Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework

Abdul Fuad Abdul Rahman
National Vulnerability Assessment Centre, (MyVAC)
CyberSecurity Malaysia,
Selangor, Malaysia
+60 17 281 5949
abdfuad@cybersecurity.my

Maslina Daud
CyberSecurity Proactive Service (CSPS) Division
CyberSecurity Malaysia,
Selangor, Malaysia
maslina@cybersecurity.my

Madihah Zulfa Mohamad
MyCyberSecurity Clinic (MyCSC)
CyberSecurity Malaysia,
Selangor, Malaysia
+60 12 634 6904
madihah@cybersecurity.my

ABSTRACT
The Internet of things (IoT) refers to every object, which is connected over a network with the ability to transfer data. Users perceive this interaction and connection as useful in their daily life. However any improperly designed and configured technology will exposed to security threats. Therefore an ecosystem for IoT should be designed with security embedded in each layer of its ecosystem. This paper will discussed the security threats to IoT and then proposed an IoT Security Framework to mitigate it. Then IoT Security Framework will be used to develop a Secure IoT Sensor to Cloud Ecosystem.

Keywords
Internet of Things (IoT), Information Security, Framework, Security Threats, IoT Ecosystem

1. INTRODUCTION
The Internet of Things (IoT) can be defined as a pervasive and ubiquitous network that enables monitoring and control of the physical environment by collecting, processing, and analyzing the data generated by sensors or smart devices [1]. Internet of Things (IoT) envisions that everything in the physical world can be connected seamlessly through Internet infrastructure. When things react to the environment, data will be sensed and captured by sensors and transmitted to the Internet. The potential of IoT is huge and can be applied ranging from not only automated home appliances but also smart grids, smart cars, smart manufacturing, and healthcare.

By the year of 2020 Gartner forecasts that 26 billion units of connected devices will deliver an overall global economic value add of US$1.9 trillion, of which 80 percent will be derived from IoT services [2]. The same forecasts shared by Ericsson, however Ericsson predicts 50 Billion Connected Devices by year 2020 [3].

ICC '16, March 22-23, 2016, Cambridge, United Kingdom

DOI: http://dx.doi.org/10.1145/2896387.2906198

The exponential growth is not drive by the human population alone. The evolution of ICT has lead us to live and set in an environment moving towards ubiquitous and mobility of Internet connection. Today most things around us are connected with active information interactions through Internet. The era of interconnected things, where machine talking to other machine is already here, and known as the era of Internet of Things (IoT).

However, findings from TRUSTe Internet of Things Privacy Index reveals that the United Kingdom (UK) consumers' comfort levels varied widely depending on responsibility, ownership and usage of collected personal data. Privacy and security concerns along the information supply chain will be a potential barrier to the growth of the IoT market as only 18 percent of respondents agreed that the benefits of smart devices outweighed any privacy concerns [4]. Although the findings do not represent all consumers around the world but it shows that consumers are concerned about their privacy and security.

The wide exposures of data on the Internet actually poses security risk. Most IoT device or system is exposed to any Information security threats and vulnerability if the IoT device or system is not properly secured. This pose unprecedented data privacy and security challenges to develop secure IoT Ecosystem.

2. IoT ECOSYSTEM
According to Tarkoma and Katasonov (2011), IoT represents a global network and service infrastructure of variable density and connectivity with self-configuring capabilities based on standard and interoperable protocols and format that consists of heterogeneous things that have identities, physical and virtual attributes and are seamlessly integrated into Internet [5].

A typical IoT system consists of IoT Sensor Nodes or IoT Devices connected to the IoT system through a Base Station. IoT Sensor Node is a transducer whose purpose is to sense, detects events, changes in quantities and provides a corresponding output in electrical signal.

Base Station is usually setup as the IoT Sensor Nodes Gateway and can be installed can configured in a Personal Digital Assistant (PDA), or Tablet PC, or Smartphone, or Phablet or Laptop and in some cases, a third party database through small devices attached to belt, or wristband etc. is being used according to Farhana et. al. (2009) [6].

