Development of an Innovative Internet of Things Security System

Omar Said

Department of Information Technology, College of Computers and Information Technology, Taif University
Al-Hawiah, Taif, 5700, Saudi Arabia.

Abstract

Recently, the concept of Internet of Things (IoT) has become the most popular term through the widespread of its applications such as greenhouse and telemedicine monitoring. Actually, building IoT systems requires an accurate infrastructure planning. Furthermore, management and security of these systems are considered as the most important challenges facing system developers. Certainly, the IoT security is more than a technical problem as it needs series of regulations and faultless security system for common purposes. So, the study of IoT security problem is an emergent issue to be introduced in a research paper. In this paper, the traditional techniques are studied and evaluated. Accordingly, analysis and design of innovative general purpose system, which protect the IoT resources such as devices and data against hacking or stealing, are proposed. The idea of proposed system is based on adaptation of the traditional algorithms to be compatible with the nature of IoT infrastructure, in addition to combining new techniques with the adapted ones to handle the research problem. Furthermore, an environment to simulate and test the proposed system is constructed. Finally, the results prove that the proposed system is more robust and efficient, which lead us to standardization.

Keywords: Internet of Things, Network Security, QoS, Internetworking.

1. Introduction

Internet of things (IoT) refers to objects (things), which are uniquely identified and using the internet structure. IoT has four major features which are states as follows: sensing, information processing, heterogeneous access, services, and additional features like security and privacy. Recently, the IoT term may be called in other countries as machine-to-machine communications or cyber-physical systems. The architecture of IoT contains a most important data communication tools, which is called Radio Frequency Identification (RFID) in addition to some complex computational items. Another definition of IoT is demonstrated and can be stated as follows; a universal network infrastructure, communicate different types of objects through the utilization of sensing data and communication capabilities. Existing Internet and network tools are embedded in this infrastructure. It will offer specific object identification, sensor, actuator and connection capability as the basis for the development of independent federated services and applications [1].

Regarding the security issue, several challenges obstacle the progress of IoT applications due to the following reasons; 1) extension of IoT to collect recent technologies such as sensor network and mobile network, 2) the internet will comprise the passive and active things, and 3) communicate these things is a must. Upon these natures of IoT, new security problems will arise. More attention to the research for IoT authenticity, confidentiality, and data integrity of data should be considered [2].

This paper proceeds as follows; in Section 2, a problem formulation is demonstrated. In Section 3, related work is introduced. In Section 4, the IoT architecture and the proposed IoT security architecture are defined and discussed. In Section 5, simulation environment is constructed and simulation results are discussed. Finally, the conclusion and the future work are introduced in Sections 6 and 7 respectively.

2. Problem Formulation

Scalability of IoT system lets its security to be an attractive target for most researchers [3], [4]. The security problems of IoT systems are sensor attacks, network content security, unauthorized login, and intrusions. In addition, IoT faces other security obstacles such as information tracking, secure electronic products, and data integrity. The main challenge of the current paper is to find a general solution for these IoT security problems provided that it considers the sensitive nature of IoT architecture (i.e. collection of different network types).

