby, United Kingdom
[1]tim.french@beds.ac.uk [2]n.bessis@derby.ac.uk

*Abstract*— **This visionary paper outlines a future intelligent building office space room system that seeks to ensure that the users of a rentable and/or shared office space do not perform actions that are likely to compromise IT security. We propose that a novel room agent leverages the emergent "smart" city paradigm so as to form an accurate a measure as possible of the trustworthiness of the human agents using the office space. Namely, by leveraging pervasive urban sensors embedded in a smart city built environment, data obtained by crowd sourcing as well as data gathered via Web 2.0. Human actions detected within the room itself and its immediate environs, together with the behavioural traces and patterns of a given individual embedded within a smart city context, can be used to calculate a measurable confidence trust level. We suggest that the use of a Linking Open (or object) Data (LOD) publishing approach can be used to integrate trust related distributed data in a collective and intelligent manner. Furthermore, we suggest the use of cloud diagram and tree map visualisation approaches to depict individual and environs trust levels at both coarse and fine grain levels. To achieve this, we illustrate the approach using a low-level architecture model. We then conclude by outlining our theoretical lightweight trust model which aims to demonstrate how a smart city in general and a smart space in particular can provide an increased level of trust visualisation for it's citizens, through collective intelligence gathering.**

***Keywords: Multi-agents; Content-aware trust; Smart spaces; Internet of Things; Linking open (object) data; Network analysis; Cloud diagram; Tree map.***

## I INTRODUCTION

Considerable work has already been undertaken in the area of MAS (Multi Agent Systems) with respect to the design and pilot implementation of various intelligent buildings room agents. These agents are typically designed so as to facilitate adaptive control of ambient room temperatures and similar environmental activities [1]. Furthermore, the semiotic paradigm has been invoked as a suitably sensitive and subtle means of both modeling MAS for intelligent buildings and also potentially enabling these agents to communicate between themselves and interact with human agents so as to optimize their activities [2].

However, relatively little attention thus far has been paid to the design of passive room agents that can "police" re-configurable work spaces with respect to intangible trust and tangible security. Nor have previous approaches sought to interrelate data traces that relate to individuals as they navigate through smart city "spaces" as well as on line Web 2.0 spaces to the actions of a given human agent within an intelligent room context. We believe that it is necessary to relate real-time actions of a human agent in a room to the past actions of a given individual, for example behavioural patterns, Web 2.0 activities as well as any known past incidents that may better inform our self-confidence that an individual, hence actions/intentions are "trustworthy".

This paper also seeks to leverage the semiotic paradigm by means of a novel trust ladder, as well a novel model of mimicry derived from biological and sociological models. Developing a firm theoretical foundation for the design of the room agent, grounded within the field of Organisational Semiotics will potentially enable the room agent – as well as its collectively extended application to a smart city – to respond in an adaptive / even predictive manner to the activities of its human occupants. In so doing, the risks associated with the commercial leverage of such spaces will be minimized. A case study and simplified scenario is later presented that seeks to clarify some of the complexities involved and is designed to show the potential "added value" of a semiotically enabled room agent.

On the other hand, Internet of Things (IoT) is becoming an emerging paradigm shaping our current understanding about the future of the Internet. There are several works highlighting notable challenges for creating a framework to enable inter-operability between resources (or objects) as part of an enlarged future enterprise. Within this context, the purposefully sharing and exchanging of large (tera / petra byte sized) distributed – trust related – data sets serves to highlight the urgent need for the adoption use of a linking open (or object) data (LOD) visualisation approach.

That is, the data sets typically gathered in smart city decision support contexts (such as predictive "crime" scenarios) [3], have reached a size and degree of complexity such the human mind cannot interpret intelligently without powerful computer tools. In particular, linked data concentrates on publishing data on the web and interlinking them to seek other "related" information [4]. Thus, LOD could be used as a visualisation "bridge" to integrate trust related data gathered by different organisations and individuals using a static or dynamic cloud diagrammatic approach. The latter visualisation method has been successfully developed by [5]. Herein, we suggest the use of a cloud diagram approach as to illustrate individual and environs trust levels via a LOD approach at both a coarse and fine grain

978-0-7695-4684-1/12 $26.00 © 2012 IEEE
DOI 10.1109/IMIS.2012.62

level of detail. This will enable us in model trust levels dynamically for both individual and space (e.g. “room”) environments within intelligent buildings.

