View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by LJMU Research Online

An access control management protocol for Internet of things devices

M. Taylor, D. Reilly, B. Lempereur, Liverpool John Moores University

Abstract

Internet enabled computing devices are increasingly at risk of misuse by individuals or malware. Initially such misuse was targeted mainly at computers, however there is increasing targeting of tablet and smartphone devices. In this paper we examine an access control management protocol for Internet of things devices in order to attempt to provide some protection against misuse of such devices. Although anti-malware software is commonly used in computers, and is increasingly being used for tablets and smartphones, this may be a less practicable approach for Internet of things devices. The access control management protocol for Internet of things devices examined in this paper involves the use of physical proximity 'registration' for remote control of such devices, encryption of communications, verification of geo-location of the mobile device used to control the IoT device, safe operation controls, and exception reporting as a means of providing a tiered security approach for such devices.

Keywords: Internet security access control

Introduction

The Internet of Things (IoT) enables the integration of data from virtual and physical worlds. [1] The Internet of Things involves smart objects that can understand and react to their environment in a variety of industrial, commercial and household settings. [2] As the Internet of Things (IoT) expands the number of connected devices, there is the potential to allow cyber attackers into the physical world in which we live, as they seize on security holes in these new systems. [3] New security issues arise through the heterogeneity of IoT applications and devices and large scale deployment of such.

Vulnerabilities may be introduced via careless program design that creates opportunities for malware or misuse amongst the wide variety of IoT applications and devices. Large-scale deployment of IoT devices creates a more complex security landscape than has previously existed. [4] The IoT paradigm involves new features, mechanisms and dangers that cannot be completely addressed through the classical formulation of security problems. [5] The IoT requires a new security paradigm that considers security from a holistic perspective that includes actors and their interactions. Researchers had previously highlighted the need for security for IoT-based applications. [6, 7, 8] Although previous research had advocated multi-layer approaches to IoT security this had been limited to mainly theoretical examinations of multi-layer security at a generic level. [9, 10]

The originality of the research presented in this paper concerns a multi-tiered security approach for Internet of Things (IoT) devices that incorporates physical proximity controls, geo-location checking, instruction encryption, embedded controls, and exception reporting. In particular, the geo-locational aspects of the approach represent a novel and innovative use of existing technologies to provide additional security defences over those currently used for IoT devices. The technical challenge addressed by this research is the development of a practical approach to IoT security. The novel contribution of the research presented in this paper is a multi-tiered IoT security approach that combines physical proximity device registration, geo-location

confirmation for instruction authorisation, instruction encryption, embedded safe use logic, and separate channel instruction confirmation. Although any one of the security layers might easily be compromised, it is the combination of security tiers that would make compromise far more challenging. In addition, the multi-tiered approach to IoT security examined in this paper would be inexpensive to implement since it involves commonly available technologies and techniques, which are combined in a novel integrated manner.

Literature review

Internet of things

The Internet of Things (IoT) allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path or network and any service. [11] The Internet of Things offers the capability of integrating information from both physical and virtual worlds. The IoT enables the capability of inferring the status of real-world entities with minimal delay using a web browser. The combination of the Internet and emerging technologies including near-field communications, real-time localization, and embedded sensors allow everyday objects to be transformed into smart objects that can understand and react to their environment. The Internet of Things, requires semantically rich, high-level protocols and agents to make it usable for humans, as well as basic underlying infrastructure protocols that can support mobile connected devices, each of which might communicate infrequently but must be reachable at all times. [12]

Misuse of Internet enabled devices

Advances in technology and the growth of the internet have as a consequence heralded an increase in the number of vulnerabilities being identified, as well as an increase in the complexity of system administration and incident handling. [13] The negative impact of IoT on society may be aggravated as data from sensors are used together with personal data already available in potentially malicious ways. [14] To the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has previously done. [15] The disruption or dysfunction of devices in an IoT infrastructure could create significant threats to operation and reliability, which is an ever-increasing concern for the deployment of IoT technology. [16] The IoT poses a number of new issues in terms of trust in relation to the IoT system layers, that is the physical device layer, the network layer, and the application layer. Measures ensuring the Internet of Thing's resilience to attacks, data authentication, access control and client privacy need to be established.