3. Related Work

Xiong Li, et al. proposed in [14] a study of trusted security architecture for IoT. The weak points of this system can be stated as follows; 1) it concerned with a human being, which is not an important factor. The most important factors are IoT data and devices, 2) it demonstrated old security techniques and algorithms, which are not suitable for IoT, and didn’t show an innovative idea, 3) the algorithms and the techniques, which are demonstrated in each system layer, are too large to be executed in the IoT systems. This is due to limited power machines such as sensors and RFID that are considered as the skeleton of IoT systems, 4) in the trusted terminal module; the main requirement is secure operating system. This requirement is not accurate because most of current operating systems are not completely secured, 5) this architecture contains 4 types of agents, which are not identified in details. In addition, how these agents will communicate with each other to accomplish this architecture target is not proposed. Arijit U. et al. proposed in [15] a trail to build security system for IoT. This trail demonstrated threats and problems of low security IoT devices. The system discusses some tools, which may be stolen. These tools can be observed using monitor cars or cameras. This solution can be considered as traditional and did not in line with the nature of IoT because the devices, which are used in the monitoring such as camera, may be hacked or stolen. Kiang Z. et al. proposed in [16] security architecture for the IoT based on multimedia traffic. This trial idea is concerned with the multimedia traffic which is transmitted over IoT. So, it can be considered as a special purpose solution as it can be applicable only for multimedia. In addition, it is based on old and traditional techniques. Furthermore, it's under discussion and not implemented or evaluated so far. GAN G. et al. proposed in [17] a general analysis for IoT security problem. It discusses some general features such as identifying and controlling of sensors remotely. Furthermore, it makes a defense against the Denial of Service (DOS) attacks to sensor nodes. Hui S. et al. proposed in [18] authentication and access control techniques for IoT systems. This trial focused on simple and efficient elliptic curve cryptosystem secure key. In addition, role-based access control authorization method is adapted based on thing’s applications and roles with respect to IoT nature. This authentication system has three drawbacks; 1) it based on old security algorithms, 2) it deals with only system users and not system data or devices, 3) it is considered as a special purpose technique.

4. The Proposed System

To describe the proposed security system, the IoT architecture should be well defined. The IoT consists of three main layers; the application layer, the network layer, and the perception layer. Each layer should be classified into sub-layers to describe what are required in security issue preciously.

In the following subsections, each IoT layer with its sub-layers is clarified. Furthermore, the proposed IoT security architecture is demonstrated

4.1 IoT architecture

The application layer manages two different types of IoT applications; simple and national. Hence, this layer should be divided into two different sub-layers. The first sub-layer is called local, which mean that it comprises local applications. These types of applications manage local domains in the IoT systems such as smart homes, e-health, and e-learning. The second sub-layer is called national, which contains one general purpose application that manages the IoT local applications, which are constructed in the first sub-layer, see Fig. 1. The services of this sub-layer are supervision, translation, and national management. There are many technologies, which should be used to establish the second sub-layer, such as cloud computing, artificial intelligent as well as web technologies.

Regarding the network layer, it comprises the tools, which are used in communication of IoT hardware, such as sensors, mobiles, etc. These tools can be classified into two different types of methodology. The first one is wireless methodology, which contains tools such as wireless sensor networks and mobile communication networks. The second type is wired methodology, which contains tools such as routers and gateways. The management stations can be considered as a network layer component. The reliable data transmissions, quality of services, and connectivity issues are related to this layer, see Fig.1.

For the perception layer, it includes instrumentations, which are used to acquire data from a target environment. These instrumentations are sensors, Infrareds, and Bluetooth. This layer can be classified depending on a type of collected data. Some tools acquire multimedia data and others acquire images. This layer may contain actuator or valves, see Fig. 1.

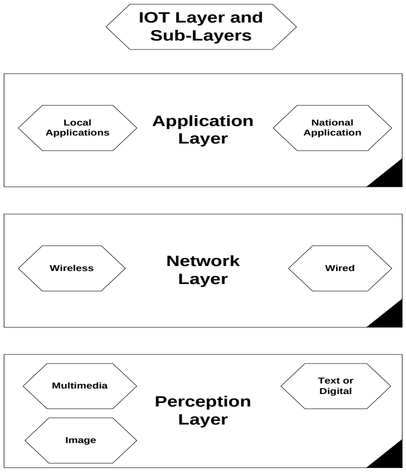

Fig. 1 IoT architecture.

4.2 Proposed IoT architecture

The proposed IoT security architecture can be extracted and clarified from above IoT architecture. So, this IoT architecture is adapted to be in concordance with the security issue. The IoT security architecture consists of six layers; the security application layer, the application layer, the security network layer, the network layer, the security perception layer, and the perception layer, see Fig. 2. In the following subsections, only three layers are clarified because the others are explained in sub-section 4-1.