The paper is structured as follows. In section II, a review of the relevant MAS room agent literature is presented, with particular reference to previous use of the semiotic paradigm. This is followed by an explication of a novel trust sign and mimicry conceptual model (in Section III). Next, we describe the technicalities and opportunities available for meeting the challenge. In particular, section V describes the applicability of IoT within the context of depicting trust levels by utilising a cloud diagram visualisation approach. This section presents a low-level conceptual architecture model. In section VI, a case is presented that seeks illustrate how such an agent might operate in practice; that is, we describe our multi-client lightweight trust model and its suggested variables. Finally, in section VII we conclude by highlighting the need for simulating our proposed multi-client lightweight trust model in smart settings.

## II Intelligent Buildings – The Need for Adaptive Trust Agents

The development of software agents for intelligent building control requires an inherently interdisciplinary approach. The central idea is that an intelligent building can autonomously manage the environment with specific reference to such concerns as: adapting a space to client user needs via reconfigurable spaces [6]; environmental adaptation to meet the comfort levels of users, via lighting and heating optimization and automated environmental monitoring. Often preferences are selected according to pre-defined criteria rather than learned from experience. The ability of an agent to learn via feedback captured from users and via unsupervised observation of occupant's behaviours has the advantage of non-intrusiveness. This has many advantages, but clearly the ability to respond to individual user preferences is limited. One of the difficulties has been the need to orchestrate intelligent building's “middleware” so as to offer a fully co-ordinated computational approach to “intelligence”. Recent advances in web-services may solve this elusive goal [7].

We propose a novel approach to the measurement of trust (i.e. trust defined as a measurable confidence level) through reference to data at three temporal and conceptual levels. These together are used to calculate TL (Trust Level) which at any given moment is updated and compared to a given threshold level that has been deemed to represent an acceptable “risk” in relation to the usage of a room. Hence, the actions of a given human agent or set of agents.

This TL level can be used for example to disable equipment (if the risk is high and trust is below the threshold) or to trigger the generation of real-time “logs” (gather evidence) in relation to a suspected incident or when a predicted incident is deemed highly probable, based on the intent of a human agent to commit an act likely to compromise the IT systems embedded within the office space.

The overall intention is to relate immediate actions to past actions (or inferred actions) as follows so as to mitigate the risk of allowing human agents to use shared IT systems a follows:

**TL** (a value denoting a scaled, and suitably weighted measurable confidence level between -1, 0, +1) = T(a) + T(b) + T(c) where:

**T(a)** = Data gathered by pervasive computing devices (an internet of things) embedded in a smart city built environment that relates to a given individual's usage of devices, patterns of behaviour, known web of trust associates. Public domain data concerning past criminal activities or on-line Web 2.0 social-network activities. Time period is typically measured in days, weeks, months (+).

**T(b)** = Near-real time data that situates the human agent within the building itself, identified presence of devices such as USB's, laptops and seeks to identify non-normative behavioural patterns. Time period should be less that a 1 hour.

**T(c)** = Real-time data gathered by the room agent that relates to immediate activities and actions of a human agent (e.g. connecting a USB to a workstation). Time period measured in minutes and seconds.

The vision is that when aggregated together the initial TL level (which will be notionally set to 0 if no data is available for a given individual) will be continuously updated via T(b) and T(c) so as to provide a real-time measure of confidence that a human agent should or should not be trusted. Thus, a truly intelligent room needs to be interrelated to its embedding within a smart city environment wherein continuous data is being gathered both passively via RFIDs, sensors and actively via participation in urban crowd sourcing, as well as informed by past-logs of Web 2.0 activities and on line shopping activities (i.e. harvesting data that relates to a person's devices, IP addresses and multiple identities).

As smart cities evolve and mature, more and more data will become available to the room agent. For example through participation in urban environmental citizen science it will be possible to reverse engineer a person's past behavioural / work/ leisure patterns from uploaded data. Indeed this has already become a reality in fields such as predictive “policing” in the USA, wherein crime mapping is now commonplace [3].