Internet of things security approaches

Current proposals to implement secure end-to-end communications between smart objects and Internet hosts mostly target the transport layer, in particular by proposing modified versions of the SSL (Secure Sockets Layer) protocol. [17] Internet and web based applications are widely used and different types of access control models have appeared, such as Role Based Access Control (RBAC), Context Aware Access Control (CWAC), and Policy Based Access Control. [18] The constrained application protocol (CoAP) can be applied to protect the transmission of sensitive information to and from IoT devices. Secure CoAP mandates the use of datagram transport layer security (DTLS) as the underlying security protocol for authenticated and confidential communication. [19, 20]

There could be varied security risks associated with deploying IoT-based applications. For example, vulnerabilities associated with smart cities, where sensors could control almost everything, from water management to power networks, or risks to individuals such as risks from misusing and manipulating IoT objects that could include the critical driving elements of a smart car or medical connected devices that provide a patient with precise doses of medicine. There is a need for security quantification to improve the quality of protection of IoT-based applications. Traditional security countermeasures and privacy enforcement cannot be directly applied to IoT technologies due to their limited computing power, and moreover the high number of interconnected devices presents scalability issues. [21] Existing research on the topic of security in the Internet of Things mainly provides an overview of the generic problems, without considering the impact of specific features. Cryptography techniques for IoT systems can easily be broken because of the weak secure nature of IoT devices and the wireless environment. [22] Compromised nodes could lead to insider attacks without being detected by any cryptography checking, thus there is a need for intrusion detection with IoT systems to raise an alarm in the case of any anomaly.

Although previous research had examined the security requirements and challenges for the Internet of Things along with generic security considerations for different enabling technologies and the implications to various applications. [23] Previous research had advocated multi-layer approaches to IoT security, however this mainly concerned theoretical examinations of multi-layer security at a generic level.

Research method

An access control management protocol for Internet of things devices was developed based upon a multidisciplinary literature review of existing research in internet based security. Internet of Things security will realistically require an explicit mapping between IoT device Identities and Internet user identities. By using the concept of threat modeling it is possible to understand how an attacker might be able to compromise an IoT application. Compromise could occur by pretending to be an authorised user of an IoT device in terms of either sending instructions or receiving data from the IoT device, or altering or intercepting instructions or data from the IoT device, or causing the IoT device to carry out actions that might be harmful. Compromise could potentially occur not just to individual IoT devices, but to numerous IoT devices within one building, or even to large numbers of IoT devices in an area or region. Based upon analysis of available technologies for security of IoT applications, the multi-tiered security approach detailed below was developed in order to attempt to address the possible types of security compromises that could occur.

In terms of the technical architecture of the access control management protocol for Internet of things devices a Bluetooth enabled mobile device would communicate via the Bluetooth Low Energy protocol to “register” with an IoT device (for example a cooker within a household). Bluetooth Low Energy protocol signals only work over a short distance (up to 50m), and this provides a layer of proximity security, in other words, the IoT device will only accept instructions from mobile devices that have been in close physical proximity. An application on a mobile device would send a unique Id field via Bluetooth Low Energy protocol to the IoT device. The geo-location from the mobile device would be stored on a text file on the IoT device, and would be used to define the geo-location of the IoT device. The application on the mobile device would allow access from any geo-location with Internet access within a specified radius from the IoT device to the text file (stored on the IoT device itself). The mobile device application allows the user to insert an instruction record on the text file containing for example

Id, temperature, start time and end time fields for a cooker with IoT capabilities. The application on the mobile device would also 'listen' for response entries on the text file. If the Id of a response record equals the Id stored on the mobile device then an SMS message from the text file would be displayed on the mobile device.

An application on the IoT device would 'listen' for a Bluetooth Low Energy signal to accept an Id from the mobile device, and would store the Id in memory. The application on the IoT device would then 'listen' for instruction entries on the text file (stored on the IoT device itself). If the Id of an instruction record equals the Id that had been stored via a Bluetooth Low Energy signal, then the application would read the temperature, start time and end time fields in the example of an IoT enabled cooker. If the temperature value is outside a pre-set range stored on the IoT device, or the end time – start time duration is outside a pre-set range stored on the IoT device, or the combination of temperature and cooking time is greater than a pre-set value, or the cooker temperature is above a set value at the start time of the instruction, then the application on the IoT device would insert a response record on the text file containing the Id and an 'Invalid instruction' field. In this manner embedded 'safe operation controls' stored on the IoT device add another separate layer of IoT security. If the values are in the acceptable ranges then a response record is inserted on the text file containing the Id and instruction values and an 'Instructions accepted' field, which would then be displayed by the application on the mobile device on the screen of the mobile device.