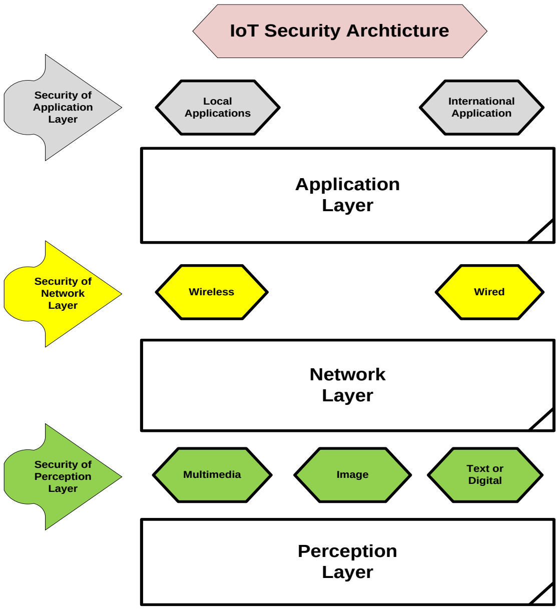

Fig. 2 IoT security architecture.

4.2.1 Security of application layer

This layer is divided into two sub-layers. The first sub-layer is related to a local application security system. For example, intelligent transportation system may use encryption on the other hand smart home system may use stenganography [22]. The second sub-layer is related to national application security system. As stated above, the national application is concerned with management of local ones. Hence, the national application should be well secured. So, its security system should comprise more than one security technique to make sure that sent and received data are secure. Accordingly, there are many security techniques, which may be applied in these types of applications such as selective disclosure, authentication, authorization, intrusion detection, firewall, and antivirus [22]. In this issue, the most important recommendation is the used security techniques in the national application should not conflict with applied security techniques in the local applications.

4.2.2 Security of network layer

Also, this security layer consists of two main sub-layers; wireless and wired. The wireless security sub-layer is concerned with equipments, which communicate IoT applications using wireless channels such as wireless internet, mobile network, and cellular networks. The security techniques, which should be applied in this type of networks, are key distribution, intrusion detection algorithms, identity based authentication, aggregated proofs, and anti-jamming [2]. The wired security sub-layer is related to instrumentations, which communicate the IoT system objects using wired channels. The security techniques, which should be used in this type of networks, are firewalls, router control, resource multiplication, routing flirting, and congestion control [22]. This security layer is an extremely important since it responsible to transmit information among IoT systems' components. In addition, it can be considered as a central unite to store critical information. So, the sensitivity in selection of suitable security technique for each IoT element is target and challenge.

4.2.3 Security of perception layer

The perception security layer consists of three sub-layers, which are classified depending on the gathered data. So, the first sub-layer, which is called multimedia, can use security techniques such as multimedia compression, encryption, time stamps, time synchronization, and multimedia session identifier [22]. The second sub-layer, which is called image, can use image compression, and cyclic redundancy checks [22]. The third sub-layer, which is called text information, can use encryption, compression, and anti-jamming [22]. Since, the perception layer contains tools, which are used to acquire data from a target area, the traditional and straightforward security solution is to put a camera beside IoT perception layer tools. But, the more advanced solution is to make each camera sensor covers other objects beside its original function in the IoT system. Furthermore, there is a tracking system for stolen things should be developed.

5. Simulation and Test

To make sure that the compatibility between the proposed IoT security architecture layers is existed, a simple study should be stated, simulated, and tested. In the following subsections, the simulation environment is described and the simulation results are showed and discussed.