Similarly, previous on-line activities leave traces, which are able to identify devices used, sites visited and build a profile that relates to their trustworthiness. Naturally public domain data such as past criminal activities, credit history ratings (etc.) can also be leveraged, as can social-networks. By integrating all of these data sets it will be possible to assign an initial trust rating to a given individual. This is to update in near-real time by the room agent itself via T(b) and T(a) so as to generate a measurable confidence level in the range[ -1, 0, +1]. Depending on the “risk appetite” it is possible to use this value to trigger countermeasures or increase or decrease the level of active monitoring needed as the room is used.

## III Trust Signs, Trust Ladder and Mimicry: Conceptual Model and Scenario

Previously a generic trust ladder has been elaborated [8] that seeks to identify trust operating at various levels of abstraction. Namely the generic levels are identified below in Table 1.

| |
|---|
| SOCIAL WORLD<br>Trust beliefs and expectations, norms |
| PRAGMATICS<br>Goals, intentions, trusted communications |
| SEMANTICS<br>Meanings, mimicry-deception, truth, falsehood |
| SYNTACTICS<br>Formalisms, trust policies, controls |
| ENTROPY<br>Crypto, channel capacity, machine level |

*Table 1: A Generic e-Trust Ladder*

The trust ladder currently functions as a *meta-model*, within system designers and their clients can conceptualize e-trust is-sues, from its earliest inception to design and implementation. Each level in the ladder (social, pragmatic, syntactic etc.) reflects the normative manner in which signs and their meanings are considered by the Organisational Semiotics community. That is, issues at the three upper layers (social world, pragmatics and semantics) are intended to focus developers upon signs, meanings and intentions within Information Systems. The two lower levels (syntactics and empirics) are concerned with how signs are structured and transmitted. It is perfectly feasible for the layers given in our trust ladder to be further sub-divided into sub-layers. The levels as currently indicated represent a convenient way in which e-trust signs and their (human) interpreters can be conceptualized. Clearly the levels are interrelated, the main distinction being that at the upper three levels interpretation (known as *semiosis*) is immediate, whereas at the lower levels that involve machine to machine signal exchange, that interpretation is often deferred.

A fundamental issue of concern at all levels of the ladder is that of mimicry and deception. Essentially the problem is how an agent can detect with accuracy a deceptive signal emitted from a human subject or technical mediator (or both) and to distinguish these signals which are typically low cost to emit by adversaries, from genuine signals. We return to this aspect in the next section, but merely state at this point the rather obvious fact that unless the system is capable of distinguishing between genuine and fake signals of trust, the system will be vulnerable to exploits, including active attacks by human agents seeking to compromise the building's IT systems and security systems. That is, the room agent unless optimally configured may actually become a portal for an adversary (through mimicry), rather than aiding in the detection of an adversary.

So as to relate this high level conceptual model more specifically to the needs of an actual intelligent building specification an imaginary scenario is presented below together with some exemplar scenarios. These form the basis of a more detailed discussion in relation to enabling the room agent(s) with a suitably powerful ability to reason on several different conceptual levels of the ladder, hence respond to specific combinations of activities detected at the social, pragmatic, syntactic and empiric levels of abstraction. Indeed the challenge is how best to enable the trust agent(s) to combine inputs detected via sensors and RFIDs enabled devices and hence to respond in an appropriate manner to these activities. That is, to combine inputs and to calculate a measurable confidence level. From this level responses can be generated according to the risk appetite of the room operator and their clients.

## IV Human Agent Trust Scenarios: Basepoint Meeting Space

Basepoint is a newly constructed intelligent building that amongst other things provides the facility for local SME's (Small and Medium Enterprises) to hire re-configurable IT (Information Technology) enabled meeting spaces on an hourly basis. Typically SME's pay an hourly fee and use the spaces for meetings, presentations and brain storming sessions. The spaces are enabled with WiFi, have standard PC's with Windows applications and Internet access.

The following exemplar user scenarios are intended to illustrate that the intelligent agent needs to detect, hence assess the trustworthiness (risk) associated with user activities operating at the social, pragmatic as well as empiric (tangible security) levels of abstraction.