This demonstrates proof of concept for the multi-tiered IoT security approach for controlling an IoT device via the example of an oven with IoT capabilities. Security would be required even for such a simple application on an IoT enabled oven, otherwise malicious individuals, or malware could alter the temperature and the cooking time of the IoT oven, and with sufficiently flammable foodstuffs in the oven could easily cause a fire. If such actions were carried out over an area or region, there could be the potential for numerous building fires.

Research results

The Internet of Things access control management protocol developed consisted of a multi-tiered security approach that included:

Identification Layer: Proximity 'registration' of mobile device(s) with an IoT device using Bluetooth Low energy communication to identify the mobile device to the IoT device.

Transmission Layer: Encryption of signals between the mobile device(s) and the IoT device would be performed using an encryption mechanism suitable for the capabilities of the IoT device.

Verification Layer: Geo-location verification to confirm that the mobile device(s) is / are within a pre-defined radius from an IoT device as identified by the Northing and Easting.

Validation Layer: Safe operation parameters are stored in embedded code in the IoT device to ensure that only valid (safe) instructions are accepted by the IoT device. If "group based" access is allowed to an IoT device, this ensures that safe operation parameters are applied to "resultant" instructions from more than one mobile device.

Reporting Layer: Notification is sent to 'registered' mobile devices of confirmed (accepted) instructions or a warning of invalid instructions by the IoT device, via a separate channel such as SMS messaging.

The more the above layers are 'separated' the more secure the system would be. Thus for example, an attacker might be able to spoof the identity of an authorised user, however they would still need to be within the defined geo-location area, or spoof their geo-location. Even then the validation layer would prevent unsafe operations, unless this too was overcome. If all these layers were overcome, the user would at least be notified that an action (which they had not instructed) had taken place via the separate SMS channel (unless this too was compromised). So although each individual layer of the IoT application could be overcome, an attack would need to be particularly sophisticated to overcome all the separate security layers. In addition to the above security layers, another security feature could be that any manual controls entered physically on the device would override any delivered via the Internet, so that a householder could override manually if for example the oven was unexpectedly turned on. To guard against persons physically entering the household and manually attempting to compromise an IoT device, the embedded safe operation controls would prevent unsafe operation, and the SMS messaging could be used to inform the legitimate user than the oven was being used. In terms of digital forensics a text file could be stored on the IoT device (or on the ISP server) to record the instructions sent (and messages received) between the mobile device(s) and IoT device.

Physical proximity registration

Zhang K. et al (2014) commented that Internet of Things (IoT) are vulnerable to Sybil attacks where attackers can manipulate fake identities or abuse pseudo-identities to compromise the effectiveness of the IoT. [24] Physical proximity registration using short distance Bluetooth Low Energy communications that operate only up to a range of 50m could limit the setting up of fake identities.

Encryption of communications

The suitability of existing cryptographic techniques for Internet of Things (IoT) devices requires appropriate analysis to ensure that given cryptographic algorithms can successfully be implemented within the constrained memory and processor speeds present in IoT devices. [25, 26] There is a need for lightweight and efficient implementations of security protocols and cryptographic algorithms for IoT applications.

Geo-location verification

Geolocation could be a part of IoT access control, but this would require a deeper analysis in order to assess the adaptability to different IoT scenarios. [27] Typically, for any given IoT device, a user would not normally operate such a device outside a given locality, especially for home based devices. However, in certain instances for example when a householder might go on holiday, the geo-location usage radius might be extended.

Safe operation controls

Fault tolerance becomes essential in the design of IoT devices and applications, IoT devices need to be resilient to attacks. [28] In the example of an IoT oven, the following safe operation logic could be applied, in order to demonstrate proof of concept:

If temperature control variable < 100
    Then error message

If temperature control variable > 250
    Then error message

If End time – Start time > 5 hours
    Then error message

If temperature control variable X (End time – Start time) > 500
    Then error message

If temperature > 40 C at start time
    Then error message

The last embedded control "If temperature > 40 C at start time" could help to prevent attempts to override safe operation by repeatedly turning the cooker on and off and thus building up the temperature. In the case of an IoT enabled oven the cooking End time and Start time variables might be stored in hours format e.g. 14:30, and the temperature variable would be stored in degrees Celsius.

