全球商業經營管理學報
第九期　106.09　page 121-133
ISSN：2076-9474

無線區域網路物聯網資訊安全研究

A Study of Information Security of Internet of Things in WLAN

馬維銘[a]

摘要

利用物聯網（IoT）可以改善人們的生活品質，具有自我意識的物件可以形成智慧型環境和空間，將可以大幅提升人類的生活福祉。但是，目前物聯網裝置具有資訊安全的弱點，包括：運算能力較低、能源需求低、較不可靠的無線通訊管道特性以及實體漏洞。若物聯網資訊安全遭駭客惡意破壞，可能會對人類的生存造成威脅。本研究旨在探索和實作物聯網資訊安全架構，以解決物聯網系統許多特性因素所形成的資訊安全弱點。本研究以建構適用於區域醫療照護物聯網資訊安全系統的架構為例，達到解決高複雜度物聯網資訊轉換系統和無線安全問題的目標。

關鍵字：物聯網、IoT、資訊安全、無線網路安全

ABSTRACT

Utilizing Internet of Things (IoT) can improve the quality of human life, these smart environments and spaces and self-aware things will largely contribute to the improvement of the general population’s wellbeing. But the information security vulnerabilities of the IoT devices include the low computing capabilities, low energy requirements, the unreliable nature of the wireless channel, and physical vulnerability. Hackers malicious damage to IoT information security, may be a threat to people's lives. This study is to explore and practice of an architecture of information security of IoT to solve many volubility’s caused by the natures of the IoT system. An architecture-oriented of the information security of IoT applied to healthcare in local area was built up. This research reach the goals of resolving some problems of high complexity of information transitions System of IoT and wireless Security.

Key words: Internet of Things, IoT, Information Security, Wireless Security

1. Introduction

In this chapter the Research Background, Research Goal and Research Method are described.

1.1. Research Background

As a new wave of Internet-enabled technologies arrive, it is imperative to understand fully the security and privacy concerns (Thierer, 2015). Currently, there is a lack of guidance for securing IoT, IoE, and WoT as a cohesive unit (Dawson, 2016). There are several investigations done in the domains of IoT enabling technologies, applications, protocols, and security and privacy issues. The information security vulnerabilities of the IoT devices are including the low computing capabilities, low energy requirements, the unreliable nature of the wireless channel, and physical vulnerability (Eltayeb, 2017).

The IoT is more than 13 billion units of interconnected digital, electronic equipment in the world, and the active development of areas of agriculture, life, information, manufacturing, logistics, and transportation. The challenges of the IoT are: the cost of internet of everything, the respective network systems are interconnected, understanding between information and event, information security challenges, and better business applications. Just like networked information systems played a fundamental role in the transformation of almost every business, connected objects will fundamentally change the design of most industrial and automation processes. The Internet emerged as the information backbone interconnecting all information systems, and the

[a] 正修科技大學資訊管理系副教授 Email: 3666@gcloud.csu.edu.tw

Internet of Things is now emerging as the backbone interconnecting all objects.

Chellappan and Sivalingam (2016) studied the IoT revolution is expected to drive change in our society in an unprecedented way. They summarized recent research results in the area of IoT security. It emphasizes the challenges of privacy and security in IoT. The discussion considers open challenges in security and data privacy such as (1) scale and constrained network elements, (2) privacy in data collection as well as data sharing and management, and (3) identity management and authentication.

1.2. Research Goal

The purpose of this study is to explore and practice of construct an architecture-oriented of methodology for Information Security of Smart Healthcare Cloud Applications and Services IoT System (ISSHCASIS) to solve many difficulties caused by the process-oriented approach to the same system. This research will reach the goals of resolving the problem of high complexity of information transitions system of IoT, high cost of development, and low expandability of system.

1.3. Research Method

Enterprise architecture is complex that it comprises multiple views such as strategy, version, goal, object, concept, analysis, design, implementation, structure, behavior and input/output data views. Accordingly, an enterprise is defined as a set of interacting components forming an integrated whole of that enterprise’s multiple views. Structure-Behavior Coalescence (SBC) results in the coalescence of multiple views. Therefore, it is concluded that the SBC architecture is so proper to model the multiple views of an architecture enterprise. Therefore, the SBC architecture is used to model the ISSHCASIS meet their objectives. Those engaged in business analysis are charged with identifying the activities that enable the enterprises to define the business problem or opportunity, define what the solutions looks like, and define how it should behave in the EC website.

2. Literature Reviews

The previous studies about Definition of IoT, the IoT Security Frameworks, IoT in the Ubiquitous Healthcare, Short Distance Wireless Transmission Technologies, Security and Privacy in the IoT.

2.1. Definition of IoT

Ashton (2009) is accredited for using the term “Internet of Things” for the first time during a presentation in 1999 on supply-chain management. He believes the “things” aspect of the way we interact and live within the physical world that surrounds us needs serious reconsideration, due to advances in computing, Internet, and data-generation rate by smart devices. At the time, he was an executive director at MIT’s Auto-ID Center, where he contributed to the extension of RFID applications into broader domains, which built the foundation for the current IoT vision (Russell and Duren, 2016).

New IoT definitions give more value to the need for ubiquitous and autonomous networks of objects where identification and service integration have an important and inevitable role. For example, Internet of Everything (IoE) is used by Cisco to refer to people, things, and places that can expose their services to other entities. International Telecommunication Union (2012) defined the IoT is a global infrastructure for information society enabling services by interconnecting physical and virtual things based on existing and evolving interoperable Information Communication Technologies (Holler, 2014; Miller, 2015).

Minerva et al. (2015) defined An IoT is a network that connects uniquely identifiable "things" to the Internet. The "things" have sensing/actuation and potential programmability capabilities. Through the exploitation of the unique identification and sensing, information about the "thing" can be collected and the state of the "thing" can be changed from anywhere, anytime, by anything (Ning, 2013; Waher, 2015).

