RESEARCH ARTICLE OPEN ACCESS

Study on Enterprise Architecture of IoT Information Security in a Medical Management System

Wei-Ming Ma*
**(Department of Information Management, Cheng Shiu University, Taiwan, R.O.C.*

ABSTRACT
The Internet of Things (IoT) has the characteristics of self-conscious objects, which can form a smart environment and space, which can improve the quality of people's medical care and significantly improve the well-being of human life. However, devices such as IoT sensors have weaknesses in information security, including lower computing power, lower energy requirements, less reliable wireless communication channel characteristics, and physical vulnerabilities. If hackers maliciously damage the IoT information security, it may pose a threat to human survival. This study takes the perspective of enterprise architecture to construct a framework suitable for the government's regional medical care IoT information security system as an example. It explores and implements the medical care IoT information security architecture to achieve a solution to the highly complex IoT information conversion system and the goal of preservation of digital evidence and reducing development costs.

Keywords - enterprise architecture, information security, Internet of things, IoT, medical management system

---

Date of Submission: 25-02-2020 Date Of Acceptance: 05-03-2020

I. INTRODUCTION

1.1. Background and Research Motivation

Internationally, the proportion of the population over 65 years of age has reached 7%, 14%, and 20%, which are called aging society, aged society, and ultra-aging society, respectively. The Ministry of the Interior of Taiwan R.O.C. pointed out that the elderly population aged 65 and over in Taiwan increased year-on-year from 14.91 million at the end of 1993 to 3.312,000 at the end of March 2018, a total increase of 1.821 million, and the proportion of the total population rose from 7.10% to 14.05. %, which means that within 25 years, Taiwan has moved from an "aging society" to an "aged society." Medical care for the elderly will become challenging issues of concern to countries around the world.

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

Chellappan and Sivalingam [1] studied the IoT revolution 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.

The motivation for this study is to delve into the four issues that government agencies have faced for a long time in medical management and to try to come up with improvement plans:

(1) The high cost of IoT medical system development: shortcomings such as high complexity of IoT information transmission systems, high development costs, and low system scalability.

(2) Medical resources are not effectively used: At present, government agencies have invested considerable medical resources. However, some responsible departments do not know the characteristics of each resource, so they cannot use medical resources effectively and fully exert their medical functions.

(3) The team lacks the overall concept: each department only provides professional insights for its professional part, and falls into the guise of professionalism, failing to comprehensively review, resulting in the lack of the overall concept of

medical resources. Due to the process-oriented medical management method, each member should do what and how to do it, which makes it easy to focus on some people and increase the workload, while the rest of the staff sit idly and cause uneven distribution of human resources.

(4) Outdated medical information: scattered data sources, inconsistent data formats, and failure to implement a timely life signal detection system, so that only post-event reports can review, and medical prevention effects cannot exert.

1.2. Research Goals

This research uses the Structure-Behavior Coalescence (SBC) Methodology [2] to integrate the organizational structure of participating government medical management units with effective information security management behaviors, to visually solve the three problems faced by government agencies for IoT to achieve the goal of effective improvement:

(1) Effective use of management resources: Through the SBC methodology, the overall observation and implementation of the unit's organizational structure and standard operating procedures, the effective use of management resources, and prevention of security and protection loopholes.

(2) Real-time update of physiological data: use the architecture-oriented medical system to transmit real-time physiological data through the IoT through the wearable device of the patient, improve the correct judgment rate of medical staff, and effectively improve the implementation efficiency of the medical system.

(3) Strengthening empowerment and awareness of information security: By explaining the six diagrams of the SBC methodology and interviewing the enterprise, each medical manager can accurately understand the structure of the medical system and improve communication and coordination among various departments to reduce security events happened.

This research will reach the goals of resolving the problem of the high complexity of information transitions System of IoT, high cost of development, low expandability of the system, and preservation of digital evidence.

1.3. Research Method

Enterprise architecture is a complex that comprises multiple views such as strategy, version, goal, object, concept, analysis, design, implementation, structure, behavior, and input/output data views. Accordingly, an enterprise defined as a set of interacting components forming an integrated whole of that enterprise's multiple views. SBC results in the coalescence of multiple views. Therefore, it concluded that SBC architecture is so proper to model the multiple views of an architecture enterprise of the government's medical management system. Therefore, the SBC architecture used to model the system to meet its objectives for the preservation of digital evidence.