5.1 Simulation environment

The simulation environment contains two high resolution camera sensors for gathering data in multimedia format such as intruder activity, two low resolution camera sensors for gathering data in image format such as intruder image, and two sensors for gathering data in text format such as intruder session time. In addition, three motion sensors, one sensor for each camera sensor. Each type of camera sensor should be distributed among three different areas to detect the intruder in different positions. The simulation supposed that each area is targeted from the intruder. The three camera sensors are communicated in wireless mode using Internet. The gathered data are stored in a local media. Accordingly, these collected data are stored in a central media in another different location. The national management station should access a central storage unite with full authority. The flow of data can be stated as follows, the motion sensor receives the infrared signal from the target object, which moves in a specific area. If this infrared signal became more than a predetermined value, the object is considered as a person and the security system should store his activities. The motion sensor sends a packet contains position axes of this moving person. Hence, its local application sends a packet contains an order to camera sensor(s) for moving directly to a target object depending on its' axes. Accordingly, the camera sensor starts to take a picture or store a video for this person activity and sends it to its local application. The Internet bandwidth determines the type of person activity stored file (video, image, or text). The local application should send a report about this person to the national application alarming the manager to take an action against this intruder. If the intruder moves outside the frame of the cameras, the local application may send copies from the control packet to two or more camera sensors instead of one. The quality of image depends on some parameters such as time of its taken, the resolution of used camera, and the quality of Internet signal, and the environment. The sate of each sensor (i.e. wakeup or sleep) can be determined using the local application depending on importance of coverage area and the powerful level of each sensor. In this simulation, it is supposed that the camera sensor have low level energy, hence the importance of a coverage area is not high. Also, It is supposed that the target environment didn’t have a light and the camera sensors has enough local memory to store a collected data periodically [23], [24], [25], [26], see Fig. 3, and Fig. 4. To simulate this scenario, a handmade code using C++ in addition to MATLAB are used. MATLAB is used to construct a simulation environment for sensors and communication between them [27]. Most of this scenario is supposed to be executed without human intervention.

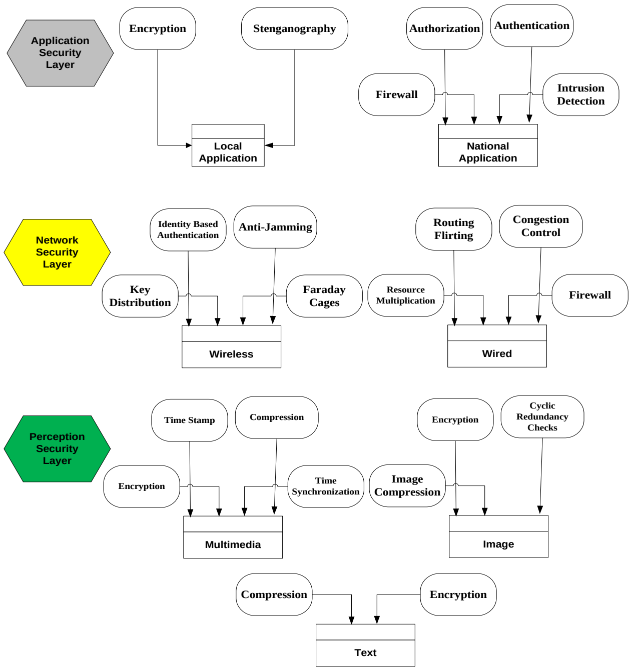

Fig. 3 The suggested security techniques for the proposed IoT architecture layers.