2.2. The IoT Security Frameworks

Today, there is no standardized conceptual model that characterizes and standardizes the various functions of an IoT system. Cisco Systems Inc. has proposed an IoT reference model that comprises seven levels. The IoT reference model allows the processing occurring at each level to range from trivial to complex, depending on the situation. The model also describes how tasks at each level should be handled to maintain simplicity, allow high scalability, and ensure supportability. Finally, the model defines the functions required for an IoT system to be complete. The seven levels and their brief characteristics are shown in Table 1:

Table 1 IoT World Forum Reference Model

Levels	Characteristics
Physical devices and controllers	End devices, exponential growth, diverse
Connectivity	Reliable, timely transmission, switching, and routing
Edge computing	Transform data into information, actionable data
Data accumulation	Data storage, persistent and transient data
Data abstraction	Semantics of data, data integrity to application, data standardization
Application	Meaningful interpretations and actions of data
Collaboration and processes	People, process, empowerment, and collaboration

The fundamental idea is to present a level of abstraction and appropriate functional interfaces to provide a complete system of IoT. It is the coherence of an end-to-end IoT architecture that allows one to process volume of context specific data points, make meaningful information, manage intrinsic feature of large scale, and ultimately design insightful responses (Green, 2014; Ren et al., 2014; Buyya and Dastjerdi, 2016).

Zhou (2014) mentioned the European Telecommunications Standards Institute (ETSI) IoT or machines-to-machines (M2M) system architecture had three layers Device, Connect, and Manage (DCM). Device layer provides local/ad-hoc sensor networks, embedded middleware, and sensors and actuators. Connect layer provides machine type communication, edge middleware and pervasive networks. Manage layer vertical applications, server-side middleware platform, and data management. The three-layer DCM classification is more about the IoT value chain than its system architecture at runtime.

Generically, an IoT deployment can consist of smart sensors, control systems and actuators, web and other cloud services, analytics, reporting, and a host of other components and services that satisfy a variety of business use cases. IoT services can be public or may be open to external agencies; as such, security can be an issue. Because of an increase in theft, privacy issues, misuse of information, lack of policy guidance, and ethical issues, it has become increasingly imperative to govern the use of information technology. This has increased the demand for security management. Hardware and software manufacturers of IoT applications and peripherals need to be able to determine what impact their decisions will have on overall consumer satisfaction. The IoT provider and manufacturer should address privacy and security issues through adopting best practices for the development of risk management processes (Pohls et al., 2014; Stackowiak and Licht, 2015; Moolayil, 2016).

Weber (2010), Kellmereit & Daniel, (2013), and Eltayeb (2017) studied the privacy and security requirements for protecting IoT systems as follows: (1) Resilience to Attacks: The system has to avoid single points of failure and should adjust itself to node failures. (2) Data Authentication: Access to objects' information must be authenticated as a principle. (3) Access Control: Information providers must be able to implement access control on the data provided. (4) Client Privacy: Measures need to be taken to ensure that only the information provider can infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

International Telecommunication Union (2012) shown the IoT reference model. It is composed of four layers as well as management capabilities and security capabilities which are associated with the four layers. The four layers are as follows: application layer, service support and application support layer, network layer, device layer. The application layer contains IoT applications. The service support and application support layer consists of two capability groups such as Generic support capabilities and Specific support capabilities. Network layer consists of Networking capabilities and Transport capabilities. Device layer capabilities can be logically categorized into Device capabilities and Gateway capabilities. The IoT management capabilities can be categorized into generic management capabilities and specific management capabilities. There are two kinds of security capabilities: generic security capabilities and specific security capabilities. Generic security capabilities are independent of applications. They include: at the application layer: authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus; at the network layer: authorization, authentication, use data and signaling data confidentiality, and signaling integrity protection; at the device layer: authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection. Specific security capabilities are closely coupled with application-specific requirements, e.g., mobile payment, security requirements (International

Telecommunication Union, 2012; Zhang and Cho, 2015; Hu, 2016), as shown is Figure 1:

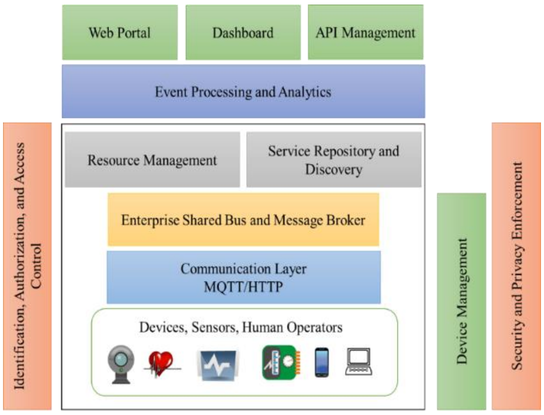

Web Portal
Dashboard
API Management
Event Processing and Analytics
Resource Management
Service Repository and Discovery
Enterprise Shared Bus and Message Broker
Communication Layer MQTT/HTTP
Devices, Sensors, Human Operators
Identification, Authorization, and Access Control
Device Management
Security and Privacy Enforcement

Figure 1 A Reference Architecture for IoT (Redraw from WSO2)

2.3. IoT in Ubiquitous Healthcare Applications

In healthcare, using the IoT for patient care and using the IoT to reduce costs can co-exist as mutual goals to improve healthcare quality, as joint benefits emerge from streamlining for efficiency and improvement of service quality (Chaudhry et al., 2006). The IoT strategies for healthcare should enhance and leverage legacy systems rather than reduce services as a by-product of automation. Connecting a device to the IoT framework requires transforming the external information a device produces and consumes into a form that can be transmitted over a network (Gubbi et al., 2013; Islam et al., 2015). Examples of relatively straightforward healthcare IoT applications enable scales, blood pressure monitors, temperature and other visit quantification devices to share data directly by transmitting on demand usable measurements to a requesting network agent. One or more network agents could manage the patient's record from each device. For example, as a patient enters a room, the room could be either activated by sensor, or could activate when a healthcare worker logs into the room's network and verifies the patient identity in the room. As the healthcare worker takes the measurements on various devices, the smart machines can send their readings to an open file, with buttons on the devices as options to skip logging the reading, or a way to do that in software in case there is a patient request to not update certain readings. Automating this data entry would save the time of the healthcare worker, who currently must scribe and re-enter the data into the computer after completing the data collection with the patient (Wears and Leveson, 2015; Spaanenburg, 2016; Smith, 2017).