Exception reporting

Through exception reporting, the users of IoT applications can be informed of unusual activity related to the IoT application. [29, 30] Figure 1 shows a class diagram for an IoT application that controls a cooker based upon the multi-tiered security approach discussed in this paper.

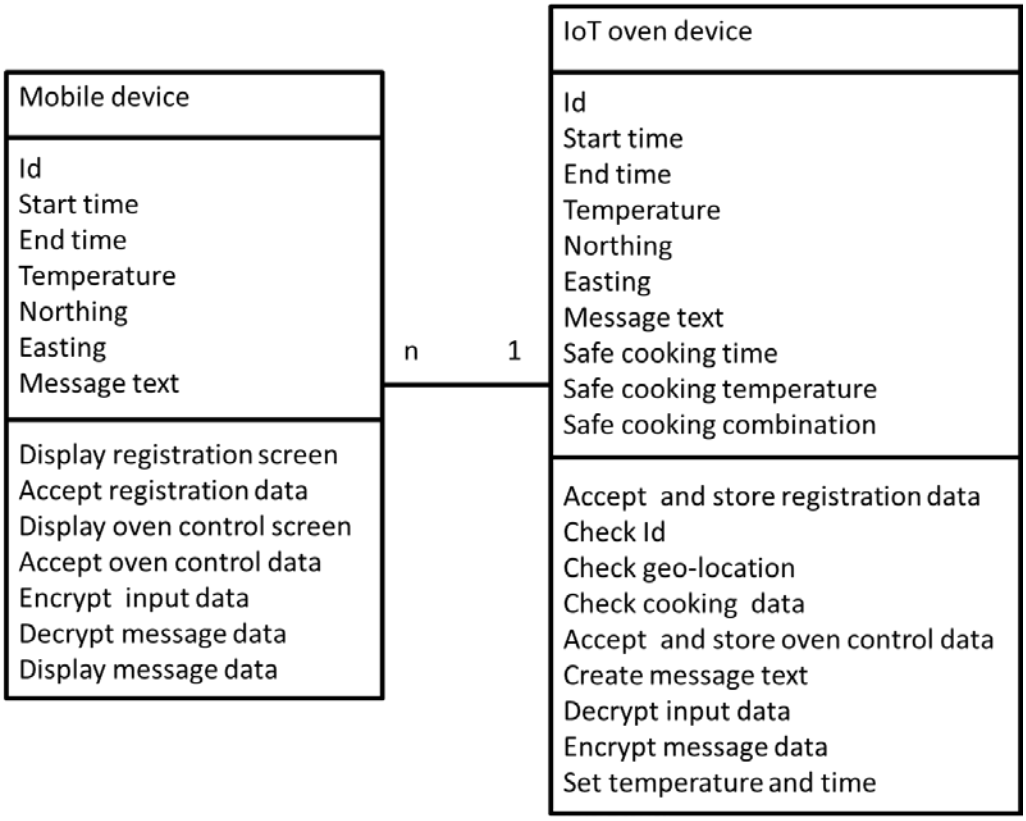

Figure 1. Class diagram showing the data and functions for an IoT enabled cooker that implements the multi-tier IoT security approach.

Evaluation

To demonstrate the multi-tiered IoT security approach discussed in this paper we shall take the example of an Internet of things enabled cooker. Different types of security breaches for an IoT cooker could include:

- Interception of data transmitted between the user of the IoT cooker and the IoT cooker itself. This might be used to determine when someone might or might not be in the dwelling (since instructions might be more typically entered manually when someone was in the dwelling).

- Blocking or disruption of data transmitted between the user of the IoT cooker and the IoT cooker itself. This might be used to maliciously disrupt the operations of the IoT cooker.

- Manipulation of data transmitted between the IoT user and the IoT cooker. This could be used to maliciously alter the operation of the IoT cooker.

- Unathorised use of the IoT cooker, this could involve malicious operation of the IoT cooker.

- Unathorised modification of embedded software in the IoT cooker. This could concern both present and future malicious operation of the IoT cooker.

The different security layers in the multi-tiered security approach described in this paper would counter the different types of potential security breaches:

- The use of encryption to reduce the likelihood of interception or manipulation of data transmitted.

- The use of separate communication channels for data transmission from the user to the IoT cooker, and from the IoT cooker to the user. This could reduce the likelihood of blocking or disruption.

- The use of proximity registration and geo-location confirmation to reduce the likelihood of unauthorised use.