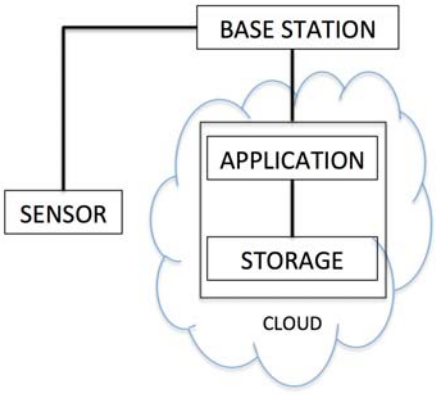

Figure 1. Typical IoT Ecosystem

The Base Station connects the IoT Sensor Nodes to the IoT system. In this paper, the IoT System is configured inside a Cloud system. Nowadays all system applications, web application, storage, and database can be configured in a Cloud system. Therefore a typical IoT ecosystem can be summarized into a process flow as shown in Figure 1.

Gartner divided IoT Ecosystem into 5 different layers [2]. Layer 1 represents Things consists of all IoT Sensor Nodes and devices. Layer 2 represents Communication and Network. Layer 3 represents Computing and Storage. Layer 4 represents Application and Services and Layer 5 represents Analytics [2]. However, as previously discussed, nowadays all system applications, web application, storage, and database can be configured in a Cloud system, this paper choose to simplify and therefore combine Layer 3 and Layer 4 as a single layer as shown in Figure 2.

Figure 2. 4 Layers of IoT Ecosystem

3. SECURITY THREATS ON IoT

As discussed earlier, if each IoT Layers are not properly configured, the IoT devices and system might expose to the security threats. The vulnerabilities appear in all code from time to time and this includes compromise of device, infrastructure, network and interface.

According to HP, the current state of IoT security seems to take all the vulnerabilities from existing space, such as network security, application security, mobile security, and Internet connected devices, and combine them into a new (even more insecure) space [7]. Furthermore, based on their study, 90% of IoT devices collected at least contains one personal information [7]. 80% of devices along with their cloud and mobile application components failed to require password of a sufficient complexity and length [7]. 70% of IoT devices did not encrypt communications to the Internet and local network [7]. 70% of IoT devices along with their cloud and mobile application enable an attacker to identify valid user account through account enumeration techniques [7]. 6 out of 10 IoT devices that provide user interfaces were vulnerable to a range of issues such as persistent Cross Site Scripting (XSS) [7].

A research conducted by Researchers from CyberSecurity Malaysia (CSM) identifies that IoT devices and system is heavily dependent on wireless and cellular network [8]. This indirectly expose the IoT system to the same security threats faced by wireless and cellular network. Recent research work by Rahman and Mohamad (2014), shows that IoT system using WBAN sensor can be exploited to compromise Confidentiality, Integrity and Availability (CIA) of the IoT System [8]. During the study it was discovered that IoT System is vulnerable to Eavesdropping, Denial of Service (DoS), Authentication Bypass and Role Bypass [8]. The study concluded that major challenge is to deploy advanced security mechanism into IoT device which is characterized with constrained memory, power and processing capability [8].

OWASP Internet of Things Top Ten Project listed the security issues and impact related to IOT includes Insecure Web Interface, Insufficient Authentication/Authorization, Insecure Network Services, Lack of Transport Encryption, Privacy Concerns, Insecure Cloud Interface, Insecure Mobile Interface, and Insufficient Security Configurability as shown in Table 1 [9].

Table 1. Common IoT Security Threats

Category	Description
Insecure Web/Cloud/ Mobile Interface	Examples of such risks include, API dependencies, limited monitoring/logging capabilities, inflexible access controls, anonymous access, reusable tokens/ passwords, clear-text authentication and/ or transmission of content, and improper authorizations.
Insufficient Authentication/ Authorization	It occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate
Insecure Network Services	Secure network services may be susceptible to buffer overflow attacks or attacks that create a denial of service condition
Lack of Transport Encryption	Allows data to be viewed in plaintext as it travels over networks or the internet
Privacy Concerns	Lack of privacy means that the IoT system has lack of ability to secluded itself therefore exposing

Insufficient Security Configurability	Insufficient security configurability is present when users of the device have limited or no ability to alter its security controls.
Insecure Software/ Firmware	Software/Firmware should be embedded with security during its development, improper secure coding will result in insecure software and firmware
Poor Physical Security	Sensor are most susceptible to physical theft and therefore has a very low physical security protection

4. DEVELOPING IoT SECURITY FRAMEWORK

4.1 IoT Security Approach

Since IoT will consists a complex infrastructure from sensors to cloud, the challenge to cybersecurity is to choose which area to be secure first and worth invested in. Any approach taken should consists and cover all angle of IoT components and the most important is that the approach is easy to implement. If the developed security approach is too complex, it will be extremely difficult for other organizations to implement it. Any security approach should be easy to implement so that organizations can use it as the guideline for measuring how well their IoT system are secured. Therefore, it is important to know all the IoT security requirements before designing a security approach.