Common to everyday living, wearable and wireless implantable medical devices, as well as home monitoring devices, are endowed with transmitting capabilities (Natarajan et al., 2016) that make information about a patient available for hospital staff analysis. For example, these devices may be wireless interconnected with sensors that measure the glucose level, the heart rate, the blood pressure, the weigh, and other medical parameters. These characteristics will turn these devices into a real part of IoT. In this sense, various applications are currently deployed, especially regarding the measurement and monitoring of a patient's vital signs, including glucose level sensing, electrocardiography, and blood pressure monitoring (Elk, 2016; Elkhodr, et al., 2016; Hameur and Brahimi, 2016), as shown in Table 2:

Table 2 Sensor for Monitoring of a Patient's Vital Signs

Patient's Vital Signs	**Sensor**	**Communication capabilities**	**Authors**
Glucose	Glucose Meter	Wireless, Blue tooth	Li, 2014; Lu, 2015
Electrocardiography	Electrocardiography (ECG or EKG)	Radio, Wireless	Anurag, 2014; Macala, 2016
Blood pressure	Blood pressure monitoring system	Bluetooth, ZigBee	Xin et al., 2013
Heart rate	Heart rate monitor	Wireless, BT, ZigBee	Natarajan, 2013
Body weight	Body scale (Kg)	Wireless, BT, ZigBee	McCallum, & Higgins, 2012; Tamura, et
Body Temperature	Body Temperature sensor (C)	Xbee, Wireless, ZigBee	Mansor, et al., 2013;
Respiration rate	Breath sensor (Airflow)	Wireless, ZigBee	Bachfischer, 2014

Short range network layer communication methods are Point-to-point communication, such as Near field connections (NFC) and Infrared data association (IrDA)with the network composition capacity communication mode ZigBee, Bluetooth, and Wi-Fi (802.11). Remote network layer communication method are existing mobile network system (~ 4G), and 5G for Massive Machine Type Communication such as Long Range (LoRa), and Narrow-band IoT (NB-IoT) for Low Power Wide Area Network (LPWAN) (NMazima et al., 2014; Gilchrist, 2015; Gilchrist, 2016).

2.4. Short Distance Wireless Transmission Technologies

Short range network layer communication methods are Point-to-point communication, such as Near field connections (NFC) and Infrared data association (IrDA)with the network composition capacity communication mode ZigBee, Bluetooth, and Wi-Fi (802.11). Remote network layer communication method are existing mobile network system (~ 4G), and 5G for Massive Machine Type Communication such as Long Range (LoRa), and Narrow-band IoT (NB-IoT) for Low Power Wide Area Network (LPWAN) (Greengard, 2015; Penttinen, 2016).

Short Distance Wireless Transmission Technology includes Wi-Fi, Bluetooth and ZigBee. The security of these technologies is primary concerned in this research. The 14 items of the 3 technologies are compared, which are Standard Protocol, Band, Transmission rate, Power consumption, Number of connections, Connection distance, Connection speed, Security, Current application levels, Characteristics, Price, Network Type, Contents, and Applications, as shown in Table 3:

Table 3 Compared with Short Distance Wireless Transmission Technology

Technology Items	Wi-Fi	Bluetooth	ZigBee
Standard Protocol	IEEE 802.11 x	IEEE 802.15.1	IEEE 802.15.4
Band	2.4 GHz, 5 GHz	2.4 GHz, 915 MHZ, 868 MGz	2.4 GHz, 915 MHZ, 868 MGz
Transmission rate	600 / 54 Mbps	(HS) 24 Mbps	250 Kbps
Power consumption	High	Medium (0.01~1W)	low
Number of connections	Dozens	Hundreds of millions	Tens of thousands
Connection distance	1-100 m	1-100 m	1-100 m
Connection speed	3 sec	10 sec	30 ms
Security	SSID, WEP, WAP, WAP2	Classic: 56/128-bit, user defined application BLE: 128-bit AES, user defined application	128-bit AES, user defined application
Current application levels	Large transmission, computing equipment networking	Peripheral, wearable device	Monitoring and control
Characteristics	High transmission rate, IP	Convenient, low cost	Low power, low cost
Price (US$)	25	3	2
Network Type	WLAN	WPAN	Ad Hoc
Contents	Internet, Audio, Video	Internet, Audio, Video	Text, Voice
Applications	Tablet PCs, PC, game consoles, home appliances, Smartphones, Printers, Laptops and other peripherals	Headset, Security Proximity app, Medical, Spots, Home appliances	Remote control, Smart retail, Lightings, Home automation,

2.5. Security and Privacy in the IoT

The Internet of Things (IoT) promises to revolute communications on the Internet. The IoT enables numerous business opportunities in fields as diverse as e-health, smart cities, smart homes, among many others. It incorporates multiple long-range, short-range, and personal area wireless networks and technologies into the designs of IoT applications. This will result in the IoT being pervasive in many areas which raise many challenges the IoT with regard to security, privacy, and management.

Chellappan and Sivalingam (2016) mentioned the challenges that must be overcome to resolve IoT security and privacy issues are immense. This is primarily because of the many constraints attached to the provision of security and privacy in IoT systems. The deployment of the IoT raises many security issues arising because of the following aspects: (1) the very nature of smart objects, for example, the adoption of lightweight cryptographic algorithms, in terms of processing and memory requirements. (2) the use of standard protocols, for example, the need to minimize the amount of data exchanged between nodes. (3) the bidirectional flow of information, for example, the need to build an end-to-end security architecture.

Dhanjani (2015) studied the confidentiality: transmitted data can be read only by the communication endpoints; availability: the communication endpoints can always be reached and cannot be made inaccessible; integrity: received data are not tampered with during transmission, and assured of the accuracy and completeness over its entire lifecycle; authenticity: data sender can always be verified and data receivers cannot be spoofed and authorization: data can be accessed only by those allowed to do so and should be made unavailable to others. The requirements for securing the IoT are complex, involving a blend of approaches from mobile and cloud architectures, combined with industrial control, automation, and physical security.

However, the smart IoT devices expose much more sensitive information, and provide much less scope for this type of commercial model as it is largely back-end data. Hence users are likely to be both vulnerable and sensitive to privacy concerns. These challenges make it very complex to operationalize IoT in a secure way, while fully preserving privacy. There are several promising approaches that are being investigated to solve for each aspect of the privacy issues, and there is still some distance to go before we can see production ready commercial implementations that are standardized and widely adopted.

