International Journal of Advanced and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

EXPERIMENTAL RESEARCH TESTBED FOR INTERNET OF THINGS: A SURVEY FROM SECURITY SERVICES PERSPECTIVES

A. H. Azni*, N. H. M. Alwi and K. Seman

Faculty Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia

Published online: 10 September 2017

ABSTRACT

IoT testbed has been continuously on the rise in line with the significant advances of technology in sensor network to provide real-world interconnection. Researchers have developed numerous testbeds for IoT applications with many unique innovations. However, there is still a missing element in the testbed analysis on the security services and its methodologies that can lead to secure IoT application systems. This paper provides a framework to evolving IoT testbeds from the security services perspective, methodology and competency in IoT security which supports and enable multidisciplinary experimentation. Through a comprehensive literature survey of existing IoT testbeds, a set of core security design requirement for IoT security testbed is identified by examining vulnerabilities and attacks at every layer of architecture to get a deep understanding of the security assessment and best practices to conduct IoT security services.

Keywords: internet of things (IoT); security testbed; security service; security requirement for IoT.

Author Correspondence, e-mail: ahazni@usim.edu.my

doi: http://dx.doi.org/10.4314/jfas.v9i3s.20

1. INTRODUCTION

For the last few years the important of IoT testbed has been continuously on the rise in line with the significant advances of technology in sensor network to provide real-world interconnection. However, difficulties associated with the evaluation of IoT application under realistic environment still hamper their maturation. Furthermore, the challenges of security requirements must be address at every layer of technologies [1]. Thus, there is a need for a real-world security testbed for the evaluation of IoT security measures. Given such a testbed, security architecture for IoT can be developed, implemented and evaluated. The development of IoT security testbed is one of the initiatives to design significant infrastructure and methodology, as well as to evaluate security protocols and hardware platform for IoT application under realistic environment.

The aim of this paper is to develop a framework for IoT testbed security architecture with a focus on security services and multidisciplinary experiments. In this paper discusses an overview of security threats and challenges in IoT applications. Furthermore, based on existing architecture, this paper will identify a set of core design requirement for IoT security testbed by examining pragmatic testbed architecture, hardware, software and security services in IoT testbed. Subsequently, the paper will expose existing prominent IoT testbed and examine for each category their designs to get a deep understanding of their approaches and best practices to conduct IoT security services. The security testbed framework is proposed with relevant security assessment methodology and the future works will be discussed in conclusion.

Data in IoT are exposed to security threats and vulnerability that not only conducted by malicious people but accidentally by the users. Furthermore, radical transformations of data by IoT means managing big data and if not well preparation, this will pose unprecedented data privacy and security challenges [2]. Before the framework on IoT security testbed can be proposed, an overview of wide exposures of data and the security risk in IoT applications systems will be discussed.

Potential attacks against IoT fall into three primary categories based on the target of the attack which are attacks against IoT device, attacks against the communication between devices and masters, and attacks against the masters [3]. Fig. 1 describes the three categories of threats and attacks on IoT and its countermeasures. To protect end users and their connected devices, all of these threats and attacks need to be address carefully. Each layer of security requirements in IoT testbed must be imposed security measures to safeguards the data and protection for privacy.

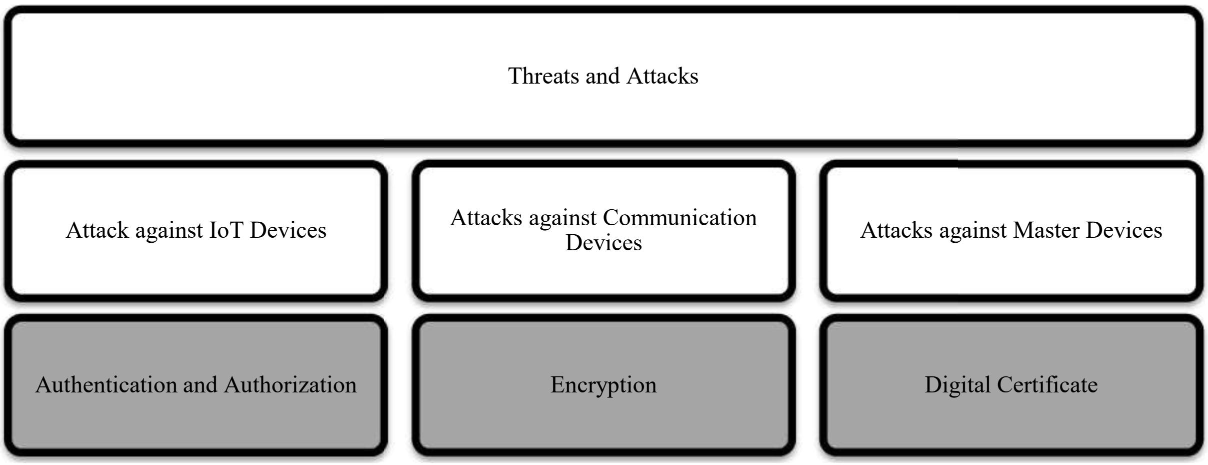
Threats and Attacks
Attack against IoT Devices
Attacks against Communication Devices
Attacks against Master Devices
Authentication and Authorization
Encryption
Digital Certificate