II. LITERATURE REVIEW

This section summarizes the research topics and related essay knowledge of domestic and foreign scholars, including the definition of IoT, The IoT Security Frameworks, Security and Privacy in the IoT, IoT in ubiquitous healthcare applications, and enterprise architecture to build an entire argument for this research based on the wisdom established by the predecessors.

2.1. IoT Security Frameworks and Applications

The previous research about the definition of IoT, the IoT Security Frameworks, Security and Privacy in the IoT, IoT in ubiquitous healthcare applications are summarized.

2.1.1. The Definition of IoT

Ashton [3] 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, the 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 [4].

New IoT definitions give valuable needs for ubiquitous and autonomous networks of objects where identification and service integration have an important and inevitable role. For example, the 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 [5] 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.

2.1.2 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 handle 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 Fig 1 [6]:

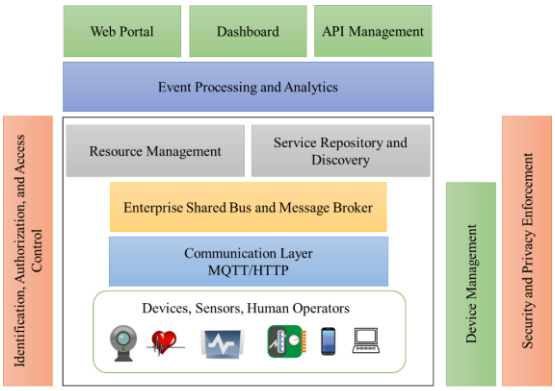


Figure 1. A Reference Architecture for IoT (Redraw from WSO2 [6])

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 the volume of context-specific data points, make meaningful information, manage intrinsic feature of large scale, and ultimately design insightful responses [7][8].

2.1.3 Security and Privacy in the IoT

The challenges that must overcome to resolve IoT security and privacy issues are immense. It 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 [9][10].

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 verify, 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 [11].

2.1.4 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 [12]. 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 transmit over a network [13].

Common to everyday living, wearable, and wireless implantable medical devices, as well as home monitoring devices, are endowed with transmitting capabilities [14] that make information about a patient available for hospital staff analysis. For example, these devices may wirelessly interconnect with sensors that measure the glucose level, heart rate, blood pressure, weight, 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, as shown in Tab. 1:

Table 1. Sensor for Monitoring of a Patient's Vital Signs

Patient's Vital Signs	Sensor	Sensor Experiment	Communication capabilities
Glucose	Glucose Meter		Wireless, Blue tooth
Electrocardiography	Electrocardiography (ECG or EKG)	AD8232	Radio, Wireless
Blood pressure	Blood pressure monitoring system	AD8232、MAX30100	Bluetooth, ZigBee
Heart rate	Heart rate monitor	AD8232	Wireless, BT, ZigBee
Bodyweight	Body scale (Kg)		Wireless, BT, ZigBee
Body	Body	NTC	Xbee,

Temperature	Temperature sensor (C)		Wireless, ZigBee
Respiration rate	Breath sensor (Airflow)	MAX30100	Wireless, ZigBee

2.2. Enterprise Architecture

Zachman first defined the definition of enterprise architecture (EA): Enterprise architecture is a comprehensive discussion of all the key elements and relationships that make up an enterprise [15]. Weill [16] defined "Enterprise Architecture is the organizing logic for business processes and IT infrastructure reflecting the integration and standardization requirements of the firm's operating model. " In other words, the enterprise architecture can adjust the use of IT technology, so that IT investments can cooperate with the implementation of corporate strategies and achieve strategic goals. For the discussion of enterprise architecture issues, we will start from the perspective of six views: What, Why, How, Where, Who, Who to understand what is enterprise architecture, what is the purpose of enterprise architecture, how is it structured, and how is it used and who is using enterprise architecture.