3. Architecture-Oriented IoT Information Security Management Model Application

Chao (2016) studied an architecture description is a formal description and representation of a system. A description of the systems architecture must grasp the essence of the system and its details at the same time. In other words, an architecture description not only provides an overall picture that summarizes the whole system, but also contains enough detail that the system can be constructed and validated.

The language for architecture description is called the architecture description language (ADL) (Chao, 2016). An ADL is a special kind of language used in describing the architecture of a system. Since the architectural approach uses a coalescence model for all multiple views of a system, the foremost duty of ADL is to make the strategy/version n, strategy/version n+1, concept, analysis, designs, implementation, structure, behavior, and input/output data views all integrated and coalesced within this architecture description. SBC-ADL uses six fundamental diagrams to describe the integration of systems structure and systems behavior of a system. These diagrams are: a) architecture hierarchy diagram (AHD), b) framework diagram (FD), c) component operation diagram (COD), d) component connection diagram (CCD), e) structure-behavior coalescence diagram (SBCD), and f) interaction flow diagram (IFD) (Ma, 2012, Ma, 2013).

The Structure-behavior coalescence architecture (SBC) description language has been used to describe and represent an Architecture-Oriented IoT Security Management Model. The model extended the Systems Architecture of Smart Healthcare Cloud Applications and Service IoT System (SHCASIS) (Chao, 2016) and emphasized on information security of IoT.

An architecture hierarchy diagram (AHD) was used to structure the architecture-oriented the systems architecture of Information Security of Smart Healthcare Cloud Applications and Services Internet of Things (IoT) System (ISSHCASIS) for decomposition and combination to understand the complex Smart Healthcare Cloud Applications and Services systems. The structure elements of the IoT security management model were the basic elements, and they composed of the model structure. The necessary structure elements were analyzed from the model. composed of Application_Layer, Data_Layer, and Technology_Layer. Applicalion_Layer is composed of Presentation_Layer and Logic_Layer. Presentation_Layer is composed of Patient_Account_Registering_UI, Alerts_Notifiying_UI, Emergency_Response_Starting_Time_UI, and Emergency_Response_End_Time_UI. Logic_Layer is composed of Patient_Vital_Signs_Deamon. Data_layer is composed of ISSHCASIS_Database. Technology_Layer is composed of Patient_Vital_Signs_Sensor_P, IAA (Identification, Authorization, and Access Control)_Contorller, and IoT_Security_&_Privacy_Manager.

After collection of non-aggregated systems or structure elements of architecture hierarchy diagram, we obtain the Framework Diagram (FD). Presentation_Layer and Logic_Layer are sub-layers of Application_Layer. Presentation_Layer contains the Patient_Account_Registering_UI, Alerts_Notifying_UI, Emergency_Response_Starting_Time_UI, and Emergency_Response_End_Time_Ul components. Logic_Layer contains the Patient_Vital_Signs Daemon component; Data_Layer contains the ISSHCASIS_Database component. Technology_Layer contains the Patient_Vital_Signs_Sensor_P, IAA _Contorller, and IoT_Security_&_Privacy_Manager components

For a system, we use component operation diagram (COD) to illustrate all components operations. COD is the third fundamental diagram to achieve structure-behavior coalescence. The structure components provide many operations throughs the interface or work content of the structure components with input or output parameters is called a COD (Sweeney, 2010; Lawler and Howell-Barber, 2007). Input parameter of the service is denoted by an arrow symbol directed to structure element. Output parameters of the operation are denoted by an arrow symbol leave the component. Based on the collection of literature, standard operation procedure (SOP), and sorted out the structure components step by step, operations of nine structure elements were obtained for the ISSHCASIS.

A structure component connection diagram (CCD) connects operations between the various structure components in accordance with its priorities. CCD is obtained after the analysis phase is finished. We use the CCD to describe how the components and actors (in the external environment) are connected within ISSHCASIS. CCD is the fourth fundamental diagram to achieve structure-behavior coalescence. Rectangular frame is the system boundary, and the Five_Minute_Interval, Healhcare_Provider, IoT_Security_Administrator, Server_Root, Patient_Vital_Signs are the external environment.

The purpose of using the architectural approach, instead of separating the structure model from the behavior model, is to achieve one single coalesced model. In Figure 2, systems architect can see that systems structure and systems behavior coexist in the Structure Behavior Coalescence Diagram (SBCD) (Ma, 2010; Ma, 2013). Systems architect not only see its systems structure but also see its systems behavior simultaneously in the SBCD of ISSHCASIS. From the structure element diagram and structure element service diagram, we further derive out six behaviors of the ISSHCASIS model: (1) Alerts Notifying Behavior (2) Registering Patient Account Behavior (3) Recording Emergency Response Starting Time Behavior (4) Recording Emergency Response End Time Behavior (5) Sensing Patient Vital Signs Behavior, and (6) IoT Security and Privacy Management Behavior.

SBCD is the structure-behavior coalescence diagram we obtain after the architecture construction is finished. Figure 2 shows a SBCD of the ISSHCASIS in which interactions among the Five_Minute_Interval, Healhcare_Provider, IoT_Security_Administrator, Server_Root, Patient_Vital_Signs actors and the Aterts_Notifying_UI, Patient_Account_Registeritig_UI, Emergency_Response_Starting_Time_UI, Emergency_Response_End_Time_UI, Patient_Vital_Signs_Daemon, ISSHCASIS_Database, Patient_Vital_Signs_Sensor_P, IoT_Security_&_Privacy_Manager, IAA_Controller components shall draw forth Registering_Patient_Account, Sensing_Patient_Vital_Signs, Alerts_Notifying, Recording_Emergency_Response_Starting_Time, Recording_Emergency_Response_End_Time, IoT_Security_&_Privacy_Management behaviors. In other words, these six behaviors together provide the overall behavior of the ISSHCASIS.