**Scenario A**

A client enters the room by using a biometrically enabled smart card. After logging on to one of the room's PC's using a time-delimited text based password they proceed to connect their USB via the built-in USB port. Upon connecting the USB unbeknown to the user the USB infects the PC (hence local area network) with malware. The user proceeds to upload a Powerpoint file in preparation for a meeting with a client.

***Smart enabled Scenario A:***

A client enters the room by using a biometrically enabled smart card. Single biometric identity is resolved into multiple previous/ current Web 2.0 on-line identities. Weightings are applied accordingly. Room-agent leverages smart city data and known device usage, Internet activities to calculate initial TL of human agent [0.4]. This level indicates that this agent whilst not deemed to be actually malevolent needs to be given restricted access to devices. (Previously the agent's smart phone was infected by a virus detected whilst uploading crowd-source db level data in their job as a cycle courier). Agent attempts to connect USB. This has been disabled by room-agent. Human agent is advised that access has been limited until all their devices are screened for malware. Once screened using a high-level scan, access is re-enabled. TL is updated to [0.5]. The user proceeds to upload a Powerpoint file in preparation for a meeting with a client.

**Scenario B**

A client enters the room using their smart card. They notice that a USB has been left by a previous client. They pick this up and connect this to one of the PC's in the room. Having viewed the confidential data on their laptop they up-load the data to their web e-mail account and hand back the mislaid device into reception upon leaving the room.

***Smart enabled Scenario B:***

Client enters the room. TL is initially calculated as [-0.6], as this person has multiple Web 2.0 identities, chat-room activities etc. Room agent detects human action and detects USB ownership mismatch. Room-agent detects attempt to upload data and disables WiFi connection. Upon exit, the room agent invokes security staff who clean off the data from the laptop and actively ensure the USB is returned to the owner. TL is updated to [-0.8] thus in future the human agent will be denied access to this facility.

## V MEETING THE CHALLENGE

The design analysis and deployment of an intelligent room agent that learns from experience is generally referred as "third level" intelligent buildings design that is in reality still in its infancy [9]. Clearly the complete specification of such an advanced room agent lies outside the scope of this paper. Having said that, this section will offer an overview of possible technologies including Internet of Things (IoT), Linked Data, Cloud Diagrams and tree map visualisation techniques, which could enable the development of a *trust-aware* and adaptable smart room agent.

IoT is becoming an emerging paradigm shaping our current understanding about the future of the Internet. Its importance is described in terms of providing a different lens on how to link data and hardware resources as well as services that can be available from the Internet; these further focus on how to link the Internet with real world's objects. As such the IoT paradigm postulates that any object that is identified with a unique identifier will be considered as a smart object able to be interconnected. Those objects can be transformed in ways that they can be understood better by reacting to and with their environment in a more advanced and meaningful manner.

IoT has also been described as a paradigm that mainly integrates and enables several technologies and communication solutions including but not limited to tracking and localisation technologies, wired, wireless sensors, their networks, exchanged networked communication which in turn, lead to a shared next generation Internet (see [10]). IoT has been defined as ''a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols." In a more comprehensive way, it has been perceived as a paradigm that connects the real world with the digital world [11].

Although a very promising area, there are as yet divergent visions associated with the future paths of IoT paradigm. There have been several proposals for IoT applications especially, as a visionary way to transform current business world as well as to augment the impact on our everyday lives. The visions range from the remote consultation system accessing medical information and thus increasing service quality [12] to multimedia aggregators applied to interactive television program availability [13]. An early prototype is currently under development for mobile interactions within the IoT contexts [14]. There are several ongoing attempts to standardise protocols that if adopted, offer the prospect of a more fluent IoT data inter-exchanges [10]. In addition, there have been various challenges addressed which illuminate the potentials of IoT for practical applications. Those that have been described range from day-to-day needs solutions to high-level information for diagnostics, performance indicators, traceability and other purposes [15]. In turn, these highlight the potential of interconnecting individual's past activities and interactions as linked data objects that are available from a smart space environment.

Moreover, given that the IoT deals with complex systems that integrate multiple disperse components towards their synergetic use, it becomes crucial to identify relevant linking and integration techniques towards their leverage. With this in mind, several approaches could be utilised including but not limited to interlinking network of objects (or web of things) via linking analysis, social network analysis and linked open (object) data approach.