Chou et al. [17] summarized three viewpoints of the EA. The first: EA refers to the organizational enterprise structure or documents and diagrams that describe organizational structure; the second: EA refers to the methodology of business operations, which used to understand the organization's operation and describe the organizational structure of the enterprise; the third: EA refers to a reference model used by business teams to construct an EA description using an EA methodology. In short, the current EA divided into three major viewpoints: the first viewpoint focuses on the structure of the enterprise; the second viewpoint focuses on the behavior of the enterprise, and the third viewpoint is the structure-behavior coalescence of the enterprise. Chao [2] proposed the Structure-Behavior Coalescence (SBC) Methodology includes six major diagrams, called The Six Golden Rules, and there are Architecture Hierarchy Diagram (AHD), Framework Diagram (FD), Component Operation Diagram (COD), Component Connection Diagram (CCD), Structure Behavior Coalescence Diagram (SBCD), and Interaction Flow Diagram (IFD). The SBC Methodology adopted in this research, as shown in Fig. 2:

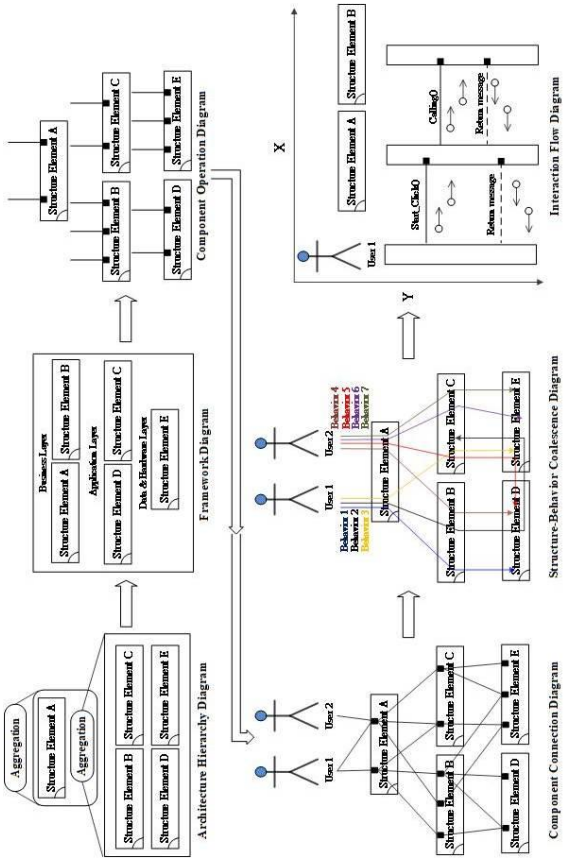


Figure 2. The Six Golden Rules of SBC Methodology [18].

III. THE ARCHITECTURE-ORIENTED MEDICAL MANAGEMENT SYSTEM MODELING

3.1 The Architecture-Oriented Medical Management System Modeling

Chao [18] 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) [2][19]. 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 an 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). The SBC description language has 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) and emphasized on information security of IoT [19][20].

An architecture hierarchy diagram (AHD) used to structure the Architecture-Oriented Medical Management System (AOMMS) for decomposition and combination to understand the complex Smart Healthcare Cloud Applications, IoT, and Services systems. The structural elements of the IoT security management model were the basic elements, and they composed of the model structure, as shown in Fig. 3:

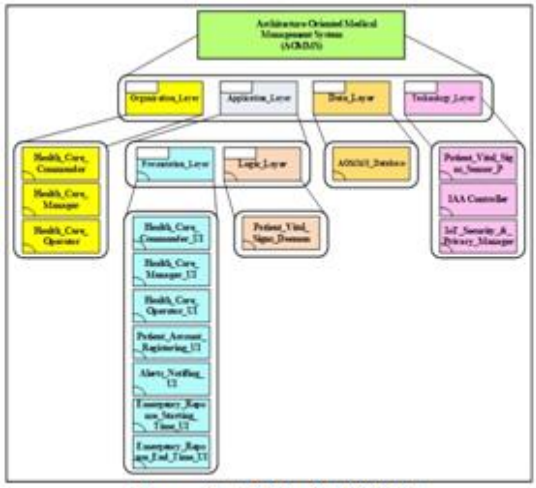


Figure 3. AHD of AOMMS

Figure 3. AHD of AOMMS

The necessary structure elements analyzed from the model and composed of Organization_Layer,Application_Layer, Data_Layer, and Technology_Layer. Organization_Layer composedofHealth_Care_Commander,Health_Care_Manager,andHealth_Care_Operator.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 AOMMS_Database. Technology_LayeriscomposedofPatient_Vital_Signs_Sensor_P, IAA (Identification, Authorization, and AccessControl)_Contorller,andIoT_Security_&_Privacy_Manager.