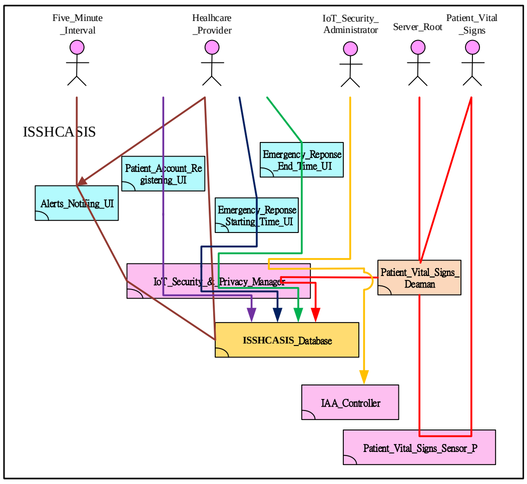


Figure 2 Structure-Behavior Coalescence Diagram of ISSHCASIS

We use interaction flow diagram (IFD) to demonstrate individual behavior. IFD is the sixth fundamental diagram uses in achieving structure-behavior coalescence. Each behavior presented on the SBCD of the ISSHCASIS can be drawn as an IFD. The construction of IFD of the ISSHCASIS describes the outside environment and structure elements, and their interactions according to the time. Each individual behavior is represented by an execution path. We use an IFD to define each one of these execution paths. There are 6 interaction flow diagrams in total for the ISSHCASIS: (1) Interaction Flow Diagrams for Alerts Notifying of ISSHCASIS (2) Interaction Flow Diagrams for Registering Patient Account Behavior of ISSHCASIS (3) Interaction Flow Diagrams for Recording Emergency Response Starting Time Behavior of ISSHCASIS (4) Interaction Flow Diagrams for Recording Emergency Response End Time Behavior of ISSHCASIS (5) Interaction Flow Diagrams for Sensing Patient Vital Signs Behavior of ISSHCASIS, and (6) Interaction Flow Diagrams for IoT Security and Privacy Management Behavior of ISSHCASIS.

Figure 3 represents IFD for Alerts Notifying of ISSHCASIS. X-axis represents structure elements and the external environment in which information flow direction is from left to right. Y-axis represents the implementation of an interactive timeline from the top to the bottom in the time sequence. Figure 3 shows an IFD of the Alerts_Notifying behavior. First, actor Five_Minute_Interval interacts with the Alerts_Notifying_UI component through the Show_All_Alerts operation call interaction, carrying the Current_Time input parameter. Next, component Alerts_Notifying_UI interacts with IoT_Security_&_Privacy_Manager component through the Manage_S_&_P_Vital_Signs_for_Alters_Analysis carrying the Current_Time input parameter. Next, IoT_Security_&_Privacy_Manager interacts with ISSHCASIS_Database component through the SQL_Select_Patient_Vital_Signs_for_Alerts_Analysis operation call interaction, carrying the Current_Time input parameter and Patient_Vital_Signs_for_Alerts_Analysis_Query output parameter. Continuingly, IoT_Security_&_Privacy_Manager interacts with Alerts_Notifying_UI component through the Monitoring_IoT_Security_&_Privacy operation call interaction, carrying Current_Security_&_Privacy_Status. Finally, actor Healthcare_Provider interacts with the Alerts_Notifying_UI component through the Display_Alerts operation call interaction, carrying the Alerts_Report output parameter.

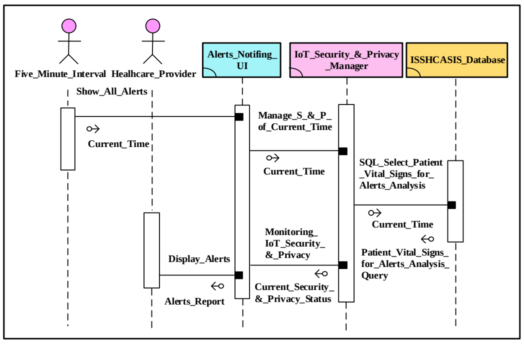


Figure 3 Interaction Flow Diagrams for Alerts Notifying of ISSHCASIS

Figure 4 shows an IFD of IoT Security and Privacy Management Behavior of ISSHCASIS. First, actor IoT_Security_Administrator interacts with IoT_Security_&_Privacy_Manager component through Manage_S_&_P_of_IoT_Security_Adminstration operation call interaction, carrying IoT_Security_Adminstration input parameter. Next, IoT_Security_&_Privacy_Manager component interacts with IAA_Controller component, carrying IAA_Control input parameter.

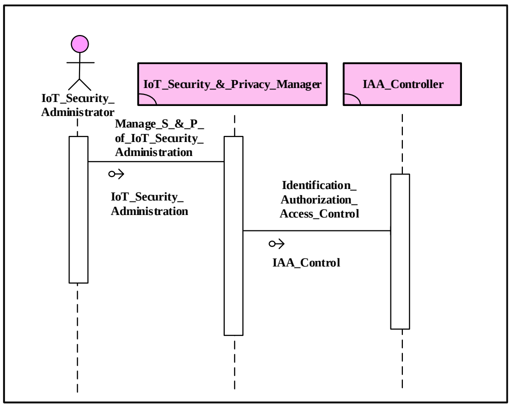

IoT_Security_Administrator
IoT_Security_&_Privacy_Manager
IAA_Controller
Manage_S_&_P_of_IoT_Security_Administration
IoT_Security_Administration
Identification_Authorization_Access_Control
IAA_Control

Figure 4 Interaction Flow Diagrams for IoT Security and Privacy Management Behavior of ISSHCASIS

4. Wireless Penetration Test

In this chapter, we will explain the plan of wireless penetration test in WLAN and then try to Wireless Penetration Test for Encrypted Wi-Fi in WLAN.