The benefits of a linking or social network analysis approach can be perceived on various levels. First, it provides a paradigmatic shift within current understanding of IoT [18]. From more pragmatic points of view, network analysis as a quantitative approach can deal with large-scale datasets and components [16]. Large-scale data points can be analysed through various levels of analysis – not only the object itself; the analysis also could include specific properties and attributes of the object. As a data-driven approach, from the data aggregation point of view it serves as a qualitative pattern immersion tool. Thus, network analysis could also offer a powerful way to make the patterns emerge from the data and thus to allow evaluating it in a quantitative manner. That is to say, by serving as a winning combination providing multi-lateral analysis of the data not only in their static state but also in dynamic ways.

Another candidate visualisation technique that could be used as to depict an individual's and/or room's online activity is the *tree map*. Specifically, a tree map [http://unaccustomed/hcil/treemap/] is a space-constrained visualisation of hierarchical structures. It is very effective in showing attributes of leaf nodes using size and colour coding. Tree maps enable analysts to compare nodes and sub-trees even at varying depth in the tree, and help them spot patterns and exceptions. Tree map was first designed by Shneiderman during the 1990s.

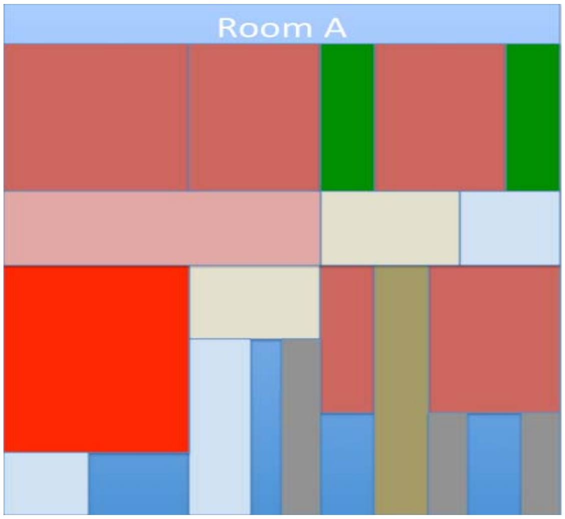

*Figure 1: An Imaginary Tree Map for a Smart Room*

In an individual trust related setting, a square could represent their online activity in a space, context or domain; this could equally serve as visualising someone's trust activity in a fine grain mode. In a similar vein, another tree map could visualise all individuals' online activities (trust scores in several course grain modes) within a space (room, block or city). Finally, another tree map (again serving as a zoom out function) could visualise several squares where each represents online trust activity and scores of rentable and/or shared smart rooms (specific spaces) to help assist prospective clients decision making. Both latter modes could serve as visualising trust activity and scores of spaces in a course grain mode. In fact, a tree map visualisation approach will enable viewing the impact of individual and groups' online activities (trust scores) within a room and urban spaces in size proportions. Thus, it will easily highlight spaces exposed to higher risks. Figures 1 and 2 illustrate relevant imaginary tree maps.

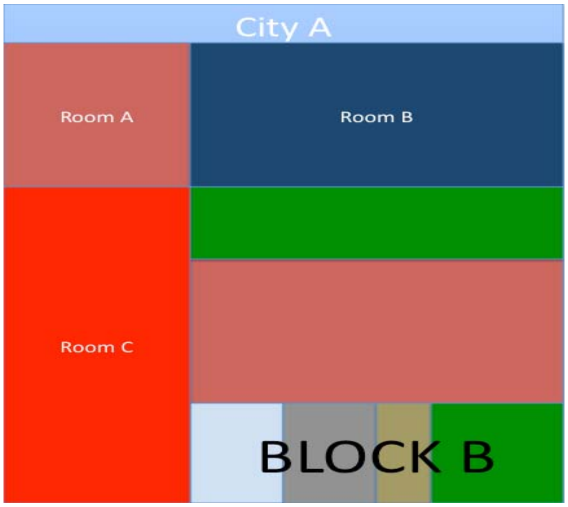

*Figure 2: An Imaginary Tree Map for a Smart Space*

Following a tree map approach, a cloud diagram approach would be useful as to drill-down and illustrate online activities and the properties which make up trust scores as well as the linking between online activities and properties in space and time. Here, we have taken the view that activity density is reflected in size (like tag clouds). In a similar vein, colour coding used in tree map could be also used to illustrate risk levels. Figure 3 illustrates a relevant imaginary cloud diagram. To read the figure (3) note that black nodes show individuals, groups, room or spaces; coloured nodes show properties; size shows risk levels, flows omit directions to avoid complexity and show online activities and their linkages.

