Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 59 (2017) 150 – 155

www.elsevier.com/locate/procedia

The Fifth International Through-life Engineering Services Conference

Secure IoT Devices for the Maintenance of Machine Tools

Stefano Tedeschi[a]*, Jörn Mehnen[a], Nikolaos Tapoglou[a], Rajkumar Roy[a]

[a]*EPSRC Centre for Innovative Manufacturing in Through-life Engineering Services*
Manufacturing Department, Cranfield University, MK43 0AL, UK

* Corresponding author. *E-mail address:* {s.tedeschi, j.mehnen, n.tapoglou, r.roy } @cranfield.ac.uk

Abstract

Through the Internet of Things (IoT) interaction between objects becomes possible in a way we have never seen before. With the advent of IoT and its introduction into almost all aspects of life, safety and security of IoT devices has to be considered for their whole life cycle. This concerns not only the large amounts of data that needs to be exchanged securely but also the design of the hardware of the devices themselves. Security has to be designed right from the start into IoT devices rather than added on later.
This paper will introduce a global strategy for secure Design for IoT which includes:

- Safe solutions for environments with rich information
- Guarantee that the devices are functioning as intended by the manufacturer and are not damaged
- Life cycle security across devices, networks and data centers
- Support for industry standards and interoperability of devices
- Ability to solve the challenges of the information link
- Secure Clouds for traditional systems.

This paper lays the foundation for the creation of a safe remote monitoring system for machine tools through IoT devices and analyses the critical issues focusing on the manufacturing environment.

Peer-review under responsibility of the scientific committee of the The 5th International Conference on Through-life Engineering Services (TESConf 2016)

Keywords: Remote Maintenance; Machine Tool; Secure Communications; Remote Monitoring;IoT

1. Introduction

Currently, the continued growth of Internet of Things (IoT) has made remarkable progress in information technology. This technique has become an important engine of economic growth around the world [1, 2]. The idea of IoT goes back to the 1998, when it was given a first description by a British researcher and co-founder of Massachusetts Institute of Technology (MIT). He called the IoT the set of “all things that are connected with Internet through sensors, such Radio Frequency Identification (RFID), to achieve intelligent identification and management” [3]. Many different definitions have since followed and each geared to highlight the main possible scope of IoT application. In this sense, the Internet of Things can be considered "a family of technologies whose aim is to make any type of object or device connected to the Internet, able to enjoy all the features that the objects created to use the network” [4].

Nowadays, the properties related to the IoT systems are essentially two: monitoring and control. With monitoring, we intend the capability of the object to behave as a sensor or to be able to produce information about itself or the encompassing environment. Instead, the control means that objects can be remotely controlled with no particular technologies but through the Internet. In the industrial sector, the Internet of Things (IoT) thing is associated with the concept that intelligent machines, devices and people are connected through them. This connection leads to the possibility of making better decisions with large databases and advanced analytics. This aspect is of high important for factories that will be increasingly intelligent. There will be a significant improvement in the ability to collect, analyse and distribute data converted into important information. This could help factories in maintenance operations through the sharing of data with the service assistance. In this paper it will be explored what enterprises can do to manage the security

Peer-review under responsibility of the scientific committee of the The 5th International Conference on Through-life Engineering Services (TESConf 2016)
doi:10.1016/j.procir.2016.10.002

risks associated with IoT devices. The paper presents the main cause of potential data loss in remote maintenance architectures. A practical example demonstrates a new approach to increase the level of safe remote monitoring system for machine tools through IoT devices.

2. Research problem

One of the aims of manufacturing enterprises is to produce high-quality products characterized by no defects. It is also requested that the machine tool can maintain high overall equipment efficiency (OEE), without compromising the company's profit because of prolonged shutdowns.

A part of the research aim is to provide support to companies that do not have a remote maintenance system for machine tools. The occurrence of a machine downtime is transformed into a loss of competitiveness on the market, loss of money and time. A company is required to immediately contact servicing, to reduce machine downtime. However, in many cases, there could be a significant delay before returning the machinery to operational status. During this time, the service engineer will perform an initial diagnosis to understand the underlying problem, extending the machine downtime.