4.1. Wireless Penetration Test in WLAN

In order to ensure the security and stability of the data from the host, we prepare an on-line UPS system, and use Raspberry Pi 3 to do the temperature sensor, infrared sensor, camera, access control and other modules to protect the security of hardware, as shown in Figure 5:

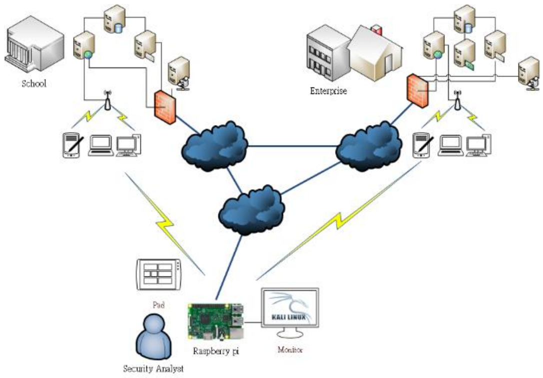


Figure 5 Wireless Penetration Test in Local Network Area

With the assistance of engineers from Zhengchuang Technology Company, we cooperate with the implementation of the four technical information security related under-graduate and graduate courses in Cheng Shiu University, Kaohsiung, Taiwan to complete the safety and PT of the IoT cloud operation and information safety control. The operation system of the test computer uses Kali Linux: including: information gathering tools, target detection, vulnerability assessment, web scanning, social engineering, database detection and attack, password cracking, vulnerability utilization, escalation rights, continuous control, Metasploit penetration testing, wireless network attacks, Stress test more than 400 penetration test tools.

The projects include 4 main tests: Password Security Penetration Test, Web Security Penetration Test, File Server Safety Penetration Test, Wireless network penetration testing, etc. More than 200 computer hosts, 5 server are tested, the initial safety penetration test results are shown to be good.

4.2. Wireless Penetration Test for Encrypted Wi-Fi in WLAN

There are four methods to encrypt Wi-Fi: Open System, Wired Encryption Protocol (WEP), Wi-Fi Protected Access (WPA), and WPA2 respectively. WPA2 is recognized the most secure encryption method. Four encryption methods are described in detail as following:

(1) Open System is no encryption.

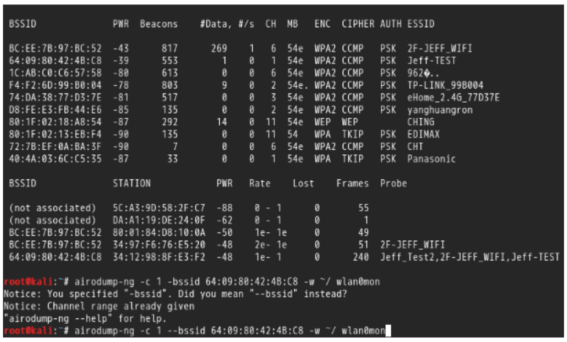
(2) WEP is the Wired Encryption Protocol wired encryption protocol. It became part of the 802.11 standard in 1999. WEP uses the 40-bit or 104-bit encryption key, which uses the Rivest Cipher (RC4) symmetric cipher. Because the initial vector (IV) of the WEP is only 24 bits, it is not enough to avoid the key duplication and thus be cracked.

(3) WPA is Wi-Fi Protected Access which was arising from the transitional wireless security solutions to solve the WEP security problems. WPA encryption method is to use 128-bit gold The key and the 48-bit initial vector (IV), and the Temporal Key Integrity Protocol (TKIP) to avoid the WEP period of the Related-Key Attack problems. Compared to WEP, WPA applies dynamic changing key reducing the WEP the Related-Key being cracked attack problem significantly.

(4) WPA2 is the official version of WPA encryption standard after the official launch of the Wi-Fi Alliance in the IEEE 802.11i standard. Because it is incompatible with the WEP, WPA2 uses a new encryption architecture, Michael algorithm in which the receiver can verify the packet integrity of the algorithm, WPA2 is recognized by the fully secure CCMP message authentication code replaced, and RC4 also replaced by Advance Encryption Standard (AES), which reduces the possibility of being cracked by brute force attack.

We followed the methodology of industrial standard, which are The Penetration Testing Execution Standard (PTES), NIST Technical Guide to Information Security Testing and Assessment (NIST 800-115), Open Source Security Testing Methodology Manual (OSSTMM) to run the wireless penetration test (PT). There are six steps to do the PT: Reconnaissance, Attacks and Penetration, Client-side attacks, Entering the network, Vulnerability assessments, Exploitation and data capture. Preventing from break the law, we built the IoT information security test environment.

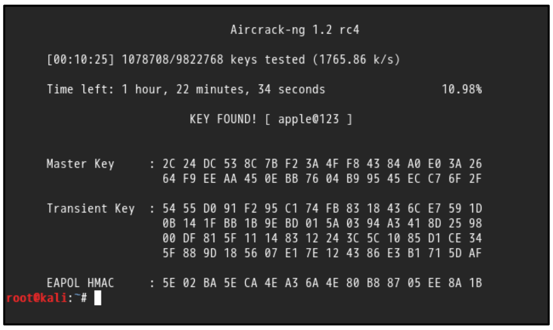
In this study, we set up a access point (AP) for wireless penetration test, Service Set Identifier (SSID) is 2F-JEFF_WIFI. The AP use WPA2 encryption algorithm. To crack WEP, we made use of a popular and fantastic utility named Aircrack-ng. Aircrack-ng uses several methods to attack WEP IVs such as using of dictionary attacks and using of brute-force attacks. The command used to crack WPA2. The whole process from the beginning to the end of test about 20 to 30 minutes of time, and then break the encryption time for the "1 second". Time left is the remaining time of the software, and the remaining time will have different results because of the different system conditions at the test time as shown in Figure 6:



```
 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 BC:EE:7B:97:BC:52  -43      817      269    1   6  54e  WPA2 CCMP   PSK  2F-JEFF_WIFI
 64:09:80:42:4B:C8  -39      553        1    0   1  54e  WPA2 CCMP   PSK  Jeff-TEST
 1C:AB:C0:C6:57:58  -80      613        0    0   6  54e  WPA2 CCMP   PSK  962�..
 F4:F2:6D:99:B0:04  -78      803        9    0   2  54e. WPA2 CCMP   PSK  TP-LINK_99B004
 74:DA:38:77:D3:7E  -81      517        0    0   3  54e  WPA2 CCMP   PSK  eHome_2.4G_77D37E
 D8:FE:E3:FB:44:E6  -85      135        0    0   2  54e  WPA2 CCMP   PSK  yanghuangron
 80:1F:02:18:A8:54  -87      292       14    0  11  54e  WEP  WEP         CHING
 80:1F:02:13:EB:F4  -90      135        0    0  11  54   WPA  TKIP   PSK  EDIMAX
 72:7B:EF:0A:BA:3F  -90        7        0    0   6  54e  WPA2 CCMP   PSK  CHT
 40:4A:03:6C:C5:35  -87       33        0    0   1  54e  WPA  TKIP   PSK  Panasonic

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 (not associated)   5C:A3:9D:58:2F:C7  -88    0 - 1      0       55
 (not associated)   DA:A1:19:DE:24:0F  -62    0 - 1      0        1
 BC:EE:7B:97:BC:52  80:01:84:D8:10:0A  -50    1e- 1e     0       49
 BC:EE:7B:97:BC:52  34:97:F6:76:E5:20  -48    2e- 1e     0       51  2F-JEFF_WIFI
 64:09:80:42:4B:C8  34:12:98:8F:E3:F2  -48    1e- 1      0      240  Jeff_Test2,2F-JEFF_WIFI,Jeff-TEST

root@kali:~# airodump-ng -c 1 -bssid 64:09:80:42:4B:C8 -w ~/ wlan0mon
Notice: You specified "-bssid". Did you mean "--bssid" instead?
Notice: Channel range already given
"airodump-ng --help" for help.
root@kali:~# airodump-ng -c 1 --bssid 64:09:80:42:4B:C8 -w ~/ wlan0mon
```