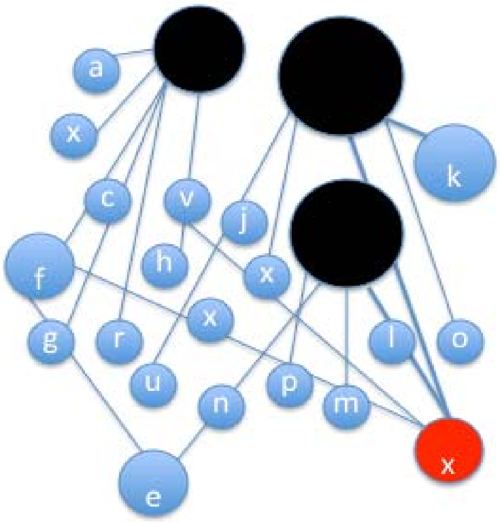

*Figure 3: An Imaginary Cloud Diagram*

A low-level conceptual model architecture diagram is shown in figure 4. Here, we seek to illustrate the components for such a context-aware trust system where one of the core elements is the trust engine. This proposed context-aware trust system will enable users to use drill-down visualisations to monitor activity. The expectation is that room or space system administrators will be able to adjust trust variables to suit their local needs. An important component of the context-aware trust system is the engine itself, which encompasses a lightweight trust model. This is described in section VI.

Indeed, elsewhere, we have sought to point out that in general terms there exists a trust 'gap' with respect to capturing, modeling and implementing and validating intangible trust requirements [8]. Rather, in view of the fact that filling a methodological as well as a notational trust gap is far too ambitious an aim in the context of our current work. Clearly the room agent will need to learn from experience using sensory inputs. Again this aspect although central to the actual run-time performance of the agent is a complex area that lies outside our present scope. Suffice it to say, that a period of training will be necessary prior to the actual "live" running of the system so as to ensure that risky human/machine activities are indeed detected and responded to an a timely manner.

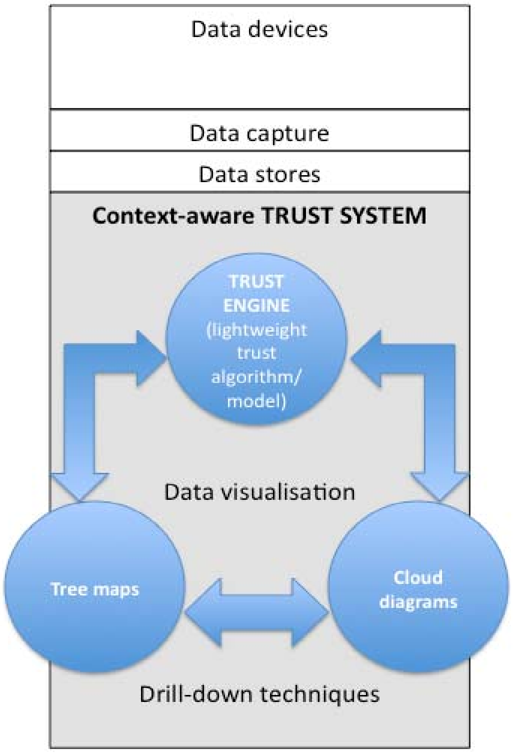

*Figure 4: A Context-aware Conceptual Trust System enabling Drill-down Visualisations*

Categorising behaviours into manual, safety, emergency, efficiency and self-taught will be essential to this training phase. It may be that by mapping scenarios to the various layers of the ladder trust issues will become more explicit. However, a meta-model e-trust ladder can only realistically act as a tool to aid conceptualisation. To enable a room trust agent we need to formalise trust by using variables that can be computed. This is the aim of the next section. In so doing, semiosis is made concrete (formalised) as a measurable confidence level that operates across multiple-levels of the trust ladder.