Ideally, a company is configured with a remote maintenance system for machine tools. In this case, the major problems arise to ensure long life to the maintenance system, evaluating the reliability of all the connected devices. Remote maintenance, however, is linked with the issue of the protection of machine data over public or private networks. Another problem involves the secure communications with the assistance service on the public networks.

This paper addresses this challenge through providing guidance to companies that consider remote maintenance as a solution to higher productivity, involving the protection of machine data from threats which would entail a leak of information knowledge.

3. Related work

Currently, many research projects have been proposed to develop remote monitoring and maintenance systems (RMMS). Yang et al. [5] developed an Internet-based remote maintenance system for process control. Feldmann and Göhringer [6] have developed an Internet-based diagnosis of a monitoring system for maintenance. Lung et al. [7] developed a maintenance tool to facilitate remote decision making. Cunha et al. [8] developed a service module as input for production planning. Mori et al. [9] proposed a practical way to improve the efficiency of maintenance by monitoring and analysing the state of operation of 8000 machine tools simultaneously worldwide.

With respect to remote monitoring and maintenance systems through IoT devices, Yonggang et al. [10] developed a wall-mounted boiler remote monitoring and control system based on IoT cloud platform. Wang et al. [11] developed an IoT application for fault diagnosis and prediction. Sharma and Suryakanthi [12] developed a system called IoT for University. Lee at al. [13] developed a smart home web of object architecture. Alexandru et al. [14] develop a smart web-based maintenance system for a smart manufacturing environment.

With regards to system data protection through IoT devices Tiburski et al. [15] developed a security architecture for SOA-based IoT middleware. As a threat analysis for embedded devices, and monitoring systems, Shahri and Ismail [16] developed a model for identification of threats as the first stage of risk assessment in Health Information System (HIS). Di and Smith [17] developed a hardware threat modelling concept for trustable integrated circuits. Di-Battista et al. [18] analysed side-channel attack methods. Kim et al. [19] developed an extensive analysis of side-channel attacks on cryptographic module. Nakai et al. [20] studied the cause of memory-dependent EM geometric leaks.

These developments published in literature present different remote monitoring and maintenance systems and strategies useful to evaluate the health status of industrial machines. Moreover, a collection of the papers focused particularly on the IoT applications within the home, university, and industry field. Shahri and Ismail reviews common threats in the industrial environment such as human, technical and physical threats.

Throughout most of these examples from literature, particularly those focused on IoT and monitoring systems, the reader is confronted with a situation in which many do not focus on security related issues of these remote technologies, which will be a significant concern for industries looking to utilize and exploit these technologies. This paper introduces a strategy to analyze and design a safe solution for environments with rich information.

4. Identified threats

The identification of threats is a fundamental stage in risk management and the social science has long had privacy and security issues as a major subject. In literature a lack of a systematic investigation for the identification and categorization of threats related to information security and privacy can be observed [21].

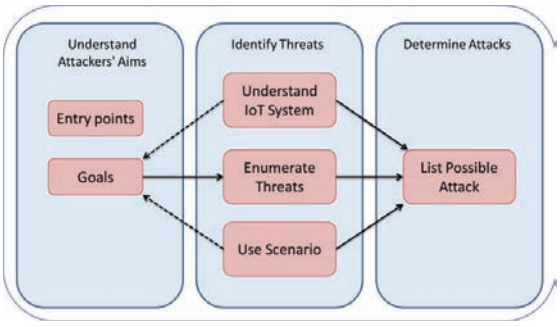

Figure 1: Threats modelling process

In Figure 1, the three high-levels constituting the preliminary hardware threat modeling process are shown. They consist in Understanding Point of View, Identifying Threats, and Determining Attacks. Furthermore, the first two steps can be divided into logical sub-steps.

Understanding Attackers' Aims

The purpose of this level is the understanding of what the attackers want. It represents a critical aspect considering that the threat modeling aims to prevent the satisfaction of the attackers' goals which, then, must be well understood.