Figure 6 Screen Snapshot of WPA2 Password Analysis Process Using Airodump-ng.

The weakest password for the AP was found as shown in Figure 7:



```
                              Aircrack-ng 1.2 rc4

      [00:10:25] 1078708/9822768 keys tested (1765.86 k/s)

      Time left: 1 hour, 22 minutes, 34 seconds                 10.98%

                           KEY FOUND! [ apple@123 ]


      Master Key     : 2C 24 DC 53 8C 7B F2 3A 4F F8 43 84 A0 E0 3A 26
                       64 F9 EE AA 45 0E BB 76 04 B9 95 45 EC C7 6F 2F

      Transient Key  : 54 55 D0 91 F2 95 C1 74 FB 83 18 43 6C E7 59 1D
                       0B 14 1F BB 1B 9E BD 01 5A 03 94 A3 41 8D 25 98
                       00 DF 81 5F 11 14 83 12 24 3C 5C 10 85 D1 CE 34
                       5F 88 9D 18 56 07 E1 7E 12 43 86 E3 B1 71 5D AF

      EAPOL HMAC     : 5E 02 BA 5E CA 4E A3 6A 4E 80 B8 87 05 EE 8A 1B
root@kali:~#
```

Figure 7 Screen Snapshot of WPA2 Password Analysis Process Using Aircrack-ng.

The eight steps can be used to improve the problem are: the panel was established to improve the problems, description of the problems, temporary measures to implement and confirm, reason analysis and confirm, permanent improvement measures drawn, permanent measures to improve the implementation and effectiveness, prevent problems recurrence, and finished.

5. Conclusions and Recommendations

Risk of IoT devices are lack of rigorous encryption mechanism, perfect access system, the ability to protect personal privacy is poor, and mobile device security issues. Network media security issues are low-throughput technology is difficult to carry out reliable security communication mechanism, such as NFC and Bluetooth, unencrypted transmission channel, Man-in-the-middle attack and other attacks. Service system security issues are opening system and opening challenge, risk of user data leakage, getting equipment control (prevent from replay attack). The current IoT equipment manufacturers should be established as soon as possible awareness and prevention capabilities. Data manages as light as possible. Information security education for personnel of the enterprise. For improving resolutions for wireless network encryption vulnerability summarized, as show in Table 3:

Table 3 Improvement resolutions for Wireless Network Encryption Vulnerability

Vulnerability	Explanations	Improvement resolutions
Use default password on management interface	Because we can know the management password by analyzing the label of the target device by using the default password.	Suggest changing password immediately, if the user name can be customized with the change at same time.
WPS enabled	Because it uses only 8 words and all digital for the WPS password, it is easier to penetrate WPS than the use of non-WPS devices.	It is recommended to immediately close the function of WPS, to reduce the chance of being penetrated. We cannot shut down computer, but we must ask manufacturers to help deal with security events
Weak wireless network encryption	Because the use of words in dictionary or too short text as a wireless network password, it will cause the wireless network can be easily misappropriated by criminals.	Avoid using word on the dictionary as a password, the strong passwords (above 8 character passwords with upper- and lowercase letters, digits, and special characters) and AES encryption should be used as the password for the wireless network.
OpenSSL Vulnerability	Because OpenSSL program design defects results by the user's information disclosure.	Ask the vendor to update OpenSSL to the latest version, and if it could not fix immediately, it might be disabled the software service associated with the vulnerability.
Using XSS to bypass CSRF protection	Cross Site Scripting Attack	Ask the vendor to fix the vulnerabilities

By this study introduction and elaboration of the enterprise architecture of protect security and privacy of patient’s information, we may understand clearly how the SBC helps architects effectively construct fruitful enterprise architectures. The ISSHCASIS enterprise architecture focus on: (1) Verifying input data for security and privacy checks before storing data in ISSHCASIS database. (2) Verify inputting emergency response starting or end time for security and privacy checks before updating data in ISSHCASIS database. (3) Verify PVS alerts data for security and privacy checks before updating data in ISSHCASIS database. (4) Manage IoT Security & Privacy is by configuring properly of IoT Security & Privacy manager, and managing IAA Controller for PVSSP. (5) IAA Controller manages identification, authorization, and access control of IoT for protection security and privacy. (6) IoT Security & Privacy Manager is used to manage IoT protocols, authentication, and encryption of patient vital signs.

References

1. Ashton, K., 2009, That ‘internet of things’ thing. RFiD J., 22(7), pp.97–114.

2. Buyya, Rajkumar and Amir Vahid Dastjerdi, 2016. Internet of Things, New York: Morgan Kaufmann.

3. Chao, William S., 2012. Systems Architecture: SBC Architecture at Work, Taipei, LAP LAMBERT Academic Publishing, p. 344.

4. Chao, William S., 2016. Systems Architecture of Smart Healthcare Cloud Applications and Services IoT System: General Architectural Theory at Work, Amazon Digital Services LLC, pp. 116.