Fig.1. Threats and attacks on IoT

To identify attacks at each pillars security assessment must be performed specifically to a different security principle which are integrity, confidentiality and availability. Table 1 shows analysis of different types of security assessment associate with attacks and threats in IoT applications.

Table 1. Comparative analysis for security testing and requirement

Security Principles	Types of Threats
Integrity	• The breached of a device and its data either partially or entirely typically over a network, hardware or software • Intercepted or modified of network traffic.
Confidentiality	• Disclosure of information in case of interception of communication session. • Unauthorized persons to alter the data and system due to weak physical security procedures.
Availability	• Link or node failure. • Service is lost, either partially or entirely on a temporary or a permanent basis.

2. METHODOLOGY

2.1. Iot Architecture

This section discusses important architecture for IoT security testbed in which the architecture, hardware and software, and testbed security services will be analyzed and determined. The proposed IoT security testbed architecture is developed from the basis of previous testbed development discuss in various research paper [4-8] and it is illustrated in Fig. 2.

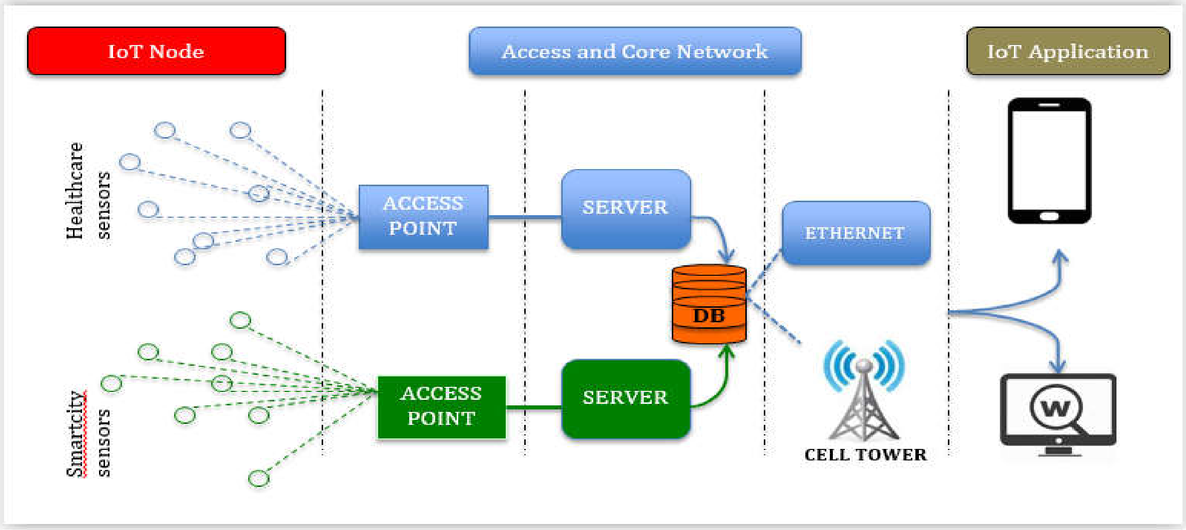

Fig.2. Security IoT architecture

The testbed proposed for IoT is composed of a 3-tier architecture, in which devices of every tier can be freely configured and programmed for experimentation needs to deploy as:

1) IoT node: Responsible for sensing the corresponding parameters (e.g: wireless sensors for healthcare, smartcity and environmental system).
2) Access and core network: Device that collects the measurements from a large number of sensor nodes and uploads all this data to servers through Internet uplink.
3) IoT application: Applications will access resources that are needed to achieve the goal of the business logic through services and also provide services. It can be implemented on a device such as PDA, smart phone or tablet, in an enterprise system or in the cloud.