Entry points – are the entrances where the attackers can interface with the target. Unlike in software/network systems, where the entry points are usually difficult to enumerate and subject to change, entry points for hardware are much fewer and relatively fixed.

Goals – Usually, the hardware attackers' goals are linked to the integrated circuits. They can determine:

- ✓ Information leakage – attackers manage to directly extract information from an integrated circuit, passively or actively, as an individual component or as an element of an integrated system. Information to be protected includes the IP associated with a chipset and its design, data with both the hardware and deployed software, and data embedded [22].
- ✓ Tampering – attackers eavesdrop on or modify the data associated with the integrated circuit by prolonged inspection and monitoring.
- ✓ Denial of service – attackers manage to modify the structure of the internal circuit of an integrated system to cause its malfunction or shutting down under operating conditions.

Identify threats

The scope of this level is the identification of all possible threats to the IoT system for the attackers aiming to reach their goals. An attacker could be interested in acquiring of the cryptographic key stored in an integrated circuit from IoT system, and then the corresponding threat would be the access to the RAM chip and controlling the internal bus.

Understand IoT structure – The goal of this sub step is to understand the integrated circuits functionality and its internal circuit structure, which will help identify the threats.

Use scenarios – This sub step aim is to determine the potential applications of the target IoT.

By so doing will expand the threats modelling process with human and physical factors.

Enumerate threats – It is possible to enumerate all potential threats in an IoT system because once configured, the IoT structure will be fixed. All threats will be enumerated based on the understanding of attackers' goals, IoT structure, and external scenarios.

Determine attacks

The purpose of this level is to individuate how the attackers could reach their objective by enumerating and listing all possible attacks associated with each threat individuated in the previous level. This process will take into account both the internal circuit structure and the external scenarios.

5. Classification of threats

An important part of this research is to analyse the most common causes for data loss in industrial applications. This served as a starting point for analysing the remote monitoring system and to find some mitigation useful to develop robust remote monitoring system architectures. To furnish this analysis, a literature review [16-20], survey and interview have been undertaken. Table 1 shows an overview of threats considered in this research work. The threat research is categorized into three main groups: Human, Physical and Technical. Categories depend on the work environment. In the case of this paper, remote monitoring of a 24-hour manufacturing environment is considered.

Table 2 shows an overview of threat examples that contributes to the development of a more secure remote monitoring system through secure IoT device.

Human Threats	
Threats	**Descriptions**
Inadvertent Acts or Carelessness	Are unintentional acts that could cause system performance degradation or system loss.
Data entry errors or omissions	Are non-malicious threats that could affect system resources and the safeguards that are protecting other system resources.
Physical Intrusions	Are deliberate malicious acts that could cause damage, destruction, or loss of system assets. Such an act could also enable other threats, such as compromise of interconnected systems.
User Abuse	Addresses authorized users who abuse their assigned access privileges or rights to gain additional information or privileges.
Unauthorised use of remote maintenance accesses	Are continuous acts that could cause damage of system assets. Such an act could also enable other threats, such as the insertion of virus, collect sensitive information.
Introduction of malicious code via removable media and external hardware	Access to external ports for the introduction of viruses into the system, or new settings.
Physical Threats	
Threats	**Descriptions**
Electromagnetic interference	Is the impact of signal transmitters and receivers operating in proximity integrated system, which could cause an interruption in the electronic operation of the system.
Physical cable cuts	Could be an intentional or unintentional event that affects the system's ability to perform its intended function.
Power fluctuation	Is a disruption in the primary power source (power spike, surge, brownout, and blackout) that results in either insufficient or excessive power.
Voltage spikes	Refers to a rapid variation of voltage, more specifically to a voltage peak and short duration, may cause damage system assets.
Technical Threats	
Threats	**Descriptions**
Dangerous emanations	Are the unintentional data-related or intelligence-bearing signals, which, if intercepted and analyzed, could disclose sensitive information being transmitted and/or processed.
Data/system contaminations	Is the intermixing of data of different sensitivity levels, which could lead to an accidental or intentional violation of data integrity.
Hardware	Is the unexpected loss of operational functionality of any system hardware asset.
Software	Is the malicious intent to change a system's configuration without authorization by the addition or modification of code, software, database records, or information.
Installation errors	Are the errors, which could occur as an of result poor installation procedures. Could undermine security controls.