4.2 Security Requirements for 4 Layers of IoT Ecosystem

As discussed in previous section, this paper chooses to presents IoT Ecosystem in 4 Layers. Layer 1 Things Layer, Layer 2 Communication Layer, Layer 3 Infrastructure Layer and Layer 4 Data Analytics Layer. Each Layer has its own security requirements as shown in Table 2.

Table 2. The IoT Security Requirements

Layer	Security Requirements
Layer 1: Things Layer	• Secure Localization in order to protect sensor nodes from unauthorized tracking and enhance its physical security [10]. • Trusted Sensor Nodes is needed to protect data authenticity and integrity [10]. • Access Control to provide access level to user and administrator of the IoT system [10]. • Strong Authentication and Authorization is needed to authenticate authorized user only and prevent unauthorized access [10]. • Secure IoT Platform is needed to protect IoT system from malicious code and malware [10]. • Operating System (OS) Security is needed to protect IoT system from malicious code and malware [10].
Layer 2: Communication Layer	• Network Security is needed to seclude IoT communication from eavesdropping [10]. • Secure Machine-to-Machine (M2M) Gateway is needed to secure IoT communication from Sensor Nodes to Cloud [10]. • Secure Tunnel/ Data Encapsulation is needed to seclude IoT communication from eavesdropping [10]. • Communication Encryption is needed to seclude IoT communication from eavesdropping [10]. • Wireless Protocol is needed to seclude IoT communication from eavesdropping [10].
Layer 3: Infrastructure Layer	• Web/Web Application Security is needed to protect IoT system from malicious code and malware [10]. • Cloud Security is important because it will not only host IoT System but also IoT storage, IoT infrastructure and cloud service such as SaaS PaaS NaaS IaaS MaaS CaaS and XaaS [10]. • Secure Software Development Life Cycle (SSDLC) is needed to protect IoT system from malicious code and malware [10]. • Secure Platform is needed to protect IoT system from malicious code and malware [10]. • A Periodic Security Assessment conducted on quarterly basis will reduce the amount of security threats towards IoT system [10]. • Secure Middleware is needed to protect IoT system from malicious code and malware [10]. • Secure Storage is needed to protect IoT system from malicious code and malware, data leakage and also from unauthorized user access [10].
Layer 4: Data Analytics	• Big Data Management is needed to organized huge amount of data obtained from IoT system [10]. • Big Data Analysis will provide more accurate analysis, uncover hidden patterns and unknown correlations [10]. • Predictive Analysis will provide more accurate analysis on future security threats [10].

4.3 IoT Security Framework

Based on Dong et. al. (2015), in order to develop a secure IoT Ecosystem, the IoT Components should consider both technical and management perspective [11]. However, Jung et. al. (2013) states that to develop an integrated security mechanism specifically designed for IoT is a big challenge because of the diversity of the IoT system itself [11]. Jung (2013) suggests to approach IoT Security with multiple security mechanism and recommend to evolves from the notion of security mechanism to the notion of security management [12].