2.2. Hardware Requirements

The IoT testbed hardware infrastructure consists of a set of testbed nodes which tied within a global networking backbone to provides power, connectivity, in-band and out-of-band signal network capacity for command and monitoring, various servers and database space as described in Fig. 2 [9-12]. Furthermore, Table 2 list technical description of the hardware needed for each tier in mobile IoT testbed.

Table 2. Hardware description for IoT architecture

Tier Level	Hardware Descriptions
Tier 1-Nodes	Sensors, actuator, for healthcare, smart city and environment
Tier 2-Access and Core Network	Access point, server, database server, 3G/cellular tower
Tier 3-Application	PDA, mobile phone

2.3. Software Requirements

The IoT testbed offers full support for embedded software development, which are ranging from direct access, node hardware to operating system (OS) level features where they can leverage the different components, APIs and development environments to build a wide range of applications. Various operating systems (OS) may be run on open nodes, depending on software maturity and node capacity [13]. Two operating systems specifically designed for the IoT: Contiki and TinyOS. Both of them are development tools that include many libraries and provide an IDE for writing operating systems for microcontrollers to be used by the end-devices. Contiki uses the C programming language and TinyOS uses nesC, which is a variation of C.

2.4. Security Testing Tools

Security testing has become an absolutely critical part of any application development strategy. This is due to the increase in the number of privacy breaches that users are facing today. In order to be able to effectively address security testing needs, security service for IoT testbed needed to adopt the latest industry standards and testing methodologies for IoT applications. Security testing objective is to assess the vulnerabilities of entire IoT ecosystem from IoT nodes to network backbone to application devices [14].

Every tier of IoT architecture is exposed to threats and attacks which must be addressed specifically. Thus, security testing tools are needed to perform security assessments such as:

1) Penetration testing tools like Nessus or OpenVAS: Strong physical security methods are applied to protect sensitive data. All physical network devices and access points are tested

for possibilities of any security breach.

2) Spectrum analyzer: the tool needed to measure carrier power level, harmonics, spurious, sidebands, phase noise and more. To help discover unwanted signals and network analyzer helps measure known signals.
3) Packet reconstruction and analyzer: Signal reconstruction to avoid packet loss and error during transmission.

2.5. Embedded Device Security Assessment

Embedded device security assessment service provides an in-depth security assessment to identify physical and logical security threats to the embedded system such as local controllers/gateways and determine risk at the device level of an IoT ecosystem [15]. With that the security assessment can be done through:

Table 3. Embedded device security assessment

Testing Category	IoT Security Assessment
Testing for Insecure Network Services	• Assessment on network services to ensure they do not respond poorly to buffer overflow, fuzzing or denial of service attacks [16]. • Assessment on test ports to ensure its present.
Testing for Poor Authentication/ Authorization	• Assessment for the use of strong passwords where authentication is needed • Assessment for multi-user environments and to ensure functionality for role separation is included. • Assessment for the implementation of two-factor authentication where possible • Assessment for password recovery mechanisms • Assessment for the option to require strong passwords • Assessment for the option to force password expiration after a specific period • Assessment for the option to change the default username and password

Testing for Poor Physical Security	• Assessment on the device to ensure required physical external ports (e.g. USB ports) on the device is utilized. • Assessment on the device to determine whether it can be accessed via unintended methods such as through an unnecessary USB port • Assessment to determine whether it allows to disable an unused physical ports such as USB • Assessment to determine if it includes the ability to limit administrative capabilities to a local interface only

2.6. Wireless Security Assessment

IoT application using wireless IEEE 802.11 signals making it a lot easier for intruders to monitor traffic, disturb the transmission of data and break into the network [17]. This scenario is very worrisome for business with sensitive data for which security is paramount. In order to protect the network, wireless network assessment evaluates the security of the wireless protocols used for local device communication such as ZigBee, 6LoWPAN and Bluetooth LE. The following test in Table 4 are needed to ensure proper implementation and security best practice.