Tampering	Is an unauthorized modification that alters the proper functioning of equipment in a manner that degrades the security functionality the asset provides.
Takeover of authorized session	Is gaining control of an authorized session, and assuming the access rights of the authorized party.
Online attacks via office	Is an unauthorized modification takes place within the local network that alters the proper functioning of equipment.
Reading and messages in the integrated system	Access to communications equipment that allows the free leakage of sensitive information.

Table 1: A summary threat analysis descriptions, condensed from [16]

Human Threats	
Threats	**Examples**
Inadvertent Acts or Carelessness	-Programming and development errors result in software vulnerabilities. -Incorrect operations of database synchronization procedures could result in data errors and deletion. -Improper upgrades to database management software. -Programming and development errors could cause a buffer overflow. -Installation, upgrade, and maintenance errors could leave data unprotected.
Data entry errors or omissions	-Failure to disable or delete unnecessary accounts (network, Internet), could provide unauthorized access to system resources. -If the system administrator fails to perform some function essential to security, it could place a system and its data at risk of compromise.
Physical Intrusions	-Disgruntled employees could create both mischief and sabotage of system data. -Sensitive data could be captured through application vulnerabilities, and held hostage. -Disgruntled employees could sabotage a computer system by installation of software that could damage the system or the data. -Destruction of hardware or facilities could destroy data that might not be recovered. -Computer abuse such as intentional and improper use, alteration and disruption could result in loss of system assets. -Cleaning staffs/vendors or contractors could steal unsecured sensitive information
User Abuse	-Use of information (password) as an indirect aid for subsequent misuse -The opening of an unprotected port on a firewall could provide unauthorized access to information
Unauthorised use of remote maintenance accesses	-Unauthorised personnel could change passwords, account and system assets -Modify maintenance parameters
Introduction of malicious code via removable media and external hardware	-Trojan -New system assets
Physical Threats	
Threats	**Examples**
Electromagnetic interference	-Malfunctioning equipment -An extended power surge, over-stress power supplies and lead to computer equipment damage. -A power failure, disrupting network operation, computer screens to go blank, and servers to crash.
Physical cable cuts	-A disgruntled employee could sabotage transmission media -Animals could cause damages to cables resulting in broken cables.
	-Lightning strikes could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure. -Lightning strikes could cause severe damage resulting in broken cables.
Power fluctuation	-Malfunction or failure of Central Processing Unit (CPU) or hardware could impact the timeliness and quality of the delivered services.
Voltage spikes	-Malfunction of CPU or hardware equipment. -Internal power disturbances could result in loss of system data.
Technical Threats	
Threats	**Examples**
Dangerous emanations	-Radiation or signals that emanate from a communications circuit could disclose to unauthorized persons or equipment the sensitive or proprietary information that is being transmitted via the circuit.
Data/system contaminations	-Anomalies and multiple numbers for the same entity could allow unauthorized access to data. -Corrupted system files could contain strings of sensitive information. -File fragments containing sensitive information could be scattered throughout a drive instead of in an encrypted sector to protect them from compromise.
Hardware	-Malfunction or failure of Central Processing Unit (CPU) -Faulty network components such as hosts, routers and firewalls could result in interruption of communications between the connected stations. -Improper hardware maintenance could allow a system crash to occur. -Timing Attack
Software	-Modification, insertion, or deletion of data or lines of code could compromise data and/or system. -Unauthorized modification of database records could compromise data integrity and availability. -Trojan Horse applications could be installed through code and software modifications. -Logic bombs could be placed within authorized software and perform malicious system actions on a given trigger event.
Installation errors	-Poor installation procedures could leave data unprotected, e.g. built-in security features of software packages are not implemented. -Incorrect installation or a conflict with another device that is competing for the same resources within the computer system could impact system data and resource availability.
Tampering	-Web hacks could deface a web site, or disable the web server functionality. -Domain Name Service hacks could prevent authorized users from properly accessing network or Internet resources.
Takeover of authorized session	-When a user leaves the immediate work area and a session remains open, unauthorized use could occur.
Online attacks via office	-Unauthorized staffs could have access to sensitive information.
Reading and messages in the integrated system	-Sharing of badges, key cards, and passwords could provide unauthorized access to private information. -Forged email messages could reveal sensitive information.