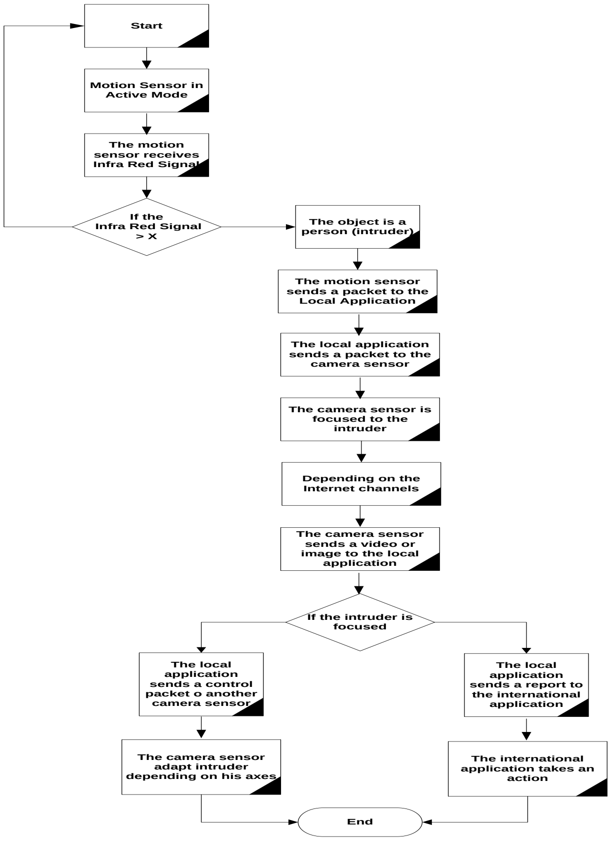
Start
Motion Sensor in Active Mode
The motion sensor receives Infra Red Signal
If the Infra Red Signal > X
The object is a person (intruder)
The motion sensor sends a packet to the Local Application
The local application sends a packet to the camera sensor
The camera sensor is focused to the intruder
Depending on the Internet channels
The camera sensor sends a video or image to the local application
If the intruder is focused
The local application sends a control packet o another camera sensor
The camera sensor adapt intruder depending on his axes
The local application sends a report to the international application
The international application takes an action
End

Fig. 4 The simulation scenario.

5.2 Simulation results

The simulation contains four different parameters, which are stated as follows; the consumption of energy, the cost, the consumption of time, and the accuracy of security. In the following sub-sections, each simulation parameter is described and the results are discussed.

5.2.1 The energy consumption

In this parameter, the energy, which is consumed from the start to the end of a system session, is scaled. The formula, which is used to compute the energy parameter of sensors, is stated in [28]. In our simulation, it is supposed that the transmitted bits from/to the camera sensor is calculated randomly depending on sensor states (active or sleep). The consumed energy should be decreased to increase the time of coverage. Fig. 5 shows the relationship between the energy consumption and the transmission rate within an interval of time. This relation is direct in most time slots (i.e. when the transmission rate increases the energy consumption increases). But, in some time slots such as 5, 13, 10 and 18 the energy consumption is notably decreased. This is due to signal propagation distance and signal obstacles.

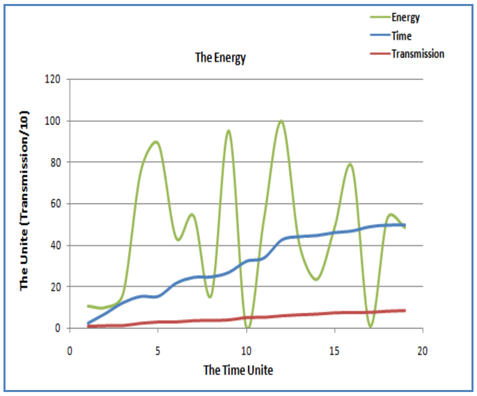

Fig. 5 The energy consumption parameter.

5.2.2 The cost

The cost parameter means how many camera sensors used to cover the intruder within a predetermined interval. Also, a probability of intruder detection for using one or more motion sensor is another factor to scale the cost parameter. The distribution, which is used to determine the camera sensors and motion sensors positions, is Gaussian [29]. The motion of intruder within a specific area is determined by passion distribution [30]. So the cost parameter depends on the motion of the intruder and type of camera sensor. Fig. 6 shows the cost parameter as regards the number of camera sensors, which are used to accomplish the intruder full coverage task. As shown in Fig. 6, if the number of camera sensors increases, the probability of full intruder coverage increases except at points 11, 13 and 16 of axis time unite. Another parameter is used to scale the cost function in the IoT security architecture. This parameter is probability of intruder detection using one or multiple motion sensors. As shown in Fig. 7, probability of detecting the intruder as regards the time unite axis is not stable (i.e. in sometimes low and in other times high). This is due to the distribution, which is used to determine sensors position (Gaussian). The sudden decrease in the probability values in some times is due to the intruder motion that is changed every simulation time periodically.