Table 4. Wireless security assessment

Testing Category	IoT Security Assessment
Testing for Lack of Transport Encryption	• Assessment to determine encrypted communication is implemented between devices and between devices and the Internet. • Assessment to determine whether an encryption practices are used up to acceptable level and proprietary protocols are avoided.
Testing for Insufficient Security Configurability	• Assessment to determine whether 20 character passwords security options or two-factor authentication are available • Assessment to determine whether encryption options using AES-256 (where AES-128 is the default setting) are available • Assessment to determine whether security event alerts and

	notifications to the user are available

2.7. Firmware Security Assessment

Anyone who is listening can intercept signal transmission from IoT node to access point or gateways. Within these points, the node nodes and gateway poses two additional threats specifically to IoT devices in which it can automatically download unencrypted and/or unsigned updates and configurations from HTTP-based sources. The first threat to the IoT device is that the contents of updates could be changed or replaced before they get to automatically updating devices. This threat will allow any attacker to run any code that her or she wishes on the device. The defenses against this are to cryptographically sign all updates and to only use HTTPS (or other secure channels), where the identity of the providing server can be cryptographically established [18]. If no encryption algorithm is implemented, any sensitive data sent in updates such as initial or hardcoded passwords or keys can be clearly read. Thus, to countermeasure against this threat is to encrypt updates whenever possible, both in transit and at rest. Thus, firmware security assessment is needed to analyze the security device firmware and its update distribution process to ensure security best practices have been implemented. The best practice which are possible to be implemented such as cryptographically signing firmware updates and using authentication capabilities in hardware devices to verify signatures. Table 5 below details out the assessment need for firmware security.

Table 5. Firmware security assessment

Testing Category	IoT Security Assessment
Testing for Insecure Software/Firmware	• Assessment of the device to ensure the update capability is implemented and can be updated quickly when vulnerabilities are discovered. • Assessment of the device to ensure encrypted update files are used and that the files are transmitted using encryption algorithm. • Assessment of the device to ensure signed files is used and then validates that file before installation.

Testing for Insecure Mobile Interface	• Assessment of the mobile interface to ensure whether it allows weak passwords. • Assessment of the mobile interface to ensure whether it includes an account lockout mechanism. • Assessment of the mobile interface to determine whether it implements two-factor authentication. • Assessment of the mobile interface to determine whether it uses transport encryption algorithm. • Assessment of the mobile interface to determine whether to require strong passwords option is available. • Assessment of the mobile interface to determine whether to force password expiration after a specific period option is available.

2.8. Application Security Assessment

Anyone who is listening can intercept signal transmission from IoT. IoT applications can be categorized into three basic applications which are:

- Mobile or desktop applications that control IoT devices;
- IoT firmware and embedded applications;
- Applications on open IoT platforms (for example, apps built for Apple Watch).

The overall goal of IoT application security testing is to uncover software vulnerabilities, demonstrate the impact of weaknesses, and provide recommendations for mitigation. All of the applications need to be protected or the risk of undesirable outcomes will occur. Applications can be attacked in many ways. In the case of an IoT solution involving a desktop or mobile app that monitors or controls the device, often all the attacker needs to do is obtain access to the application and tamper with it to do what they want with the device. IoT Application must also involve privacy concern from users. Table 5 details out the assessment need for application security.

Table 6. Application security assessment

Testing Category	IoT Security Assessment
Testing for Privacy Concern	• Assessment to determine the number of personal information collected. • Assessment to determine whether collected personal data is properly protected using encryption algorithm at rest and in transit. • Assessment to determine whether ensuring data is anonymised. • Assessment to ensure end-users are given a choice for data collected beyond what is needed for proper operation of the device.

3. RESULTS AND DISCUSSION

Security will be a major concern wherever systems are deployed at large scale. There can be many ways the system could be attacked either by accessing personal information; pushing erroneous data into the network; disabling the network availability; etc. These can be categorized based on the specific layer in IoT architecture. The specific properties of IoTs lead to special attacks as well as new challenges for countermeasure development [19]. The proposed security assessment framework based on the security services and assessment in this mentioned in this section. Fig. 3 shows the framework of the security testbed.