Table 2: A summary of threats analysis examples, condensed from [16]

6. Develop a global design strategy for securing IoT devices

The process of configuring secure IoT devices launches the bases as a new approach. This approach may not only be used in the manufacturing environmental but with the right changes also in other working environments.

Figure 2 shows a global strategy for securing IoT devices. The process is divided into four main categories.

Define requirements – includes the threats analysis and the signals to be measured to make maintenance.

Prototype concept – this category involve the physical construction of the device, paying attention to the choice of modules.

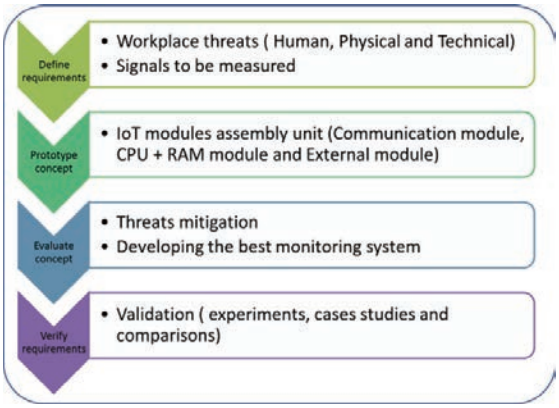

Figure 2: Configuration process

Evaluate concept -it concerns the concept of evaluation through the selection of threats mitigations. By so doing will develop best technical solution for remote monitoring. Verify requirements -it's the evaluation phase of the prototype through experiments and comparisons with other devices. Only by so doing we will understand if our monitoring system appears to be safer than those on the market.

7. Design of a safe remote system for machine tools through IoT devices

An IT scenario can be greatly influenced by IoT technology, determining a competitive advantage for business. Also, it has to be considered that the companies are subject to several new threats with the use of new technology. Figure 3 shows the architecture of a data protection and secure communication system that has been developed for this paper. From the hardware point of view, the proposed system provides a Data Acquisition Unit (DAQ), made from Raspberry Pi model B, a Wi-Fi module, the accelerometer MPU 6050, a FLIR lepton thermal imaging module for temperature monitoring, and a power bank of 3350 mAh that provides sufficient battery life for the unit.

The system is able to collect acceleration and temperature data at 1 kHz with 100 kbps baud rate in a single 14 byte read and over I2C running at 400 kbps baud rate. The thermal camera module captures infrared radiation within the wavelength band from 8 to 14 microns.

All the collected data is not stored within the microcontroller but is transferred to storage and sharing units accessible only to accredited persons via cloud storage.

Inside the system are a combined iteration of the HTTP protocol through a mechanism of encryption such as Secure Sockets Layer (SSL), the acquired data are then transferred to the Cloud system. The SSL protocol provides connection security guarantees [23]:

- ✓ Authentication (security identity of the subjects that communicate)
- ✓ Data confidentiality (protection of data from unauthorized observers)
- ✓ Data integrity (security that the data received is equal to the datum sent).

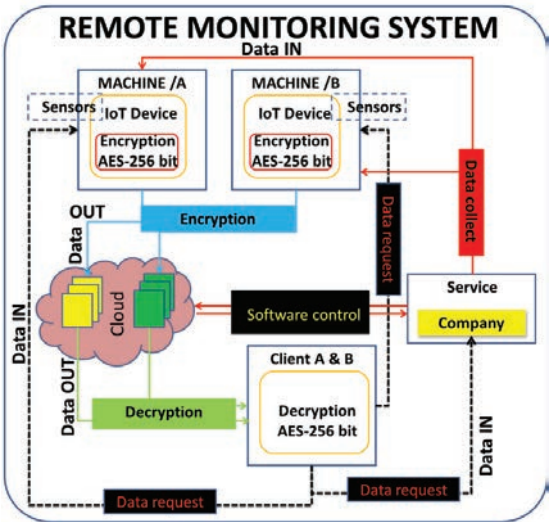

Figure 3: System data protection and secure communication

This system architecture allows for the mitigation of some possible threats that occur on the communication network that were highlighted in Table 1 and Table 2.