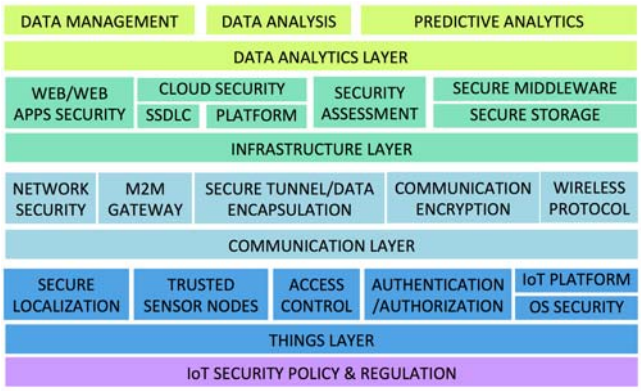

Figure 3. IoT Security Framework

In this paper, the IoT security will be approach by developing IoT Security Framework based on the 4 Layers of IoT Ecosystem. This paper chooses to approach the IoT security by developing a framework because a framework is one of the tools that are available to help organization secure their IoT system better and faster. A framework provides organization with the certainty that they are developing an application that is in full compliance with the IoT security requirements, that is organized and structured, and that is both maintainable and upgradable. Framework also allows developers to save time by reusing generic modules in order to focus on other areas. While not technology specific, the framework will focus on incorporating security management and technical requirements of each layer. Based on the IoT security requirements listed in previous section, the IoT Security Framework will be design based on 4 Layers of IoT Ecosystem as shown in Figure 3.

5. SECURE IoT SENSOR TO CLOUD ECOSYSTEM

In this section, all the discoveries in the previous sections will be translated into a secure IoT Sensor to Cloud Ecosystem that have the ability to withstand internal and external attacks. From previous section, a typical IoT Ecosystem consists of IoT Sensor Nodes, Base Station and Cloud will be merge with the IoT Security Framework thus produce a Secure IoT Sensor To Cloud Ecosystem as shown in Figure 4. All the components for Secure IoT Sensor To Cloud Ecosystem details listed in Table 3.

Table 3. The IoT Security Requirements

Layer	Component	Description
1	IoT Sensor Node	The IoT Sensor Node has the secure localization capability and capable of sampling, processing, and communicating multiple data, sent its data to the Base Station through secure and encrypted communication. The Sensor Nodes should be develop using secure coding approach.
	Base Station	The Secure Base Station is develop with secure coding for its application, act as a secure gateway, and capable of sending data through an encrypted communication to the cloud.
2	Network	The network is encrypted from end to end (sensor to cloud) preventing eavesdropping and the IoT network also should be include network segregation, which separated from other corporate network.
	Wireless Protocol	The lightweight wireless protocol should be able to accommodate sufficient cryptography requirements such as power consumption and processing memory. For example Zigbee and RFID.
	Tower	Secure Telecommunication Tower for cellular communication should include physical security and also the capability to prevent eavesdropping
3	Cloud	Cloud security has the ability to authenticate authorized user only with sufficient Access Control to avoid privilege escalation. Secure SDLC should be include in order to secure software running inside the cloud system.
	Storage	Secure storage should be able to prevent unintended data leakage and should be encrypted
4	Data Analytics	Big data analytics should be able to prevent unintended data leakage and should be encrypted

The Figure 4 shows the proposed Secure IoT Sensor to Cloud Ecosystem, which consists of secure components as listed in Table 3. Table 3 discussed all the requirements needed for each component in each IoT layers in order to produce a Secure IoT Sensor to Cloud Ecosystem. It is recommended that the Secure IoT Sensor to Cloud Ecosystem to be researched and enhanced in future research in order to create a comprehensive security solution for IoT.