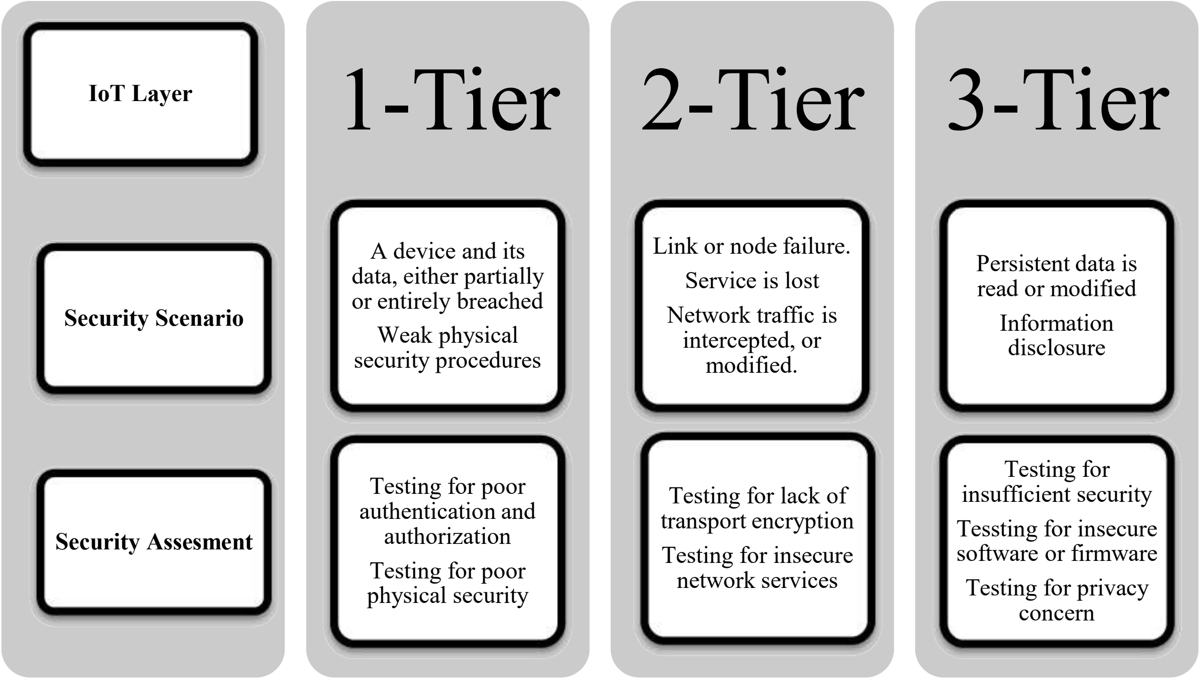
IoT Layer
Security Scenario
Security Assesment
1-Tier
A device and its data, either partially or entirely breached
Weak physical security procedures
Testing for poor authentication and authorization
Testing for poor physical security
2-Tier
Link or node failure.
Service is lost
Network traffic is intercepted, or modified.
Testing for lack of transport encryption
Testing for insecure network services
3-Tier
Persistent data is read or modified
Information disclosure
Testing for insufficient security
Tessting for insecure software or firmware
Testing for privacy concern

Fig.3. Security assessment framework

The three physical layers of IoT are vulnerable to specific attacks at each layer. Thus, security is critical to any IoT. From the three layers, the first IoT layer seems to be the most vulnerable as it allows person tracking as well as the objects and no high level intelligence can be enabled on these devices [20]. At this layer, encryption algorithm can be the best solution against outsider attackers which can partially or entirely breach the devices. Encryption ensures data confidentiality, whereas message authentication codes ensure data integrity and authenticity [21]. IoT devices are assumed to be trusted or uncompromised may have elevated or otherwise enhanced access to an environment or system. If this is the case, then careful consideration needs to be given to the implications if one or more devices were compromised. Thus, at this layer, testing against authentication and authorization as well as testing for poor physical security must be assess carefully. The assessment covers the use of strong passwords, password recovery mechanisms and to determine if it allows to disable unused physical ports such as USB.

Security in the core network is another important area of which will need more attention. Along with the presence of the data and tools available, core networks and Internet backbone of IoT which will make a bigger threat from attackers. This layer performs communication between two layers via transport protocol to determine the use of encrypted communication between devices and between devices and the Internet. The security assessment needed to determine if accepted level of encryption practices are used and also whether a proprietary protocol is avoided. The security assessment also needed to determine if a firewall option is available.

Application devices are expose to personal information such as name, address, date of birth, weight etc. Exposure of this personal information is of concern, given the account enumeration issues and use of weak passwords on the systems. Application security assessments will validate the security requirements by identifying known vulnerabilities and by providing risk identification, consequences of exploitation and expert guidance and recommendations of what the developer should specifically do to improve the overall security posture of an application.