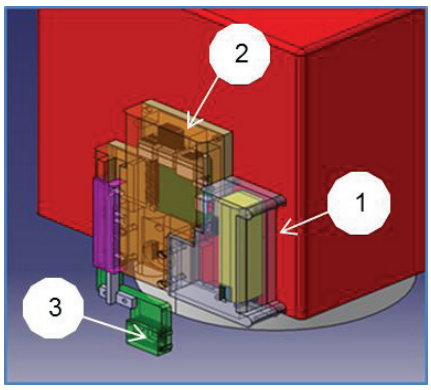

Figure 4: Data Acquisition Unit (DAQ)

Figure 4 shows the DAQ design, which is compact, lightweight and divided into 3 modules: power bank module (1), CPU module (2) and the thermal camera module (3), in order to facilitate the direct maintenance operations. The

power bank is to avoid power fluctuation and voltage spikes, and the lack of external cables avoids direct physical interfacing and tampering. The protective cover does not allow access to the unit for unauthorized persons. The system is assembled together on the DMG machine tool spindle and used during machining operations. On the board, all external ports are disabled except a USB port for the Wi-Fi connection and Micro USB for power bank. To collect vibration signals and temperature data, you must have an account and password to access the executable file that launches the remote program. The monitoring system is equipped with 256-bit AES encryption [24]. An increase of data security is achieved sby the microcontroller on board which collects the data and writes an encrypted text file that will be sent directly to the Cloud system. At this point, all data within the microcontroller is deleted so as not to occupy valuable memory and to not leave traces of data on the device. Inside the Cloud, the data will be provided in encrypted form and only those with keys and a valid certificate will have access.

8. Conclusion

In this paper, the foundation for the realization of a methodical approach for preventive maintenance through IoT device as a data acquisition unit capable of self-learning during the run-time of a machine tool has been presented. The methodical approach is focused on threats that generate a loss of data or information from the monitoring system. Future work aims to utilize this monitoring system also as a remote control system for different actuators.

Acknowledgements

This work is being undertaken with the EPSRC, grant number EP/I033246/1 and collaboration with the group Kennametal and will be conducted in the EPSRC Centre for Innovative Manufacturing in Through-life Engineering Services. Many thanks also to DMG Mori who made the CNC turn-mill centre NT1000/W available for this research.

References

[1] M. Chen, (2014) “NDNC-BAN: supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks” Information Sciences, 284: 142–156.

[2] Tedeschi, S. , Mehnen, J. , Tapoglou, N. , Rajkumar, R., (2015) “Security Aspects in Cloud Based Condition Monitoring of Machine Tools” 4th International Conference on Through-life Engineering Services, TES 2015 Procedia CIRP, 38: 47-52

[3] K. Ashton, (2009) “That ‘Internet of Things’ Thing: In the real world, things matter more than ideas,” RFID J., June 22, 2009: http://www. rfidjournal.com/articles/view?4986#sthash.NsRaiwEl.dpuf

[4] Mark Weiser, (2014) “What is the Internet of Thighs” La Stampa, http://www.aspeninstitute.it/system/files/inline/Internet%20of%20Things.pdf.

[5] S.H. Yang, Ch. Dai, and R.P. Knott (2007) “Remote Maintenance of Control System Performance over the Internet” Control Engineering Practice, 15(5): 533-544.

[6] K. Feldmann, J. Gohringer (2001) “Internet based Diagnosis of Assembly Systems” Annals of the CIRP, 50 (1):5–8.