## VI TRUST IN MULTI-CLIENT SYSTEMS: A LIGHTWEIGHT MODEL

For our proposed model we will adapt a model that has been presented in [17] for multi-client systems. In the scenario a number of clients have access to each other and are making request to a given service. Every client has an opinion about the trustability of this service and maintains four variables for this services which are given in terms of probabilities with values between [0 and 1]. The four variables are s*elfConfidence, experience, hearsay* and *prejudice*. A value below 0 for the three variables experience, hearsay and prejudice denotes a negative attitude, that for example, a human agent cannot be trusted, while a value of 1 denotes a full trust. Any value in between needs to be interpreted in the context given. The variable *selfConfidence* denotes how much the client relates to its own experience and how much the client relates to others' experience within the system.

Trust is then calculated as:

$$trust(ra,h) = selfConfidence(ra,h) * experience(ra,h) + (1-selfConfidence(ra,h)) * hearsay(ra,h)$$

where ra is the room agent and h is the e.g. human agent of which the client seeks an opinion about. We will now look into the variables into detail.

The value of *experience(ra,h)* is initialized with the value of *prejudice(ra,h)* and is then recursively computed via the formula:

$$experience(ra,h) := (immediateExperience(ra,h) + experience(ra,h))/2 \qquad \text{(A1)}$$

where the *immediateExperience(ra,h)* denotes how successful the client was with his most recent request. We see from (A1) that the immediate experience always counts with a weight of half and that the influence of previous experiences decreases exponentially over the number of trust requests the *ra* makes in relation to a given *ha*.

For the value if *hearsay(ra,h)* we assume that every room-agent c is linked to a set R of other computer -agents that are informed via smart city, on-line past history data, the referees, that also have knowledge about the ha.

The value of hearsay(c,s) is then computed as the average of trust of the referees of c, namely:

$$hearsay(c,s) := |R|-1\ \Sigma r\varepsilon R\ trust(r,s) \qquad \text{(A2)}$$

Note that *trust(r,s)* is a variable that is updated whenever r makes a request. It is not dynamically computed at access is this would lead to possibly infinite recursion. We cannot assume that the system is organized as a hierarchy, so two clients can be referees to each other. A result from [18], in the scenario given there, is that the performance of the system, measured in unsuccessful attempts to access a server, is optimal with |R| = 10 and doesn't improve if the set of referees is enlarged.

The optimal choice of *selfConfidence(c,s)* depends on the overall context of the system. The simulations made in previously suggest that under certain conditions an optimal value for *selfConfidence(c,s)* lies between [0.3 to 0.4]. Somewhat counter-intuitively for a larger number of peers that act as referees the optimal value of *selfConfidence(ra,h)* must be closer to 0.4 while for a smaller number of up to 14 referees a value of 0.3 is better. This could be explained in so far that if the number of referees is large then as well a large number of referees must make a negative experience with the service so that this experience propagates through the variable *hearsay(ra,h)* which averages across the referees. In that case the client should base its judgement a bit more on its own experience. Whilst the model outlined here is intentionally "lightweight" using a minimal set of metrics, it would appear to hold at least some potential for enabling a room agent to formalise trust using multiple inputs, "experience" as well as being enabled by a suitable set of starting parameters. The application and tailoring of the model for intelligent spaces is the subject of ongoing work and lies outside the scope this paper. Finally, we take the view that identified variable values will be updated dynamically and in particular, on a near real-time fashion.

## VII CONCLUSIONS AND FUTURE WORK

Smart cities are becoming increasingly viable and enriched through citizen participation, passive sensor data and the IoT so as to enable reverse engineering human agent behaviour patterns, as citizens engage in normal day-to-day activities in urban living contexts. Whilst there are ethical and privacy concerns, normative on-line and real-world activities generate data that can be harvested so as to reduce the risk of a human agent or agents and/or their devices triggering a security incident, either intentionally or unintentionally. As smart cities evolve it is essential that data does not reside in isolated "silos". Rather, datasets need to be harvested and integrated so as to calculate measures (such as trust) that can be used to preserve a "civil society". That is, a smart city can enable intelligent buildings, hence room agents to mitigate risk that an intelligent office space is subject to malevolent active exploits or unintentional security risks. Thus as an ideal vision of the future a smart city, comprises a set of intelligent buildings that are able to infer the level of risk and are able to actively defend costly assets and respond to incidents in near-real time so as to continuously adapt to human needs within a given risk appetite setting. In so-doing the overall level of trust (hence risk is reduced) whilst the data that is being continuously gathered in a smart city context is able to inform decision making at a fine level of granularity.