4. CONCLUSION

The proposed IoT security testbed provides researchers and developers with the ability to run experiments using potentially security testing tools and assessment on an isolated experimental network. The IoT security testbed also focus to the activity for a community of academic, industry, and government researchers who want to assess the security of their systems before it can be fully implemented. The support for testbed users includes a repository of attack traffic generators, monitoring tools, topology generators and other tools are needed to integrate these tools into an experimenters' testbed which will simplify the task of getting new experiments up and running. The testbed provides an environment that makes experiments more readily repeated and validated by others, and serves as a repository for the data and hardware and software configurations used for experiments.

5. ACKNOWLEDGEMENTS

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) for the support and facilities provided. This research paper is supported by Fundamental Research Grants No: FRGS/2/2014/ICT03/USIM/02/1.

6. REFERENCES

[1] Atzori G, Iera L, Moraboti A. The internet of things: A survey. Computer Networks, 2010, 54(15):2787-2805

[2] Webber R H. Internet of Things-New security and privacy challenges. Computer Law and Security Review, 2010, 26(1):23-30

[3] Demblewski M. Security frameworks for machine-to-machine devices and networks. Phd thesis, Florida: Nova Southeastern University, 2015

[4] Luis S. SmartSantander: IoT experimentation over a smart city testbed. Computer Networks, 2014, 61:217-238

[5] Fernandes J, Nati M, Loumis N S, Nikoletseas S, Raptis T P, Krco S, Rankov A, Jokic S, Angelopoulos C M, Ziegler S. IoT Lab: Towards co-design and IoT solution testing using the crowd. In IEEE International Conference on Recent Advances in Internet of Things, 2015, pp. 1-6

[6] Gluhak A, Krco S, Nati M, Pfisterer D, Mitton N, Razafindralambo T. A survey on facilities for experimental internet of things research. IEEE Communications Magazine, 2011, 49(11):58-67

[7] Nati M, Gluhak A, Abangar H, Headley W. Smartcampus: A user-centric testbed for internet of things experimentation. In 16th IEEE International Symposium on Wireless Personal Multimedia Communications, 2013, pp. 1-6

[8] Gubbi M, Buyyu J, Marusic R, Palaniswami S. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 2013, 29(7):1645-1660

[9] Baccelli T C, Hahm E, Gunes O, Wählisch M, Schmidt M. RIOT OS: Towards an OS for the Internet of Things. In IEEE Conference on Computer Communications Workshops, 2013, pp. 79-80

[10] Xu M T, Wendt J, Potkonjak B. Security of IoT systems: Design challenges and opportunities. In IEEE/ACM International Conference on Computer-Aided Design, 2014, pp. 417-423

[11] Babar R, Stango S, Prasad A, Prasad, Sen N, Prasad J. Proposed embedded security framework for internet of things (IoT). In 2nd IEEE International Conference on Wireless

Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, 2011, pp. 1-5

[12] Said M, Masud O. Towards internet of things: Survey and future vision. International Journal of Computer Networks, 2013, 5(1):1-17

[13] Haque M, Pawlikowski K, Ray S. Challenges to development of multipurpose global federated testbed for future internet experimentation. In 9th IEEE/ACS International Conference on Computer Systems and Applications, 2011, pp. 289-292

[14] Abie H, Balasingham I. Risk-based adaptive security for smart IoT in eHealth. In 7th International Conference on Body Area Networks, 2012, pp. 269-275

[15] Kim H, Hong W, Yoo J, Yoo S. Experimental research testbeds for large-scale WSNs: A survey from the architectural perspective. International Journal of Distributed Sensor Networks, 2015, 2015:1-18

[16] Whitehouse O. Security of things: An implementers' guide to cyber-security for internet of things devices and beyond. Manchester: NCC Group, 2014

[17] Mohammed F H, Esmail R. Survey on IoT Services: Classifications and applications. International Journal of Science and Research, 2015, 4(1):2124-2127

[18] Raza S, Duquennoy S, Hoglund J, Roedig U, Voigt T. Secure communication for the Internet of Things a comparison of link-layer security and IPsec for 6LoWPAN. Security and Communication Networks, 2014, 7(12):2654-2668

[19] Yu Y, Li K, Zhou W, Li P. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and computer Applications, 2012, 35(3):867-880

[20] Chew G P. Protecting privacy in an IoT-Connected world. Information Management, 2015, 49(6):36-39

[21] Kumar S N. Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 2015:3(1):1-11

How to cite this article:
Azni AH, Alwi NHM, Seman K. Experimental research testbed for internet of things: a survey from security services perspectives. J. Fundam. Appl. Sci., 2017, *9(3S), 231-244.*