[7] B. Lung, M. Veron, M.C. Suhner, A. Muller (2006) “Integration of Maintenance Strategies into Prognosis Process to Decision-Making Aid on System Operation” Annals of the CIRP, 54(1):5–8.

[8] P.F. Cunha, J.A. Caldeira Duarte, L. Alting (2004) “Development of a Productive Service Module Based on a Life Cycle Perspective of Maintenance Issues” Annals of the CIRP, 53(1):13–21.

[9] M. Mori, M. Fujishima, M. Komatsu, B. Zhao, Y. Liu (2008) “Development of remote monitoring and maintenance system for machine tools” Annals of the CIRP, 57:433–436.

[10] Yonggang Gong, Aide Zhou, Yanan Xiao, (2014) “Design of wall-mounted Boiler Remote Monitoring and Control System based on the Ayla IOT Cloud Platform” Applied Mechanics & Materials, Issue 571-572: 1047.

[11] Chen Wang, Hoang Tam Vo, Peng Ni, (2015) “An IoT Application for Fault Diagnosis and Prediction” IEEE International Conference on Data Science and Data Intensive Systems: 726-731.

[12] Kamlesh Sharma ,T. Suryakanthi, (2015) “Smart System: IoT for University” International Conference on Green Computing and Internet of Things (ICGCloT): 1586-1593.

[13] NamKyung Lee, HyungKeuk Lee, HyunWoo Lee, Won Ryu, (2015) “Smart home Web of Object Architecture”International Conference on Information and Communication Technology Convergence :1212-1214.

[14] Ana M. Alexandru, Alice De Mauro, Maurizio Fiasché, Francesco G. Sisca, Marco Taisch, Luca Fasanotti and Piergiorgio Grasseni, (2015) “A Smart web-based Maintenance System for a smart manufacturing environment” IEEE 1st International Forum : 579-584.

[15] Ramão Tiago Tiburski, Leonardo Albernaz Amaral, Everton De Matos, Fabiano Hessel, (2015) “The importance of a standard security architecture for SOA-based IoT middleware” IEEE Communications Magazine, 53(12) :20-26.

[16] Ahmad Bakhtiyari Shahri, Zuraini Ismail, (2012) “A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS” Journal of Information Security, 3: 169-176.

[17] Jia Di and Scott Smith, (2007) “A Hardware Threat Modeling Concept for Trustable Integrated Circuits” IEEE Region 5 Technical Conference, April: 65-68.

[18] Jerome Di-Battista, Jean-Christophe Courrege, Bruno Rouzeyre, Lione Torres and Philippe Perdu, (2010) “When Failure Analysis Meets Side-Channel Attacks” Proceedings of the 12th international conference on Cryptographic hardware and embedded systems: 188-202.

[19] HyunHo Kim , Ndibanje Bruce , Hoon-Jae Lee , YongJe Choi , Dooho Choi, (2015) “Side Channel Attacks on Cryptographic Module: EM and PA Attacks Accuracy Analysis” Lecture Notes in Electrical Engineering 339:509-516.

[20] Tsunato Nakai, Megumi Shibatani, Mitsuru Shiozaki, Takaya Kubota, Takeshi Fujino, (2014) “Side-channel attack resistant AES cryptographic circuits with ROM reducing address-dependent EM leaks” IEEE International Symposium on Circuits and Systems (ISCAS): 2547-2550.

[21] A. Appari and M. E. Johnson, (2010) “Information Security and Privacy in Healthcare: Current State of Research,” International Journal of Internet and Enterprise Management, 6 (4): 279-314.

[22] DARPA Trust RFI, Draft Trust Program Information, URL: http://www.fbo.gov/spg/ODA/DARPA/CMO/SN06%2D25/listing. html

[23] C. Parshotam, C. Rupinder, G. Aayush, (2012) “Improving the Secure Socket Layer by Modifying the RSA Algorithm” International Journal of Computer Science, Engineering and Applications (IJCSEA), 2(3): 79-86.

[24] Merline, M.A, (2015) “Implementation of triple aes encryption and decryption” International Journal of Applied Engineering Research, 10 (20):18770-18773.