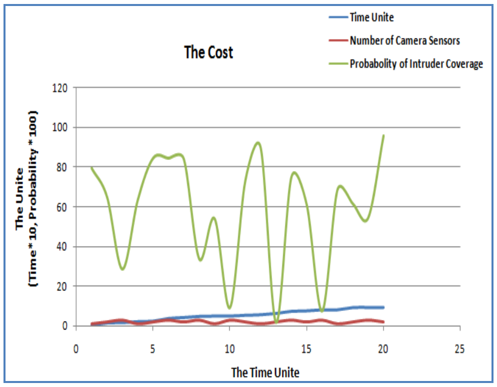

Fig. 6 The cost parameter (number of camera sensors)

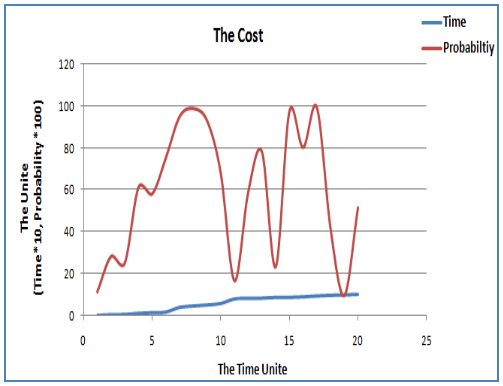

Fig. 7 The cost parameter (probability).

5.2.3 The time consumption

The consumption of time parameter scales interval time from entry of the intruder into his target until the completion of detection process. This time can be scaled using a timer (such as stopwatch in our simulation). This parameter is important in determination of the proposed security system efficiency. Fig. 8 shows that the values of consumed time during simulation intervals are extremely different. This is because different positions of the intruder in the target area make multiple camera sensors should be used to trace and register his activities. In addition, the motion sensor(s) may take a long time to detect this intruder. Using more than one camera sensor represents another consumed time. The management message, which is extracted from the local application, is supposed to be sent to one camera sensor. If this camera sensor can't cover the intruder activities, another message should be extracted from the local application to other cameras which represents additional time.

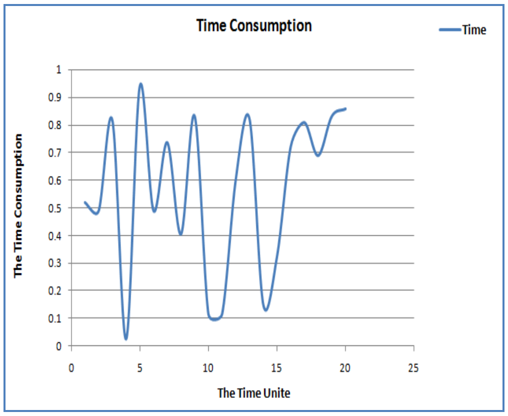

Fig. 8 The energy consumption parameter.

5.2.4 *The security accuracy*

This parameter is considered also as an important parameter to determine the efficiency of the proposed security system. This parameter is calculated by the number of success trials (the number of camera sensors, which are used to detect the intruder is considered) as regards the number of failed trials. Also, the time of intruder detection is an extremely important. Fig. 9 shows accuracy percentage for the proposed IoT security system. The percentage values are located in between 79% and 99%. So, this range can be considered as an accepted result especially under hard restrictions, which are supposed in the proposed simulation environment such as no light in the coverage environment, low number of sensors, and periodically intruder position changing.