5. Chao, William S., 2016, Systems Architecture of Smart Home Security Cloud Applications and Services IoT System: General Architectural

Theory at Work, Amazon Digital Services LLC, pp. 120.

6. Chellappan, V. and K.M. Sivalingam, 2016. Security and privacy in the Internet of Things in Internet of Things, Edited by Rajkumar Buyya and Amir Vahid Dastjerdi, New York: Morgan Kaufmann.

7. Dawson, Maurice, 2016. Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity, Hershey: IGI Global.

8. Dhanjani, Nitesh, 2015. Abusing he Internet of Things: Blackouts, Freakouts, And Stakeouts, O'Reilly Media.

9. Elk, Klaus, 2016. Embedded Software Development for The Internet of Things, Amazon Digital Services LLC, pp. 221.

10. Elkhodr, Mahmoud, Seyed Shahrestani, Hon Cheung, 2016. Internet of Things Research Challenges, IGI.

11. Eltayeb, Mohamed, 2017. Privacy and Security in Security Solutions for Hyperconnectivity and the Internet of Things, Edited by Maurice Dawson; Marwan Omar; Mohamed Eltayeb, Hershey: IGI Global.

12. Gilchrist, Alasdair, 2015. A Concise Guide to The Internet of Things for Executives, RG Consulting, pp. 30.

13. Gilchrist, Alasdair, 2016. Industry 4.0: The Industrial Internet of Things, Apress.

14. Greengard, Samuel, 2015. The Internet of Things, The MIT Press, pp. 232.

15. Green, J., 2014. IoT reference model. http://www.iotwf.com/resources/72, Browsed on Nov. 30, 2016.

16. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), pp. 1645–1660.

17. Hameur, Amina, and Samiha Brahimi, 2016. Background on Context-Aware Computing Systems in Internet of Things and Advanced Application in Healthcare.

18. Holler, Jan, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, 2014, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Academic Press, pp. 352.

19. Hu, Fei, 2016. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, CRC Press, pp. 604.

20. International Telecommunication Union, 2012. ITU-T Recommendation Y.2060: Series Y: Global information infrastructure, internet protocol aspects and next-generation networks: Frameworks and functional architecture models: Overview of the Internet of Things. Geneva: International Telecommunication Union.

21. Islam, S.M., D. Kwak, H. Kabir, M. Hossain, K. Kwak, 2015, The Internet of Things for Health Care: A Comprehensive Survey, IEEE ACCESS.2015.2437951.

22. Kellmereit, Daniel, and Obodovski, Daniel, 2013. The Silent Intelligence: The Internet of Things, DND Ventures LLC, pp. 166.

23. L.R. LLC., 2013. An introduction to the Internet of Things (IoT).

24. Ma, Wei-Ming, 2010. Study on Architecture-Oriented Information Security Risk Assessment Model, Computational Collective Intelligence Technologies and Applications, Volume 6423/2010, pp. 218-226.

25. Ma, Wei-ming, Tsai, Cheng-F, 2012. Study of Implementation of the Personal Information Protection Act Architecture on CSU Campus, 2012 Symposium on Global Business Operation and Management, Kaohsiung, Taiwan.

26. Ma, Wei-ming, 2013. Study on Enterprise Architecture Development, Journal of Global Business Operation and Management, 5, pp. 57-71.

27. Miller, Michael, 2015. The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World, Que Publishing, pp. 335.

28. Minerva, Roberto, Abyi Biru, D. Rotondi, 2015. Towards a definition of the Internet of Things (IoT), IEEE.

29. Moolayil, Jojo, 2016. Smarter Decisions – The Intersection of Internet of Things and Decision Science, Packt Publishing.

30. Natarajan, K., B. Prasath, P. Kokila, 2016. Smart Health Care System Using Internet of Things. Journal of Network Communications and Emerging Technologies, 6 (3).

31. Ning, Huansheng, 2013. Unit and Ubiquitous Internet of Things, CRC Press, pp.267.

32. NMazima, J.k., M. Kisangiri, D. Machuve, 2013. Design of Low Cost Blood Pressure and Body Temperature Interface", International Journal of Emerging Science& Engineering, 1(10).

33. Penttinen, Jyrki T. J., 2016. Wireless Communications Security: Solutions for The Internet of Things, Wily, pp.336.

34. Pohls, H. C., Angelakis, V., Suppan, S., Fischer, K., Oikonomou, G., Tragos, E. Z., Mouroutis, T., 2014. RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects. In Wireless Communications and Networking Conference Workshops (WCNCW), IEEE, pp. 122-127.

35. Ren, K., Samarati, P., Gruteser, M., Ning, P., & Liu, Y., 2014. Guest Editorial Special Issue on Security for IoT: The State of the Art. Internet of Things Journal, IEEE, 1(5), pp. 369-371.

36. Russell, Brian, and Drew Van Duren, 2016. Practical Internet of Things Security, Packt Publishing, pp. 336.

37. Smith, Sean, 2017. The Internet of Risky Things, O'Reilly Media.

38. Spaanenburg, Lambert, 2016. The Role of Time in Health IoT, in Internet of Things and Advanced Application in Healthcare, IGI Global.

39. Stackowiak, Robert, Art Licht, 2015. Big Data and The Internet of Things: Enterprise Information Architecture for A New Age, Apress.

40. Tamura, T., T. Togawa, M. Ogawa, M. Yoda, 1998. "Fully automated health monitoring system in the home," Medical Engineering & Physics, 20(8), pp. 573-579.

41. Waher, Peter, 2015. Learning Internet of Things, Packt, pp. 242.

42. Wears, R. L., and Leveson, N. G., 2008. Safeware: Safety-critical computing and healthcare information technology. Advances in Patient Safety: New Directions and Alternative Approaches, 4, pp. 1-10.

43. Weber, R. H., 2010. Internet of Things - New security and privacy challenges. Computer Law & Security Report, 26(1), 23–30.

44. WSO2, 2014. A reference architecture for the Internet of Things.

45. Zhang, Z. K., Cho, M. C. Y. S., 2015. Emerging Security Threats and Countermeasures in IoT. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, (pp. 1-6). ACM.

46. Zhou, Honbo, 2014. The Internet of Things in the Cloud: A Middleware Perspective, CRC Press, pp.348.