After the collection of non-aggregated systems or structural elements of the architecture hierarchy diagram, we obtain the Framework Diagram (FD). Organization_Layer contains Health_Care_Commander, Health_Care_Manager, and Health_Care_Operator. Presentation_Layer and Logic_Layer are sub-layers of Application_Layer. Presentation_LayercontainsthePatient_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 AOMMS_Database component. Technology_Layer contains the Patient_Vital_Signs_Sensor_P, IAA _Contorller, and IoT_Security_&_Privacy_Manager components

For a system, we use the component operation diagram (COD) to illustrate all the component's operations. COD is the third fundamental diagram to achieve structure-behavior coalescence. The structure components provide many operations through the interface, or work content of the structural components with input or output parameters is called a COD [21][22]. The input parameter of the service denoted by an arrow symbol directed to the 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 obtained for the AOMMS.

A structure component connection diagram (CCD) connects operations between the various structural components following its priorities. CCD obtained after the analysis phase finished. We use the CCD to describe how the components and actors (in the external environment) connected within AOMMS. CCD is the fourth fundamental diagram to achieve structure-behavior coalescence. The 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 Fig. 3.5, systems architect can see that systems structure and systems behavior coexist in the Structure Behavior Coalescence Diagram (SBCD). Systems architects not only see its systems structure but also see its systems' behavior simultaneously in the SBCD of AOMMS. From the structure element diagram and structure element service diagram, we further derive out nine behaviors of the AOMMS model: (1) Healthcare Strategic Management Behavior (2) Healthcare

Operational Management Behavior (3) Healthcare Operation Behavior (4) Alerts Notifying Behavior (5) Registering Patient Account Behavior (6) Recording Emergency Response Starting Time Behavior (7) Recording Emergency Response End Time Behavior (8) Sensing Patient Vital Signs Behavior, and (9) IoT Security and Privacy Management Behavior.

SBCD is the structure-behavior coalescence diagram we obtain after the architecture construction finished. It shows an SBCD of the AOMMS in which interactions among Health_Care_Commander, Health_Care_Manager, Health_Care_Operator, the Five_Minute_Interval,Healhcare_Provider,

IoT_Security_Administrator,Server_Root,Patient_Vital_SignsactorsandHealth_Care_Commander_UI,

Health_Care_Manager_UI,andHealth_Care_Operator_UI,theAterts_Notifying_UI,Patient_Account_Registeritig_UI,
Emergency_Response_Starting_Time_UI,
Emergency_Response_End_Time_UI,
Patient_Vital_Signs_Daemon, AOMMS_Database, Patient_Vital_Signs_Sensor_P,
IoT_Security_&_Privacy_Manager, IAA_Controller componentsshalldrawforthRegistering_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 nine behaviors together provide the overall behavior of the AOMMS, as shown in Fig. 4:

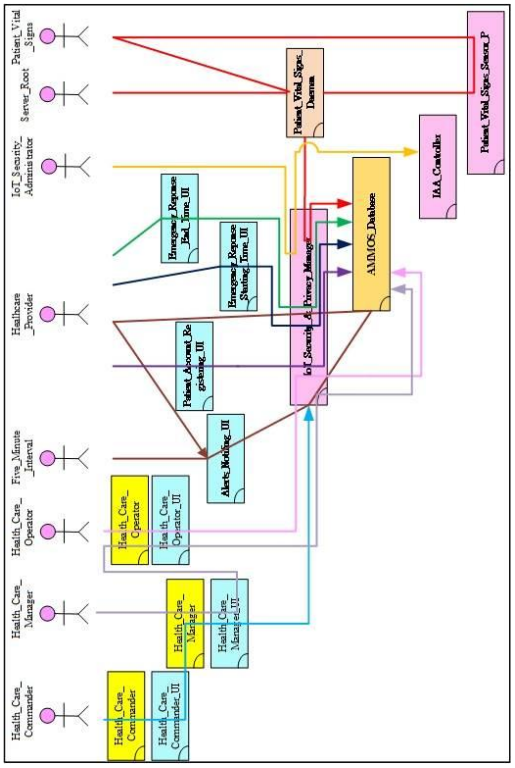


Figure 4. SBCD of AOMMS

The Interactive Flow Diagram (IFD) is the sixth golden rule of the six golden rule diagrams. This diagram explains the interaction between the external environment and components one by one so that the user can clearly understand how to deal with it through the way of the schema. To avoid the doubts caused by the plain text narrative, it is also worth noting that the direction of the information flow and the order of operation. The X-axis direction of the components and the Y-axis direction represents the time axis, and the higher the upper level serves the time, the following will explain one by one through an IFD.

IFD for the Healthcare Operational Management Behavior of AOMMS. First, the actor, the Health_Care_Manager, interacts with the Health_Care_Manager_UI component through Manage_Data call, carrying ID, and Password parameters. Next, the Health_Care_Operator component interacts with the Health_Care_Operator_UI component through Maintain_Data call, carrying ID, and Password parameters. Next, Health_Care_Operator_UI component interacts with the IoT_Security_&_Privacy_Manager component through Review_IoT_Security_&_Privacy_Manager call, carrying Current_Time parameters. Next, Health_Care_Operator_UI interacts with the IoT_Security_&_Privacy_Manager component through Review_IoT_Security_&_Privacy_Manager call, carrying Current_Time parameters. Next, the IoT_Security_&_Privacy_Manager component interacts with AOMMS_Database component through Review_IoT_Security_&_Privacy_Manager call, carrying Current_Time parameters. Next, the AOMMS_Database component interacts with the IoT_Security_&_Privacy_Manager component through Return_Data return message. Next, the IoT_Security_&_Privacy_Manager component interacts with the Health_Care_Manager component through Return_Data return message. Finally, the Health_Care_Operator_UI component interacts with the Health_Care_Manager component through Return_Data return message, carrying Return_Data parameters, as shown in Fig. 5:

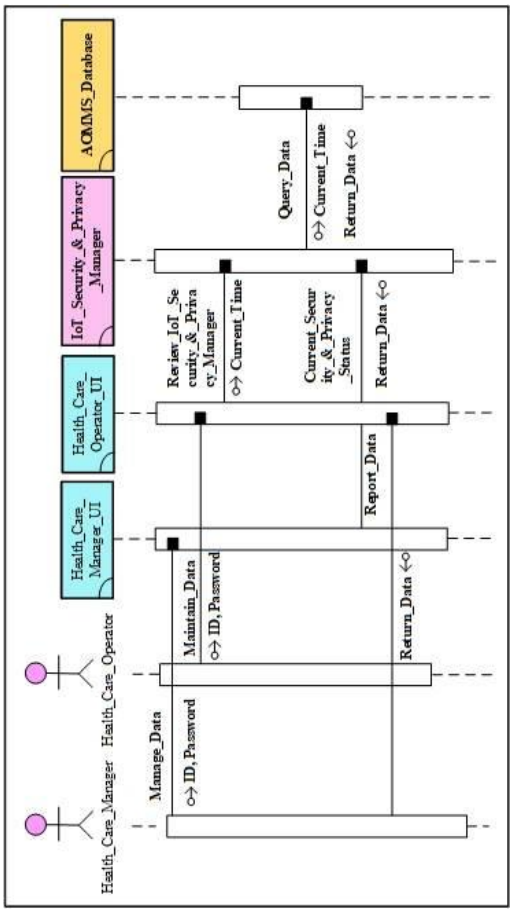


Figure 5. IFD for the healthcare operational management behavior of AOMMS

3.2. Enterprise Interviews

To understand the views of managerial and operational personnel on the structure-oriented and non-architectural medical management system practices, and to observe the advantages and disadvantages after comparing them, for this research design, three experts and scholars invited to assist, discuss and formulate ten questions for interviews with relevant personnel. The interview questions are as follows:

(1) Please briefly describe the current used medical management system?

(2) How many problems encounter when performs medical management operation?

(3) Is there any way to solve or change the problem with the question?

(4) If it is possible to implement improvements after taking the remediation measures for the problems? What are the results after the improvements?

(5) What kind of the unit's resources had used during the improvement?