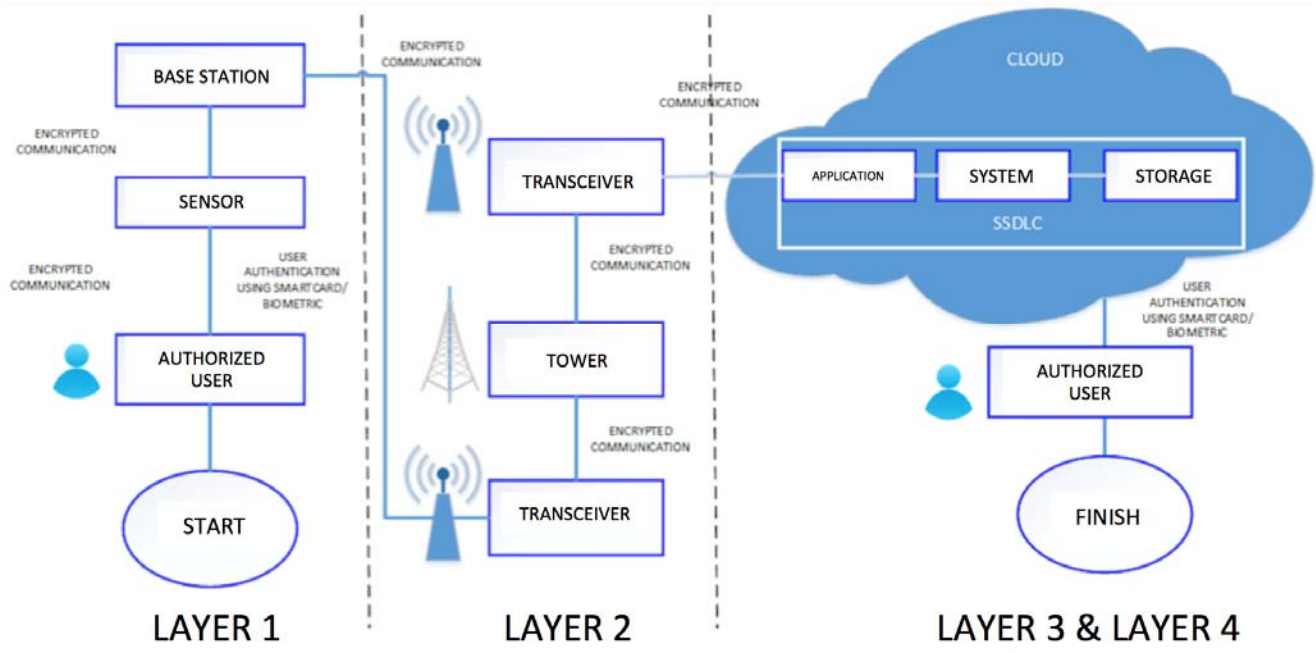

Figure 4. Secure IoT Sensor to Cloud Ecosystem

6. CONCLUSION

The idea of combining all security requirements before developing a secure network architecture and ecosystem was adopted by the recent research of developing Secure Network Architecture for WBAN by Rahman et. al. (2014). The security requirements for each IoT layers listed in the previous section was successfully merged to developed the IoT Security Framework. The objective of this paper to convert the IoT Security Framework into the Secure IoT Sensor To Cloud Ecosystem was successfully achieved. It is recommended for future research to adopt the IoT Security Framework to develop new security solutions for IoT.

7. ACKNOWLEDGMENTS

The authors would like to thank all the reviewers for their helpful comments. We also would like to thank the CyberSecurity Malaysia, an Agency under Ministry of Science Technology and Innovation Malaysia (MOSTI) for their contribution.

8. REFERENCES

[1] Anderson, C. R. 2014. The internet of Things: The possibilities are endless, but how will we get there?. IDC APeJ Internet of Things Web Conference on 19 June 2014.

[2] Prentice, S. 2014. “The Five SMART Technologies to Watch”, Gartner

[3] Higginbotham, S. 2011. Ericsson CEO Predicts 50 Billion Internet Connected Devices by 2020. Ericsson. DOI at: http://gigaom.com/2010/04/14/ericsson- sees-the-internet-of-things-by-2020/

[4] Davies, J. 2014. “Internet of Things crisis? Privacy issues could be barrier to smart-device take-up, says Ipsos Mori report”.

[5] Tarkoma, S., Katasonov, A.: Internet of Things Strategic Research Agenda. Finnish Strategic Centre for Science, Technology and Innovation. 2011.

[6] Farhana T. and H. Islam. 2009. Wearable Wireless Body Area Networks. Proceedings of the Information Management and Engineering, (ICIME ’09).

[7] Hewlett Packard (HP), Internet of Things Research Study. 2015. DOI: http://www8.hp.com/h20195/V2/GetPDF. aspx/4AA5-4759ENW.pdf

[8] Rahman A.F.A and Mohamad M. Z. 2015. Developing the Security Zone for Wireless Body Area Network (WBAN) Implementation Using Practical Security Assessment (PSA). Journal of Advance Computer and Network (JACN).

[9] Open Web Application Security Project (OWASP) IoT Top Ten Vulnerabilities. 2014. DOI https://www.owasp.org/ images/ 7/71/Internet_of_ Things_Top_Ten_2014-OWASP.pdf

[10] Kumar J. S. and Patel D. R. 2014. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications. Vol. 90. No. 11.

[11] Dong H.K. Ji Y. C., Sungjun K. and Jongin L. 2015. A study of Developing Security Requirements for Internet of Things. Advances Science and Technology Letters. Vol 87.

[12] Jung T. K. 2013. Analyses of Integrated Security Framework with Embedded RFID System for Wireless Network Architecture. Journal of Convergence Information Technology Vol 8. No. 14 2013.