An immediate step of our future work is to develop a simulation as to process dummy and imaginary individuals' online activities data and visualise them in both fine and coarse grain levels by the use of tree maps and cloud diagrams. The functioning of navigation and drill-down techniques will enable the testing and the operational order of our proposed context-aware and adaptable room trust model.

## VIII REFERENCES

[1] Luong, S., and Chong, S. (2010). Personalised Ambient Intelligence In Buildings via Context Aware Agents. Proceedings. ICISO 2010, Reading University, UK (pp. 17-23)

[2] Filipe, J. (2010). Multi-Agent Systems In Intelligent Pervasive Spaces. Proceedings. ICISO 2010, Reading University, UK (pp. 9-16)

[3] Vlahos, J. (2012). The Department of Pre-Crime. Scientific American, January 2012 (pp. 50-55)

[4] Silva, T., Wuwongse, V., & Sharma, H. N. (2011) Linked Data in Disaster Mitigation and Preparedness. Proceedings. 3$^{rd}$ IEEE International Conference on Intelligent Networking and Collaborative Systems (pp. 746-751)

[5] Cyganiak R. and Jentzsch A. (2011). The Linking Open Data cloud diagram. Available from: http://richard.cyganiak.de/2007/10/lod/

[6] Flax, B.M. (1991). Intelligent buildings, IEEE Communications Magazine, Vol. 29(4), (pp. 24-27)

[7] Perugamal, S., Ramli, A., Leong, C., Samsung, K., and Mansor, S. (2010). Middleware for heterogeneous subsystems Interroerability for Intelligent Buildings. Journal of automation in Construction, Vol. 19(2), (pp.162-168)

[8] French, T. (2009). Towards an E-Trust Framework: trust as a semiotic phenomona, PhD Thesis, School of Systems Engineering, Reading University, UK.

[9] Wong, J.K.W.,Li, H., Wang, W. (2005). Intelligent Building Research: a review, Journal of Automation in Construction, Vol. 14(1), (pp. 143-149) http://www.sciencedirect.com/science/article/pii/S0926580597000253

[10] Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A survey, Computer Networks, Volume 54, (15), October 2010, (pp. 2787-2805)

[11] Presser, M., & Gluhak, A. (2009). The Internet of Things: Connecting the Real World with the Digital World, EURESCOM mess@ge – The Magazine for Telecom Insiders, Vol. 2, 2009

[12] Wang, Y. W., Yu, & Hui-Li, Li, Y. (2011). Internet of things technology applied in medical information. Proceedings. CECNet, 2011, International Conference on Network Infrastructure and Digital Content, 2010 (pp. 430-433)

[13] Rodrigues, J., Salvador, P., Nogueira, A. Multimedia content aggregator applied to an IPTV content-zapping service. Proceedings. EUROCON 2011, IEEE International Conference on Computer as a Tool (pp. 1-4)

[14] Duquennoy, S., Grimaud, G., Vandewalle, J. J. ((2009). Smews: Smart and Mobile Embedded Web Server. Proceedings. CISIS 2009. International Conference on Complex, Intelligent and Software Intensive Systems (pp. 571-576)

[15] Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., Souza, L., Trifa, V. (2009). "SOA-Based Integration of the Internet of Things in Enterprise Services". Proceedings. ICWS 2009. IEEE International Conference on Web Services (pp. 968-975)

[16] Monge, P. R., & Contractor, N. S. (2003). Theories of communication networks. Oxford University press.

[17] Conrad, M., French, T., Maple, C., & Huang, W. (2006). A lightweight model of trust propagation in a multi-client network environment: to what extent does experience matter? Proceedings. ARESARES 2006, International Conference on Availability, Reliability and Security (pp. 6-11)

[18] Bessis, N. (2011). Next Generation Emerging Technologies, Keynote, on World Congress on Sustainable Technologies (WCST-2011), 7th-10th November 2011, London, UK