(6) If the unit introduces the AOMMS methodology, can it solve the problems encountered at present? Please explain?

(7) Do you agree that the AOMMS methodology can shorten the time for the recruitment operation compared with the current process guidance?

(8) If assured sufficient funding and no information security concerns in the architecture orientation model, the introduction of new information devices (e.g., wearable devices, wireless networks, or cloud repositories) will help to make the overall approach comprehensive. Reform? If so, what are the reasons? If not, what are the reasons?

(9) What are the benefits of thinking the logic for the AOMMS methodology?

(10) What are the recommendations to the AOMMS?

This study interviews with the relevant departments of the medical management department. First, it explains what is the AOMMS methodology, and compares it with the current process-oriented medical management system methodology to understand architecture-oriented medical management system. We would like to know whether the AOMMS is more appropriate than the process-oriented medical management system.

During the interview process, the operators reflected that they often encounter unclear rights and responsibilities for the medical management system. After analyzing the interview records, it appears the AOMMS provides a visualized presentation. Because of the inconsistent level of knowledge in the units. Most of the executives who work in the office or field, the average number of employees is 20 over the years; he/she has his/her own set of operating modes. For academic research, some operators will not be easy to accept. Through the approval of the competent authorities, complete education training will provide, and the method of chart production and judgment will be used to manage the overall operations. It should be able to eliminate the gap in the level of knowledge.

IV. AOMMS MODEL COMPARED WITH NON-ARCHITECTURE-ORIENTED MODEL

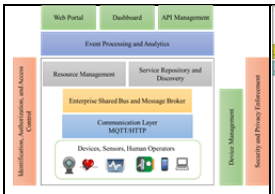
This section analyzes the results of the contrast between the architecture-oriented and non-architectural-oriented medical management system model.

4.1. Comparison of Architecture-Oriented and Non-Architectural-Oriented Medical Management System Model

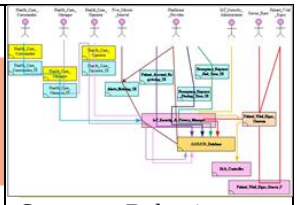
In the non-architectural-oriented Medical Management System model, it only focuses on enterprise behaviors such as management, notifying, registering, notify, recording, sensing, and IoT Security and Privacy Management. Therefore, the attachment of the organizational structure is unknown. It achieved a layered production method and a combination of logistics efficiency. It is easy

to cause problems of power and responsibility and fall into a function-oriented and not self-aware situation.

The AOMMS adopts the SBCM. The SBC methodology is to first construct the components and services in the organizational structure of each unit belonging to the structure and then interact with each other through service. Looking at the structures of the Medical Management System model, it is simple and clear. Since the architectural innovation adopts the SBC, we can see the organizational structure and corporate behavior of the medical management and operations at the same time, as shown in Fig. 6 and Tab. 2:



A Reference Architecture for IoT (Redraw from WSO2 [6])



Structure-Behavior Coalescence Diagram of AOMMS

Figure 6. Comparison of non-architectural-oriented and architecture-oriented AOMMS model

Table 2. Architecture-Oriented and Non-Architectural-Oriented Medical Management System

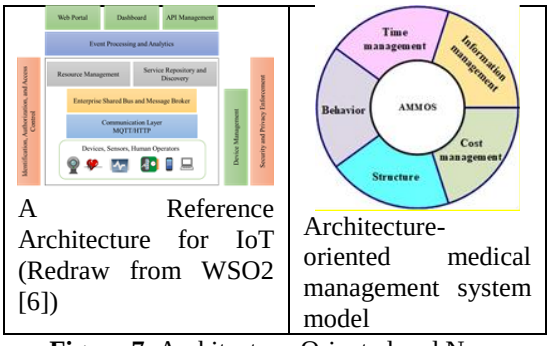
Dimension	AOMMS	Non-Architectural-Oriented
Behavior	The AOMMS clearly understands the organizational medical processes, and the duties required by the unit coordination and strive for more time to do core medical tasks.	In the process-oriented model, the organizational structure is convenient, according to the unit itself, and the tasks that can be performed by others can be carried out by other groups. The relevant units must perform the work of the non-units in charge of the business so that the tasks can carry out, and the medical treatment tasks cannot effectively and quickly promote.
Structure	In the architecture-oriented model, units include the Healthcare Commander, the Healthcare Manager, the Healthcare operator, the Healthcare provider, the IoT security Administrator. Organization_Layer composed of Health_Care_Commander, Health_Care_Manager, and Health_Care_Operator. The system interfaces are responsible for the system's component: management, operation, notification, emergency response time, and IoT security & Privacy Manager. Logic_Layer is composed of Patient_Vital_Signs	All levels of units can only enter the corresponding system interface according to their respective professional and authority. It resulted in the need to apply for more accounts and open many system interfaces at the same time to perform tasks as scheduled, which indirectly affects the speed of task execution.