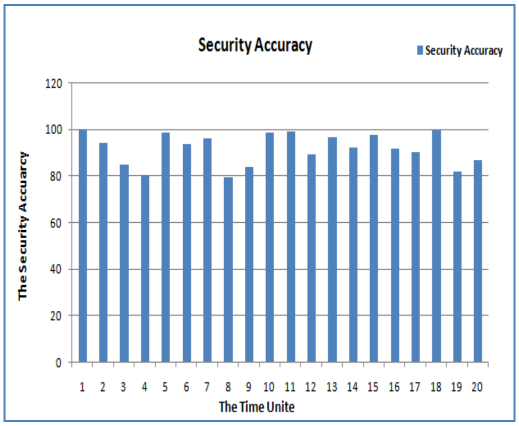

Fig. 9 The security accuracy.

6. Conclusion

In this paper, the architecture of IoT is introduced. Based on this architecture, a new security model for IoT is proposed. The proposed architecture idea is based on accurate determination of suitable security mechanism for each IoT layer. The proposed architecture divided the application layer into two security sub-layers, which are called local and national. The network layer in the IoT architecture is divided into two sub-layers, which are called wireless and wired. The perception layer is divided into three sub-layers, which are called multimedia, image, and text. To test the proposed security architecture, a simulation environment is constructed using MATLAB and handmade C++ code. Four parameters are used to scale efficiency of the proposed system; the energy consumption, the cost, the consumption of time, and the security accuracy. The results showed that the system is efficient under the constructed simulation environment.

7. Future work

More security techniques should be tested in each layer of the proposed architecture to test compatibility. So, in the future, the techniques such as authorization, authentication, and time synchronization will be tested. Also, the simulation environment should be larger (as possible) to provide more accurate results.

References

[1] Luigi A., Antonio I., Giacomo M., The Internet of Things: A survey. Science Direct journal of Computer Networks, Volume 54, Pages: 2787–2805, 2010.

[2] Yinghui H., Guanyu L., Descriptive Models for Internet of Things. IEEE International Conference on Intelligent Control and Information Processing, Pages: 483- 486, Dalian, China, 2010.

[3] Yuxi Liu, Guohui Zhou, Key Technologies and Applications of Internet of Things, IEEE Fifth International Conference on Intelligent Computation Technology and Automation, Hunan China, Pages: 197-200, 2012.

[4] Huansheng N., Ziou Wang, Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework, IEEE Communication Letters, Vol. 15, No. 4, Pages: 461, 2011.

[5] Junwei Lv, 11, Xiaohu Yuan and Haiyan Li, "A New Clock Synchronization Architecture of Network for Internet of Things", International Conference on Information Science and Technology, Pages: 685-688, Jiangsu, China, March 26-28, 2011.

[6] Castro, M. et. al., "Oxygen Cylinders Management Architecture Based on Internet of Things", International Conference on computational science and its applications (ICCSA), Pages: 271-274, Murica, Spain, 2011.

[7] Miao W., Ting L., Fei L., ling S., Hui D., Research on the architecture of Internet of things. IEEE International Conference

on Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China, Pages: 484-487, 2010.

[8] Neil Bergmann, Peter J. Robinson, Server-Based Internet of Things Architecture, 9th Annual IEEE Consumer Communications and Networking Conference, Brisbane, Australia, Pages: 360 – 361, China, 2012.

[9] Jing Liu and Yang Xiao, C. L. Philip Chen, "Authentication and Access Control in the Internet of Things", International Conference on Distributed Computing Systems Workshops, Pages: 588 – 592, Tuscaloosa, AL, USA, 18-21 June, 2012.

[10] Lan Li, "Study on Security Architecture in the Internet of Things", IEEE International Conference on Measurement, Information and Control (MIC), Pages: 374 – 377, Harbin, China, 18-20 May, 2012.

[11] Wei Jiang, Limin Meng, Design of Real Time Multimedia platform and Protocol to the Internet of Thing, IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Pages: 1805 – 1810, Liverpool, United Kingdom, 25-27 June 2012.