- The use of embedded software controls to reduce the likelihood of malicious (and potentially dangerous) operation of the IoT cooker.

- The use of separate communication channels and embedded software controls to reduce the likelihood of successful modification of embedded software, since such code would potentially need to be altered in a number of ways to prevent the user becoming aware of malicious code changes via the separate communication channel.

Existing approaches to IoT security typically either provide theoretical generic multi-layered models or concentrate on specific aspects of IoT security such as communication protocols, or encryption approaches. [31]

The level of security provided by the multi-tiered approach to IoT security discussed in this paper can be modelled to quantify the risk exposure [32] by the formula:

$P_i \times P_g \times P_e \times P_s \times P_w$

Where P_i = probability of overcoming IoT device registration (identifying and using id code used for IoT device instructions, data and messages)

P_g = probability of overcoming IoT device geo-location controls (identifying and using a geo-location within a set radius from the IoT device)

P_e = probability of overcoming encryption used to communicate with the IoT device

P_s = probability of overcoming the safe operation code embedded in the IoT device

P_w = probability of overcoming warning messages sent via separate communication channel to the mobile device.

These probabilities represent mutually exclusive events. Although the security tiers all adopt existing technologies, the novelty of the research presented in this paper concerns the combined use of the different technologies via a multi-tiered framework that reduces the probability of compromise of an IoT application due to the separation of the security controls provided in each of the tiers. The technical challenge addressed in this paper is the development of a

reliable, inexpensive and operationally sound approach to security for IoT applications based upon commonly available low cost technologies.

The originality of the research presented in this paper concerns a multi-tiered security approach for Internet of Things (IoT) devices that incorporates an integrated set of security layers including physical proximity controls, geo-location checking, instruction encryption, embedded controls, and exception reporting. In particular, the geo-locational aspects of the approach represent a novel and innovative use of existing technologies to provide additional security defences over those currently used for IoT devices.

Conclusions

Misuse of IoT devices could occur via malicious individuals or via malware. Any given type of access control management security measure could potentially be breached. Adopting a multi-tiered approach to IoT access management security makes misuse more difficult since a number of separate 'independent' layers of security would need to be breached.

The novelty of the research presented in this paper concerns the development of a practical, low-cost multi-tiered approach to security for IoT applications that combines physical proximity registration of an IoT device, encryption of communications between mobile devices and the IoT device, geo-location verification, embedded safe operation controls and exception / confirmation reporting. The low-cost aspect of the approach is achieved through the use of commonly existing available technologies that are combined together in a novel manner.

References

1. Yao, L., Sheng, Q., Dustdar, S. (2015) Web-Based Management of the Internet of Things, IEEE Internet Computing, 19, 4, 66 – 70.

2. Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V. (2010) Smart Objects as Building Blocks for the Internet of Things, IEEE Internet Computing, 14, 1, 44 – 51.

3. Shin, D. (2014) A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things, Telematics and Informatics, 31, 519 – 531.

4. Zhang, Z., Cho, M., Wang, C., Hsu, C., Chen, C., Shieh, S. (2014) IoT security: ongoing challenges and research opportunities, In Proceedings of 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 17-19 November 2014, Matsue, Japan, pp. 230-234.

5. Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z. and Bouabdallah, A. (2013) A systemic approach for IoT security. In Proceeding of 2013 IEEE International Conference on Distributed Computing in Sensor Systems, 20 - 23 May 2013, Cambridge, MA, USA, pp. 351-355.

6. Ghani, H., Khelil, A., Suri, N., Csertan, G., Gonczy, L., Urbanics, G., Clarke, J. (2014) Assessing the Security of Internet Connected Critical Infrastructures, Security and Communication Networks, 7, 2713 – 2725.

7. Hassanzadeh, A., Modi, S., Mulchandani, S. (2015) Towards effective security control assignment in the Industrial Internet of Things, In Proceedings of IEEE 2nd World Forum on Internet of Things, 14-16 December 2015, Milan, Italy, pp 795 – 800.

8. Weber, R. (2010) Internet of Things – New security and privacy challenges, Computer Law and Security Review, 26, 23 – 30.

9. Yang, X., Li, Z., Geng, Z., Zhang, H. (2012) A multi-layer security model for internet of things. In Internet of Things (pp. 388-393). Springer, Berlin Heidelberg.