	Deamon. The data layer identifies AOMMS databases, and the Technology Layer is composed of Patient_Vital _Signs_Sensor_P, IAA (Identification, Authorization, and Access Control)_Contorller, and IoT_Security _&_Privacy_ Manager, all of which are related. It is obvious.	
Information management	In the architecture-oriented model, it recommended integrating the AOMMS database into a medical management system. When performing the notification task, the display information seen by the relevant units is the same. Avoid information gaps.	Because each unit can divide according to its rights and responsibilities, the managerial personnel can only query the management system. The operator personnel can only use the management system, resulting in information that cannot connect in series, and it is easy to apply for the wrong medical treatment.
Time management	In the architecture-oriented model, many steps integrated and merged into one. During the interview, it logically verified that about 1 to 3 hours of work time could be saved between the medical manager and the operation relatively improve the efficiency of replenishment.	Due to the process-oriented approach, hierarchical control required, and the query is confirmed repeatedly. As long as an error occurs, the problem of shirking responsibility will generate, and the equipment will reserve for distribution. After the cause found, the follow-up operation can be performed, which is accessible in time - caused a significant consideration.
Cost management	The architecture-oriented model is a combination of structure and behavior. People from all walks of life have a better understanding of the general task. They also know how to do it and have good interaction with other partners. They can successfully achieve	The process-oriented model separates the structure from the behavior. The operators at all levels have a complete concept of lack of operation after the task is delivered. They only perform their professional aspects.

	immediate compensation goals. When performing tasks, the combination of structure and behavior can ultimately and allocate resources and accomplish tasks efficiently.	Even if the wrong operation information obtained, it will still execute blindly, resulting in a more extensive follow-up discovery. When encountered the error and then to figure out the cause of the failure. It is too late, and the personnel of each department can only shun the responsibility and fail to reach a useful immediate target. The correction of the error is costly.

4.2. Comparison of Architecture-Oriented and Non-Architectural-Oriented Medical management system Model

Comparison of Architecture-Oriented and Non-Architectural-Oriented Medical management system Model, as shown in Fig. 7:



A Reference Architecture for IoT (Redraw from WSO2 [6])

Architecture-oriented medical management system model

Figure 7. Architecture-Oriented and Non-Architectural-Oriented Medical Management System Model

The non-architectural-oriented medical management system model only shows medical management processes, and it cannot grasp the multiple aspects of the enterprise structure. On the other hand, the AOMMS emphasizes multiple-views of the enterprise. It is a complex system, including various perspectives: unit organization (structure), operation (behavior) facet logistics management (analysis), are all in the enterprise structure. Suppose we do not want to see all the enterprise architecture of the medical management system, but only want to understand the corporate behavioral structure. At this time, we can project the behavior from the enterprise architecture and get it - behaviors of the medical management system. Therefore, the AOMMS model can enable managerial personnel and operational personnel to grasp the overall picture of the medical management system. The AOMMS is presented like the mandala flower, extending outward from the central core of the interior, and can also interpret as being gradually concentrated from the outer perimeter to the inner core. After the development of the AOMMS model, the five facets of time management, behavior management, information management, structure management, and thinking orientation can implement effectively

V. CONCLUSIONS AND RECOMMENDATIONS

The risk of IoT devices used in the medical management system is a 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 mechanisms, 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, the risk of user data leakage, getting equipment control (prevent replay attack). The current IoT equipment manufacturers should establish as soon as possible awareness and prevention capabilities. Data manages as light as possible. Information security education for personnel of the enterprise.