[12] ShaoXiwen, "Study on Security Issue of Internet of Things based on RFID", IEEE International Conference on Computational and Information Sciences, Pages: 566 – 569, Chongqing, China, 17-19 Aug. 2012.

[13] Uckelmann, Dieter; Harrison, Mark; Michahelles, Florian, "Architecting the Internet of Things", Springer, 2011. ISBN 978-3-642-19156-5. www.cui-y.cn/.../Linux/Architecting_the_Internet_of_Things.pdf

[14] Xiong Li, Zhou Xuan,Liu Wen, "Research on the Architecture of Trusted Security System Based on the Internet of Things", IEEE International Conference on Intelligent Computation Technology and Automation, Pages: 1172-1175, Shenzhen , China, 28-29 March, 2011.

[15] Arijit Ukil, Jaydip Sen, Sripad Koilakonda, "Embedded Security for Internet of Things", IEEE International Conference on Emerging Trends and Applications in Computer Science (NCETACS), Pages:1-6, Kolkata, India, 4 - 5 March 2011.

[16] Liang Zhou, Multimedia Traffic Security Architecture for the Internet of Things, IEEE Network, Volume 25, Issue 3, Pages: 35- 40, 2011.

[17] GAN Gang, LU Zeyong, Internet of Things Security Analysis, IEEE International Conference on Internet Technology and Applications (ITAP), Pages:1 – 4, Chengdu, China, 2011.

[18] Hui Suoa, Jiafu Wan, Caifeng Zoua, Jianqi Liu, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering, Pages: 648-651, Guangzhou, China, 2012.

[19] Odrigo R., Cristina A., 2011. Key management systems for sensor networks in the context of the Internet of Things. Elsevier, Computers and Electrical Engineering, Volume 37, Issue 2, Pages 147–159.

[20] Shen Bin, Liu Yuan, Wang Xiaoyi, Research on Data Mining Models for the Internet of Things. International Conference on Image Analysis and Signal Processing (IASP), Pages: 127 – 132, Zhejiang, China, 2010.

[21] Shancang Li, Da Xu, and Xinheng Wang, 2012, Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things, IEEE Transactions on Industrial Informatics, Issue: 99.

[22] Huansheng Ning, et al. "Cyberentity Security in the Internet of Things", IEEE computer, Volume:46 , Issue: 4, Pages: 46-53, 2013.

[23] Michael J. , Rush Carskadden, "Threat Implications of the Internet of Things", IEEE 5th International Conference on Cyber Conflict, Tallinn, Pages: 1-12, 2013.

[24] By Jeremy Prince, Brad Klein, Brian Wang, & Kaustubh Jain, "Wireless Sensor Networks Perimeter Security", project. URL:w ww.isr.umd.edu/.../PerimeterWSN –Presentation.pptx.

[25] Urien, P, LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things, IEEE Conference on Consumer Communications and Networking (CCN) , Las Vegas, NV, USA, Pages: 845 – 846, 2013.

[26] Meca, F.V, et al., HIP Security Architecture for the IP-Based Internet of Things, IEEE on Advanced Information Networking and Applications Workshops (WAINA), Pages: 1331 – 1336, Barcelona, Spain, 2013.

[27] MATLAB: http://www.mathworks.com/products/matlab/.

[28] Seung Jun Baek, Minimizing energy consumption in large-scale sensor networks through distributed data compression and hierarchical aggregation, IEEE journal Selected Areas in Communications, Vol. 22, No. 6, Pages: 1130 – 1140, Aug. 2004.

[29] Yun Wang, Weihuang Fu, and Dharma P. Agrawal, "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks", IEEE Transaction on Parallel and Distributed Systems, Vol. 24, No. 2, Feb. 2013.

[30] Maduri Chopde, Kimi Ramteke and Satish Kamble, "Probabilistic model for Intrusion Detection in Wireless Sensor Network", International Journal of Communication Network and Security (IJCNS), Vol-1, Issue-3, 2011.