10. Roman, R., Zhou, J., Lopez, J. (2013) On the features and challenges of security and privacy in distributed internet of things, Computer Networks, 57, 2266 – 2279.

11. Nolin, J., Olson, N. (2016) The Internet of Things and convenience, Internet Research, 26, 2, 360 – 376.

12. Petrie, C., Spatscheck, O. (2012) Future Internet Protocols, IEEE Internet Computing, 16, 6, 11 – 13.

13. Rosado, D., Gutiérrez, C., Fernández-Medina, E., Piattini, M. (2006) Security patterns and requirements for internet-based applications, Internet Research, 16, 5, 519 – 536.

14. Almeida, V., Doneda, D., Monteiro, M. (2015) Governance challenges for the Internet of Things, IEEE Internet Computing, 19, 4, 56 – 59.

15. Atzori, L., Iera, A., G. Morabito, G. (2010) The Internet of Things: A Survey, Computer Networks, 54, 15, 2787–2805.

16. Chen, P., Cheng, S., Chen, K. (2014) Information Fusion to Defend Intentional Attack in Internet of Things, IEEE Internet of Things Journal, 1, 4, 337 – 348.

17. Granjal, J., Monteiro, E., Silva, J. (2014) Network-layer security for the Internet of Things using TinyOS and BLIP, International Journal of Communication Systems, 27, 10, 1938-63.

18. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things, Journal of Cyber Security and Mobility, 1, 4, 309-348.

19. Raza, S., Shafagh, H., Hewage, K., Hummen, R., Voigt, T. (2013) Lithe: Lightweight secure CoAP for the internet of things, IEEE Sensors Journal, 13, 10, 3711-3720.

20. Keoh, S., Kumar, S., Tschofenig, H. (2014) Securing the internet of things: A standardization perspective, IEEE Internet of Things Journal, 1, 3, 265-75.

21. Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisiniet, A. (2014) Security, privacy and trust in Internet of Things: The road ahead, Computer Networks, 76, 146 – 164.

22. Le, A., Loo, J., Lasebae, A., Aiash, M., Luo, Y (2012). 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach, International Journal of Communication Systems, 25, 9, 1189-212.

23. Li, S., Tryfonas, T., Li, H. (2016) The Internet of Things: a security point of view, Internet Research, 26, 2, 337 – 359.

24. Zhang, K., Liang, X., Lu, R., Shen, X. (2014) Sybil Attacks and Their Defenses in the Internet of Things, IEEE Internet of Things Journal, 1, 5, 372 – 383.

25. Porambage, P., Braekeny, A., Gurtovz, A., Ylianttila, M., Spinsanteet, S. (2015) Secure End-to-End Communication for Constrained Devices in IoT-enabled Ambient Assisted Living Systems In Proceedings of IEEE 2nd World Forum on Internet of Things, 14-16 December 2015, Milan, Italy, pp 711 – 714.

26. Nguyen, K., Laurent, M., Nouha Oualhaet, N. (2015) Survey on secure communication protocols for the Internet of Things, Ad Hoc Networks, 32, 17 – 31.

27. Skarmeta, A., Hernandez-Ramos, J., Moreno, M. (2014) A decentralized approach for Security and Privacy challenges in the Internet of Things, IEEE World Forum on Internet of Things, 6 - 8 March, 2014, Seoul, Korea, pp 67 – 72.

28. Oriwoh, E., Sant, P., Epiphaniouet, G. (2013) Guidelines for Internet of Things deployment approaches – The Thing Commandments in Proceedings of the 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, October 21 - 24, 2013, Niagara Falls, Ontario, Canada pp 122 – 13.

29. Franssila, H. (2016) Enhancing information interaction as a means for situation awareness maintenance in mobile field work, Cognition, Technology & Work, 18, 3, 567–582.

30. Hou, B. and Sheng-Yang, Y. (2012) Design of Distributed Remote Real-Time Monitoring and Control System Based on Internet, Journal of Emerging Trends in Computing and Information Sciences, 3, 7, 1068 - 1073.

31. Li, F., Xiong, P. (2013) Practical secure communication for integrating wireless sensor networks into the internet of things, IEEE Sensors Journal, 13, 10, 3677-84.

32. Gupta, M., Banerjee, S., Agrawal, M., Rao, H. (2008) Security analysis of Internet technology components enabling globally distributed workplaces—a framework, ACM Transactions on Internet Technology, 8, 4, 17 - 55.