By this study introduction and elaboration of the enterprise architecture of protecting the security and privacy of personal information in the medical management system, we may clearly understand how the SBC helps architects effectively construct fruitful enterprise architecture and the preservation of digital evidence. The AOMMS enterprise architecture focuses on (1) Verifying input data for security and privacy checks before storing data in the AOMMS database. (2) Verify inputting

emergency response starting or end time for security and privacy checks before updating data in the AOMMS database. (3) Verify PVS alerts data for security and privacy checks before updating data in the AOMMS 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. (7) The AOMMS clearly defined the structure and behavior of the medical management system to the preservation of digital evidence for protecting information security and personal information.

REFERENCES

[1]. V. Chellappan and K.M. Sivalingam, Security and privacy in the Internet of Things in Rajkumar Buyya and Amir Vahid Dastjerdi (Ed.), the Internet of Things, (New York: Morgan Kaufmann, 2016).
[2]. William S. Chao, Theoretical Foundations of Structure-Behavior Coalescence (Amazon Digital Services LLC, 2015).
[3]. K. Ashton, That 'internet of things' thing, RFID J., 22(7), 2009, 97–114.
[4]. Russell, Brian, and Drew Van Duren, Practical Internet of Things Security (Birmingham: Packt Publishing, 2016, 336).
[5]. International Telecommunication Union, "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, 2012).
[6]. Fremantle, Paul, "A reference architecture for the Internet of Things," WSO2 (2015).
[7]. Martin Bauer, Nicola Bui, Jourik De Loof, Carsten Magerkurth, Andreas Nettstra ¨ter, Julinda Stefa, and Joachim W. Walewski, IoT Reference Model, in Alessandro Bassi et al. (Ed.) Enabling Things to Talk (IoT-A, New York: Springer Open, 2013) 113-115.
[8]. Rajkumar Buyya and Amir Vahid Dastjerdi, "Internet of Things" (New York: Morgan Kaufmann, 2016).
[9]. V. Chellappan and K.M. Sivalingam, Security and privacy in the Internet of Things, in Rajkumar Buyya and Amir Vahid Dastjerdi (Ed.), the Internet of Things (New York: Morgan Kaufmann, 2016).
[10]. Elkhodr, Mahmoud, Seyed Shahrestani, Hon Cheung, "Internet of Things Research Challenges," IGI , 2016.
[11]. Eltayeb, Mohamed, Privacy and Security in Security Solutions for Hyperconnectivity and the Internet of Things, Edited by Maurice Dawson; Marwan Omar; (Mohamed Eltayeb, Hershey: IGI Global, 2017).
[12]. B. Chaudhry, J. Wang, SY. Wu, Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Ann Intern Med;144(10), 2006, 742-752.
[13]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M., Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, 29(7), 2013, 1645–1660.
[14]. K. Natarajan, B. Prasath, & P. Kokila, Smart Health Care System Using Internet of Things, Journal of Network Communications and Emerging Technologies, 6(3), 2016, 37-42.
[15]. Zachman, "Zachman Institute for Framework Advancement," Browsed on Jan. 20, 2020, http://www.zifa.com. (1987).
[16]. Peter Weill, Enterprise Architecture, MIT Center for Information Systems Research, presented at the Sixth e-Business Conference, 2007, Barcelona, Spain.
[17]. Henry Chou, Pingwen Yu, William S. Chao, Study on Architecture-Oriented Court Affairs Management Model, Journal of Information, Technology and Society, 18(1), 2010, 1-23.
[18]. Wei-ming Ma, A Study of Information Security of Internet of Things in WLAN, Journal of Global Business Operation and Management, 9, 2017, 121-133.
[19]. William S. Chao, Systems Architecture of Smart Healthcare Cloud Applications and Services IoT System: General Architectural Theory at Work, (Amazon Digital Services LLC, 2016)
[20]. William S. Chao, Systems Architecture of Smart Home Security Cloud Applications and Services IoT System: General Architectural Theory at Work (Amazon Digital Services LLC, 2016).
[21]. R. Sweeney, Achieving Service-Oriented Architecture: Applying an Enterprise Architecture Approach (Hoboken: Wiley, 2010).
[22]. J.P. Lawler and H. Howell-Barber, Service-Oriented Architecture: SOA Strategy, Methodology, and Technology (New York: Auerbach Publications, 2007).